GITHUB CHANNEL PARTNER DATA PROTECTION ADDENDUM

This Data Protection Addendum (this "Addendum") by and between Channel Partner and GitHub is made a part of and incorporated into the Agreement, as defined below. Capitalized terms not defined in this Addendum have the meanings ascribed to them in the Agreement. Unless explicitly agreed otherwise by the Parties in the Agreement in express reference to this Addendum, the terms of this Addendum will supersede those of the Agreement in the event of a conflict or inconsistency.

1 Definitions

1.1 "Agreement" refers to each service or similar agreement between Channel Partner and GitHub, whether entered into prior to, on or after the Addendum Effective Date, under which Channel Partner is processing GitHub Protected Data on GitHub's behalf, along with any related statement of work, order form, terms of service, or any other representation of services or documentation included in, referenced by, or otherwise incorporated into in the agreement.

1.2 "Applicable Data Protection Laws" refers to all international, national, state and local laws, regulations, regulatory frameworks, binding decisions by courts or regulatory authorities and other legislation relating to the processing or security of Personal Data, as applicable to, or in connection with, GitHub's use of Channel Partner or Channel Partner's processing of GitHub Personal Data. The Applicable Data Protection Laws will include, without limitation:

a. The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. ("CCPA"); and
b. The General Data Protection Regulation (EU) 2016/679 ("GDPR"), along with any implementing or supplementing national laws or regulations;
c. The GDPR as transposed into national law of the United Kingdom by the UK European Union (Withdrawal) Act 2018 and amended by the UK Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR");

each as may be amended from time to time.

1.3 "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "processing" or "process", "Processor" and "Supervisory Authority" will have the meanings given to them in the definitions set forth in the Applicable Data Protection Laws. In the absence of such definitions, the terms will have the following meaning:

a. "Controller" will mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;
b. "Data Subject" will mean an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
c. "Personal Data" will mean any information relating to a Data Subject;
d. "Personal Data Breach" will mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
e. "Processing" or "Process" (or "processing" or "process") will mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
f. "Processor" will mean a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller; and

g. "Supervisory Authority" will mean a supervisory or other regulatory agency or authority concerned by the processing of Personal Data.

1.4 "Data Breach" refers to a Personal Data Breach or any other confirmed or reasonably suspected breach of GitHub Protected Data.

1.5 "GitHub Personal Data" means any Personal Data processed by Channel Partner on behalf of GitHub under or in connection with the Agreement, whether supplied by GitHub for processing by Channel Partner or collected or generated by Channel Partner in the course of performing its obligations under the Agreement. GitHub Personal Data may, without limitation, include data such as billing information, IP addresses, corporate email addresses, and any other Personal Data.

1.6 "GitHub Customer Repository Data" means any data or information that is uploaded by or on behalf of GitHub customers or customers of GitHub's affiliates into their GitHub repository or other cloud or online storage services provided by GitHub and processed or otherwise handled by Channel Partner under or in connection with the Agreement.

1.7 "GitHub Protected Data" includes any GitHub Personal Data and GitHub Customer Repository Data.

1.8 "GitHub Protected EU/EEA Plus Data" refers to GitHub Protected Data processed in the context of the activities of a business establishment in the EU/EEA or Switzerland or relating to Data Subjects in the EU/EEA or Switzerland.

1.9 “GitHub Protected UK Data” refers to GitHub Protected Data processed in the context of the activities of a business establishment in the United Kingdom or relating to Data Subjects in the United Kingdom.

1.10 "Permitted Purposes" for data processing refers to those limited and specific purposes identified in the Agreement, an Order, or the Data Processing Exhibit with respect to the contractual services to be provided by Channel Partner.

1.11 "Sensitive Data" refers to any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data or biometric data processed for the purposes of uniquely identifying a natural person; data concerning health, a natural person’s sex life or sexual orientation; and data relating to criminal convictions and offenses.

1.12 "Standard Contractual Clauses" means either of the following sets of Standard Contractual Clauses, as applicable in the individual case to the transfer of Personal Data according to Section 7.1 below:

a. the Standard Contractual Clauses (MODULE TWO: Transfer controller to processor), dated 4 June 2021, for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as described in Article 46 of the GDPR and approved by European Commission Implementing Decision (EU) 2021/91 (“Standard Contractual Clauses (EU/EEA)”). The Standard Contractual Clauses (EU/EEA) are set forth in Attachment 1 to this Addendum;

b. the Standard Contractual Clauses (Processors), dated 5 February 2010, for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR, approved by European Commission Decision 2010/87/EU and recognized by the regulatory or supervisory authorities of the United Kingdom for use in connection with data transfers from the United Kingdom (“Standard Contractual Clauses (UK)”). The Standard Contractual Clauses (UK) are set forth in Attachment 2 to this Addendum.

1.13 "Subprocessor" refers to any Processor involved by Channel Partner, in accordance with the terms and provisions of this Addendum, in the processing of GitHub Protected Data for the sole purpose of providing all or some of the services contemplated under the Agreement.

2 Overall Status and Compliance

2.1 Data Processing. Depending on its nature and origin, GitHub may either be the Controller or a Processor of GitHub Personal Data. Channel Partner consequently processes GitHub Personal Data in its capacity as GitHub's Processor or subprocessor, as the case may be.

2.2 GitHub Compliance. GitHub represents and warrants that it will comply with the Applicable Data Protection Laws and will only transfer GitHub Personal Data to Channel Partner for the Permitted Purposes.

2.3 Channel Partner Compliance. Channel Partner represents and warrants that it will comply with the Applicable Data Protection Laws and will only process GitHub Personal Data on behalf of GitHub.

3 General Data Protection

3.1 Data Processing Description. Channel Partner has completed the attached *Data Processing Exhibit* regarding its processing of GitHub Protected Data.

3.2 Compliance with Instructions. Channel Partner will process GitHub Protected Data only in accordance with GitHub's instructions as represented by the Agreement and other written communications. Where GitHub is a Processor and Channel Partner a subprocessor of GitHub Protected Data, GitHub may give Channel Partner instructions on behalf of the Controller and Channel Partner will follow such instructions as if GitHub was the Controller. Channel Partner will immediately inform GitHub if, in its opinion, an instruction infringes the Applicable Data Protection Laws.

3.3 Data Quality and Proportionality. Channel Partner will enable GitHub to (i) keep GitHub Protected Data up to date, and to (ii) ensure that GitHub Protected Data Channel Partner collects or generates on GitHub's behalf (if any) is adequate, relevant, and not excessive in relation to the purposes for which it is processed. In no event will Channel Partner intentionally collect Sensitive Data on GitHub's behalf.

3.4 Assistance. Channel Partner will provide reasonable assistance to GitHub with concerns such as data privacy impact assessments, consultations with Supervisory Authorities, Data Subject rights requests, and other similar matters, in each case solely in relation to the processing of GitHub Protected Data and taking into account the nature of the processing and the information available to Channel Partner.

3.5 Data Return, Deletion and Retention. Upon GitHub's request and at GitHub's choice, Channel Partner will, within thirty (30) days of the request, return, or enable GitHub to download in a commonly used and machine-readable format, any GitHub Protected Data and delete any GitHub Protected Data from all locations where it is stored by or on behalf of Channel Partner. Channel Partner may retain GitHub Protected Data if, to the extent and for as long as required by applicable law, provided Channel Partner will notify GitHub of such requirement and the scope and nature of the resulting data retention. Upon GitHub's request, Channel Partner will promptly certify to GitHub in writing that it has complied with the obligations set forth in this Section 3.5.

4 Security, Accountability and Audit Obligations

4.1 Technical and Organizational Security Measures. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Channel Partner will implement and maintain throughout the term of the Agreement appropriate technical and organizational measures to ensure a level of security appropriate to the risks, such as against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, presented by processing GitHub Protected Data. Without limiting the foregoing, the technical and organizational measures to be implemented and maintained by Channel Partner will, at a minimum, include the measures set forth in any description of security measures that might be included or referenced in, or attached to, the Agreement. In addition, Channel Partner must maintain

a. an availability and disaster recovery process, including backups of GitHub Protected Data, to ensure complete recovery of data is guaranteed should a disaster recovery event occur within the services to be provided under the Agreement; and
b. a process for restoring critical business functions in the event of a business continuity event.

Throughout the term of the Agreement, Channel Partner will regularly test, assess and evaluate the effectiveness of implemented technical and organizational measures and make any adjustments necessary to comply with the obligations set forth in this Section 4.1.

4.2 Incident Response and Breach Notification. Channel Partner will maintain an incident response function capable of identifying, mitigating the effects of, and preventing the recurrence of Data Breaches. Upon discovering or otherwise becoming aware of a Data Breach, Channel Partner will promptly investigate the cause, nature and consequences of the Data Breach and take all reasonable measures to mitigate the harmful effects of the Data Breach. Channel Partner will notify GitHub without undue delay upon becoming aware of a Data Breach, but in no event more than 72 hours after awareness of the Data Breach. This notification must provide GitHub with sufficient information to allow it to meet its obligations under the Applicable Data Protection Laws, including at minimum a description of the nature of the Data Breach along with, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of records of GitHub Personal Data concerned; a description of the likely consequences of the Data Breach; a description of Channel Partner's actual or proposed remediation steps; a description of what steps, if any, GitHub can take to protect itself; and the name and contact information of the data protection officer or other contact information for receiving more information from Channel Partner. GitHub may request additional follow-up, including forensic investigation if deemed necessary by the type of data exposure. Unless required by applicable law, Channel Partner will not report, notify or otherwise communicate any information regarding a Data Breach to any third party or regulatory authority without first obtaining GitHub's prior written approval.

4.3 Channel Partner Personnel. Channel Partner represents and warrants that it has ensured that (i) all Channel Partner personnel processing GitHub Protected Data have agreed to keep GitHub Protected Data confidential, and that (ii) all Channel Partner personnel processing GitHub Protected Data have received adequate training to be able to comply with the obligations set forth in this Addendum and the Applicable Data Protection Laws.

4.4 Records and Documentation. Channel Partner will maintain complete, accurate, and up to date written records of all categories of processing activities carried out on behalf of GitHub containing the information required under the Applicable Data Protection Laws. To the extent this does not risk the security of Channel Partner or the privacy rights of individual Data Subjects, Channel Partner will make these records available to GitHub on request as reasonably required, such as to help GitHub demonstrate its compliance under the Applicable Data Protection Laws. In addition, upon request:

a. Channel Partner will make its privacy statements, policies and similar documentation available to GitHub. Channel Partner will also provide to GitHub any relevant compliance reports including, without limitation and where relevant: third party proof of PCI compliance (certificate), SOC 1 and/or SOC 2 audit report or HIPAA compliance attestation. GitHub will request such documentation no more than once annually.
b. Channel Partner will respond to, and cooperate with, GitHub regarding a GitHub Channel Partner Risk Assessment. For the term of the Agreement, GitHub may make one request annually for security and compliance risk-related information to be provided to it in writing to assess risk considerations. Channel Partner 's response will be provided in writing within thirty (30) days of receipt of the request, pending needed clarifications of any request.

4.5 Audit Rights. Should GitHub be involved in an audit initiated by a Supervisory Authority that requires participation from Channel Partner, or require an audit to ensure compliance with the Applicable Data Protection Laws and this Addendum, Channel Partner will fully cooperate with related requests and promptly provide access to knowledgeable personnel,

infrastructure, application software, audit reports, certifications, attestations, documentation and information as necessary to demonstrate its compliance with the Applicable Data Protection Laws and this Addendum in connection with its processing of GitHub Protected Data. In the event of such an audit or inspection, GitHub may use an independent third party (such as the Supervisory Authority, the Supervisory Authority's delegate or a third party auditor mandated by GitHub). Except in case of a Data Breach or as required by a Supervisory Authority, GitHub will provide Channel Partner with at least fifteen (15) days' prior notice of an audit or inspection. GitHub will request access to Channel Partner 's knowledgeable personnel, infrastructure and application software relevant to Channel Partner 's processing of GitHub Protected Data only during Channel Partner's business hours.

4.6 Communications with Agencies. Channel Partner permits GitHub to provide this Addendum and any relevant clauses of the Agreement to the U.S. Department of Commerce, the Federal Trade Commission, the Supervisory Authorities or competent courts on their request.

5 Receipt, Use and Disclosure of GitHub Protected Data

5.1 Receipt of GitHub Protected Data. Channel Partner acknowledges and confirms that it does not provide any payment, service, benefit or other consideration to GitHub in exchange for any GitHub Protected Data it receives from GitHub.

5.2 Access on Need-to-Know Basis. Channel Partner will make GitHub Protected Data accessible or otherwise available to its directors, officers, agents, representatives and employees only if and to the extent they have a need to know for Channel Partner to be able to provide the services contemplated under the Agreement.

5.3 Restrictions on the Use of GitHub Protected Data. Channel Partner must not collect, retain, use, share, disclose or otherwise process any GitHub Protected Data outside the direct business relationship with GitHub or for any purposes other than the Permitted Purposes. In particular, Channel Partner must not

a. communicate any GitHub Protected Data to third parties for monetary or other valuable consideration;
b. take any action that would cause any transfer of GitHub Protected Data to or from Channel Partner to qualify as "selling personal information" under the CCPA;
c. use GitHub Protected Data for the purposes of advertising any-third party goods or services; or
d. derive, exercise or grant to third parties any rights or benefits regarding GitHub Protected Data.

Channel Partner certifies, represents and warrants that it understands and will comply with the restrictions set forth in this Section 5.3.

5.4 Confidential Treatment. With the exception of Subprocessors, Channel Partner will treat as confidential and not disclose GitHub Protected Data to any third party.

6 Subprocessing and Onward Transfer

6.1 General Authorization to Engage Subprocessors. GitHub authorizes Channel Partner to engage (and permit each Subprocessor appointed in accordance with this Section 6 to engage) Subprocessors in accordance with this Section 6 and any other restrictions that may be set forth in the Agreement.

6.2 Current Subprocessors. A list of Subprocessors engaged by Channel Partner as of the Addendum Effective Date is set forth in Section 6 of the *Data Processing Exhibit*. Channel Partner may continue to use such Subprocessors for the processing of GitHub Protected Data, provided they meet the requirements set forth in Section 6.4 below.

6.3 Changes to Subprocessors. Channel Partner will, at any given time during the term of the Agreement, provide thirty (30) days' prior written notice to GitHub of the addition of a new Subprocessor or the replacement or removal of an existing Subprocessor. If GitHub has an objection to Channel Partner's engagement of a new Subprocessor reasonably related to the protection of GitHub Protected Data, GitHub will notify Channel Partner in writing within

fifteen (15) days following receipt of Channel Partner's notice. In the event GitHub objects to a new Subprocessor as set forth above, Channel Partner will use commercially reasonable efforts to implement a solution avoiding the processing of GitHub Protected Data by the objected-to new Subprocessor. In the event that Channel Partner is unable to provide such solution within fifteen (15) days following GitHub's objection, GitHub may terminate the Agreement with immediate effect and without any penalties. In this event, Channel Partner will refund to GitHub any fees (if any) paid by GitHub for unused services to be provided by Channel Partner under the Agreement following the effective date of the termination.

6.4 Protection of GitHub Protected Data. Prior to transferring, disclosing or otherwise making available any GitHub Protected Data to a Subprocessor, Channel Partner will ensure that

a. the Subprocessor provides sufficient guarantees to implement appropriate technical and organizational measures with respect to the processing of GitHub Protected Data;
b. the Subprocessor is contractually bound to comply with (i) the Applicable Data Protection Laws, and (ii) either the same obligations that Channel Partner is subject to under this Addendum or obligations at least as protective of GitHub Protected Data as Channel Partner's obligations under this Addendum; and that
c. the Subprocessor's access to GitHub Protected Data will be restricted to what is strictly necessary to perform the Subprocessor's services.

6.5 Liability for Subprocessors. Channel Partner will be fully liable to GitHub for the processing of GitHub Protected Data by Subprocessors and the performance of their related obligations.

6.6 Disclosure of Subprocessor Agreements. Channel Partner will, upon GitHub's written request at any given time following the Addendum Effective Date, provide GitHub with a list of all Subprocessors it has engaged to process GitHub Protected Data, along with a copy of the data processing terms under which each Subprocessor processes GitHub Protected Data and information on the categories of GitHub Personal Data processed by each Subprocessor, the type of processing the Subprocessor performs, and the location of its processing. Pursuant to Subprocessor confidentiality restrictions, Channel Partner may remove any confidential or commercially sensitive information before providing GitHub with a copy of the data processing terms imposed on a Subprocessor. If and to the extent that Channel Partner cannot disclose confidential or commercially sensitive information to GitHub, Channel Partner must provide all information it reasonably can in connection with the data processing terms agreed upon with its Subprocessors and cooperate with GitHub as necessary for GitHub to confirm and demonstrate compliance with the Applicable Data Protection Laws.

7 GitHub Protected EU/EEA Plus Data

7.1 Standard Contractual Clauses. If and to the extent Channel Partner receives GitHub Protected EU/EEA Plus Data from GitHub or collects or generates such data on GitHub's behalf, the Standard Contractual Clauses (EU/EEA) (Attachment 1) and Applicable Data Protection Laws shall apply. If and to the extent Channel Partner receives GitHub Protected UK Data from GitHub or collects or generates such data on GitHub's behalf, the Standard Contractual Clauses (UK) (Attachment 2) and Applicable Data Protection Laws shall apply.

7.2 Compliance with Laws. Channel Partner represents and warrants that it complies with the Applicable Data Protection Laws. If and to the extent Channel Partner received GitHub Protected Eu/EEA Plus Data from GitHub or collects or generates such data on GitHub's behalf, Channel Partner represents and warrants that that it abides by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. Channel Partner shall ensure that all transfers of Personal Data to a third country or an international organization are made subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

7.3 Subprocessors. Prior to transferring, disclosing or otherwise making available any GitHub Protected EU/EEA Plus Data or GitHub Protected UK Data to a Subprocessor, Channel

Partner will ensure that the Subprocessor has agreed in writing to only process GitHub Protected EU/EEA Plus Data or GitHub Protected UK Data (i) in a country that is subject to an adequacy decision by the European Commission or UK government authorities (as applicable); or (ii) subject to the Standard Contractual Clauses (EU/EEA) or the Standard Contractual Clauses (UK) (as applicable), or any other appropriate safeguards for the transfer of GitHub Protected EU/EEA Plus Data or GitHub Protected UK Data as permitted in accordance with the GDPR, the UK GDPR or other Applicable Data Protection Laws.

8 Term, Suspension and Termination

8.1 Term. This Addendum will have the same term as the Agreement.

8.2 Suspension. In the event that Channel Partner is in breach of its obligations under this Addendum or the Applicable Data Protection Laws, GitHub may temporarily suspend the transfer of any or all GitHub Protected Data to Channel Partner and the processing of any or all GitHub Protected Data by Channel Partner until the breach is cured or the Agreement is terminated.

8.3 Termination With Cause. In addition to any termination rights GitHub has under the Agreement or this Addendum, GitHub may terminate the Agreement with immediate effect, without any penalties and without prejudice to any claims GitHub may have under the Agreement, at law or in equity in the event that:

a. Channel Partner is in material breach of, or notifies GitHub that it can no longer meet, any of its representations, warranties or obligations under this Addendum or the Applicable Data Protection Laws including, without limitation and to the extent applicable, its obligations under the Standard Contractual Clauses or any other appropriate safeguards for the transfer and protection of GitHub Protected EU/EEA Plus Data implemented by Channel Partner or the Parties in line with the GDPR or other Applicable Data Protection Laws;

b. the transfer and processing of all GitHub Protected Data has been temporarily suspended for longer than one (1) month pursuant to Section 8.2; or

c. Channel Partner is no longer carrying on business, is dissolved, enters receivership, or a winding up order is made on behalf of Channel Partner.

8.4 Breach. A material breach by Channel Partner of its obligations under this Addendum or the Applicable Data Protection Laws is considered a material breach under the Agreement.

8.5 Changes in Law or Regulation. If, at any time during the term of the Agreement, changes in law or regulation (i) render performance of this Addendum impossible or commercially unreasonable, or (ii) require modifications or amendments to this Addendum, and, in either case, GitHub notifies Channel Partner accordingly, Channel Partner will work with GitHub in good faith to renegotiate this Addendum and cure the impossibility or render performance of this Addendum commercially reasonable or, as the case may be, implement the required modifications or amendments to this Addendum. If, in either case, the Parties are not able to do so within thirty (30) days of GitHub's notice, GitHub may terminate the Agreement with immediate effect and without any penalties.

8.6 Notifications. In addition to other notification requirements in this Addendum, Channel Partner must notify GitHub as follows:

a. In the event that Channel Partner determines that it can no longer meet its representations, warranties or obligations under this Addendum, Channel Partner must notify GitHub in writing immediately.

b. In the event that changes in law or regulation render performance of this Addendum impossible or commercially unreasonable, Channel Partner must notify GitHub in writing immediately.

c. In the event that Channel Partner's data processing or privacy practices materially change in a way affecting the protection of GitHub Protected Data or GitHub's rights under the Agreement, Channel Partner must give GitHub thirty (30) days' prior written notice of the change.

8.7 Termination Requirements. Upon termination of the Agreement, Channel Partner must:

a. stop the processing of GitHub Protected Data;

b. within the earlier of ninety (90) days of termination or in response to GitHub's reasonable request, certify that it has returned, enabled GitHub to download and deleted all GitHub Protected Data pursuant to Section 3.5; and
c. provide GitHub with reasonable assurance and information demonstrating that Channel Partner has complied with its obligations in this Section 8.7.

In the event that GitHub reasonably believes Channel Partner is in breach of these requirements, GitHub reserves the right to audit Channel Partner under the terms of Section 4.5 to ascertain compliance.

8.8 Survival. Sections 4.6, 6.5, 8.8 and 9 of this Addendum will survive the termination of the Agreement indefinitely. Sections 4.4 (except Section 4.4 (b)), 4.5 and 6.6 of this Addendum will survive the termination of this Addendum for four (4) years. All other Sections of this Addendum will survive the termination of this Addendum for as long as Channel Partner might be processing GitHub Protected Data beyond the effective date of the termination. Channel Partner's obligations under this Addendum will survive any merger, acquisition, change of ownership, or other such transfer.

9 Liability for Data Processing

9.1 Limitations. Except as limited by the Applicable Data Protection Laws, Channel Partner 's liability to GitHub for any breach of this Addendum will be unlimited.

Addendum: Data Processing Exhibit

This Data Processing Exhibit sets forth specific details regarding the data processing of GitHub Protected Data by Channel Partner on behalf of GitHub. Channel Partner has completed this Data Processing Exhibit pursuant to Section 3.1 of the Addendum.

A. List of Parties

1 Data exporter(s)

The End Customer is the data exporter. GitHub, Inc. transfers the Personal Data to the Channel Partner acting as a subprocessor of GitHub, Inc.

GitHub address: see Agreement the Addendum is incorporated into.

GitHub contact person's name: see Agreement the Addendum is incorporated into.

GitHub activities relevant to data transferred under the Standard Contractual Clauses: The data exporter is a user of professional services provided by GitHub that require the processing of the Personal Data.

Signature and data: see Agreement the Addendum is incorporated into.

Role (controller/processor): the End Customer is the controller. GitHub acts as processor.

2 Data importer(s)

The Channel Partner is the data importer and receives the Personal Data as subprocessor of GitHub, Inc.

Name: see Agreement the Addendum is incorporated into.

Address: see Agreement the Addendum is incorporated into.

Contact person's name: see Agreement the Addendum is incorporated into.

Activities relevant to data transferred under the Standard Contractual Clauses: The data importer provides services to GitHub as described in the Agreement. The services require the processing of the Personal Data.

Signature and data: see Agreement the Addendum is incorporated into.

Role (controller/processor): subprocessor.

B. Description of Transfer

1 The subject matter and duration of the processing of GitHub Protected Data

[Information to be provided by Channel Partner, e.g. in reference to the performance of Channel Partner's obligations under the Agreement and the term of the Agreement]

2 The nature and purpose of the processing of GitHub Protected Data

[Information to be provided by Channel Partner, e.g. in reference to the collection, storage, analysis, alteration or other use of the GitHub Protected Data to achieve a certain outcome as contemplated by the Agreement]

3 The types of GitHub Protected Data to be processed

[Information to be provided by Channel Partner, e.g. first name, last name, address, contact information, etc.]

4 The types of sensitive data contained in GitHub Protected Data to be processed

[Information to be provided by Channel Partner, 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]

5 The categories of Data Subject to whom the GitHub Protected Data relates

[Information to be provided by Channel Partner, e.g. customers or employees of GitHub or of GitHub's affiliates, etc.]

6 The frequency of the transfer of GitHub Protected Data to be processed

[Information to be provided by Channel Partner, e.g. whether the data is transferred on a one-off or continuous basis]

7 The period for which GitHub Protected Data will be retained, or, if that is not possible, the criteria used to determine that period

[Information to be provided by Channel Partner, e.g. return or deletion of GitHub Protected Data according to Section 3.5 of the Addendum, etc.]

8 The competent supervisory authority/ies in accordance with Clause 13 of the Standard Contractual Clauses (EU/EEA)

The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679.

9 List of Channel Partner Subprocessors as of Addendum Effective Date

Subprocessor Name	Address and Location	Type and Duration of Processing by Subprocessor
[Information to be provided by Channel Partner]	[Information to be provided by Channel Partner]	[Information to be provided by Channel Partner]

The obligations and rights of GitHub and Channel Partner are set out in the Agreement and this Addendum.

Attachment 1: The Standard Contractual Clauses (EU/EEA)

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) 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 organisational 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 its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and

delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([1]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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. ([2]) 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

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

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 authorised to do so by the data exporter.

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

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

Clause 11

Redress

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

(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, organisation 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.

[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.

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([3]);

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

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

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

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

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the

country of destination; such notification shall include all information available to the importer.

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

In these cases, it shall inform the competent supervisory authority 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 the Netherlands.

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 the Netherlands.

(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 to the Standard Contractual Clauses (EU/EEA)

Please see Addendum (Data Processing Exhibit), which is incorporated herein by reference.

Annex II to the Standard Contractual Clauses (EU/EEA)

Description of the technical and organizational security measures implemented by the data importer:

1. Data Security Certifications

Data importer holds the following data security certifications:

[Information to be provided by Channel Partner]

2. Physical Access Controls

(a) Measures that data importer takes to restrict inappropriate access to personal data, and transfer of media and equipment on which personal data is stored, include:

(i) Data importer limits access to facilities where information systems that process personal data are located to identified authorized individuals.

(ii) Data importer maintains emergency and contingency plans for the facilities in which its information systems that process personal data are located.

(iii) Data importer personnel and subcontractors must obtain authorization prior to storing personal data on portable devices, remotely accessing personal data, or processing personal data outside Data importer's facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing personal data from Data importer's facilities.

(iv) Data importer maintains records of the incoming and outgoing media containing personal data, including the kind of media, the authorized sender/recipients, date and time, the

number of media and the types of personal data they contain.

(v) Data importer uses industry standard processes to delete personal data when it is no longer needed.

(vi) Data importer restricts access to personal data in media leaving data importer's facilities (e.g., through encryption).

(vii) Data importer classifies personal data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption).

(viii) Data importer maintains an inventory of all media on which personal data is stored. Access to the inventories of such media is restricted to data importer's personnel and subcontractors authorized in writing to have such access.

(b) Examples of physical access controls:

(i) Data importer uses a central datacenter access request process with authorized approvers.

(ii) Users must use two-factor authentication (biometrics and access card) to gain entry to sensitive areas.

3. Technical access controls

(a) Measures data importer takes to restrict access to its data-processing systems include:

(i) Data importer uses industry standard practices to identify and authenticate users who attempt to access information systems.

(ii) Data importer maintains and updates a record of personnel and subcontractors authorized to access data importer's systems that contain personal data.

(iii) Data importer uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

(iv) Data importer stores passwords in a way that makes them unintelligible while they are in force.

(v) Data importer identifies those personnel and subcontractors who may grant, alter or cancel authorized access to personal data and resources.

(vi) Data importer ensures that de-activated or expired identifiers are not granted to other individuals.

(vii) Data importer ensures that where more than one individual has access to systems containing personal data, the individuals have separate identifiers/log-ins.

(viii) Data importer maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

(ix) Data importer de-activates authentication credentials that have not been used for six months.

(x) Data importer requires that user sessions with access to personal data are automatically closed in case of non-activity during a pre-determined period of time of no more than ten minutes.

(xi) Data importer instructs users to log-off when leaving data importer-controlled premises or when computers are otherwise left unattended.

(xii) Data importer limits repeated attempts to gain access to the information system using an invalid password.

(xiii) Where authentication mechanisms are based on passwords, data importer requires that

the passwords are renewed regularly.

(xiv) Where authentication mechanisms are based on passwords, data importer requires the password to be at least eight characters long.

(b) Examples of technical access controls:

(i) Authentication mechanisms

- Connections to servers require dedicated credentials and the connection must originate from the data importer's controlled premises which has both physical and logical access controls
- Protected network gear and other infrastructure devices requires access using a two-factor security token and password

(ii) Password protections

- All passwords are converted to an obfuscated form using a one-way hash to prevent those with access to the authentication systems from deriving the actual passwords of other users
- Passwords must be changed according to a strict technical policy or they will expire and become unusable.

4. Use controls

(a) Measures data importer uses to restrict individuals from accessing personal data to which they do not have access privileges include:

(i) Data importer maintains a record of security privileges of individuals having access to personal data.

(ii) Data importer restricts access to personal data to only those individuals who require such access to perform their job function.

(iii) Data importer logs access and use of information systems containing personal data, registering the access ID, time, authorization granted or denied, and relevant activity.

(iv) Data importer's security personnel verify the logs every month to propose remediation efforts to identify any irregularities in access or use and propose remediation efforts for such irregularities, if any.

(v) Data importer's personnel and subcontractors with access to personal data are subject to confidentiality obligations.

(b) Measures data importer uses to keep unauthorized individuals from reading, copying, changing or removing personal data during processing and use or after storage include:

(i) Data importer has controls to avoid individuals assuming access rights they have not been assigned to gain access to personal data they are not authorized to access.

(ii) Data importer has anti-malware controls to help avoid malicious software gaining unauthorized access to personal data, in particular malicious software originating from public networks.

(c) Examples of use controls:

(i) Access privileges

- Data importer uses role-based security to establish permissions and access to each set of assets
- Access must be approved and granted by the designated asset owners
- When an employee ceases to be employed by data importer, access is removed

on a timely basis

(ii) System Maintenance

- Data importer requires the use of antivirus software which is centrally managed and controlled including the deployment of regular virus definition updates
- Data importer requires security patches to be deployed within 30 days for high priority security patches, or immediately in the case of critical or emergent issues
- Servers are scanned continuously for patch and antivirus compliance

5. Distribution controls

(a) Measures data importer uses that are designed to prevent unauthorized reading, copying, changing or removing of personal data during transmission or storage on media include:

(i) Data importer encrypts personal data that is transmitted over public networks.

(ii) Data importer tracks disclosures of personal data, including what data has been disclosed, to whom, and at what time.

(iii) Data importer imposes restrictions on printing personal data and has procedures for disposing of printed materials that contain personal data.

(b) Examples of distribution controls:

Asset classification and handling

(i) Print services do not run within the production environment – personal data to be printed must go through centralized security measures including physical access to printers and output material.

(ii) Employees with access to personal data are required to take training on the proper handling of personal data.

6. Input controls

(a) Monitoring and logging measures data importer uses to audit inputs, changes, and deletions from its data-processing systems include:

(i) Data importer logs the use of its data-processing systems containing personal data.

(ii) Logs include ID, time, authorization granted or denied, and relevant activity.

(iii) Data importer's security personnel verify logs every six months to propose remediation efforts to identify any irregularities in access or use and propose remediation efforts for such irregularities.

(b) Examples of input controls:

Logical access controls

(i) Access to all personal data assets is granted through role-based security measures.

(ii) Event logging provides an audit trail regarding access attempts (both successful and failed).

7. Purpose controls

(a) Measures data importer uses to limit processing it performs as a data processor to only processing in accordance with the instructions of the data controller include:

(i) Data importer restricts internal testing efforts with actual personal data.

(ii) When data importer does use actual personal data for testing, it provides, and documents, the relevant level of security for the processing.

(iii) Data importer backs up any actual personal data prior to using it for testing.

(iv) Data importer uses security logs only for their intended security purpose.

(v) When data importer is engaged to process special categories of data, data importer maintains logical separation between this data and other data.

(vi) Technical support personnel and subcontractors only have access to personal data when needed.

(b) Examples of purpose controls:

Separation of environments

(i) Data importer policy requires that test and production environments be physically and logically separated.

(ii) Network access control lists (ACLs) and firewall rules are in place to prevent cross-communication of environments.

8. Availability controls

(a) Measures data importer uses to protect against incidental destruction or loss of personal data include:

(i) Data importer does not initiate any data recovery procedures without the written authorization of the data exporter.

(ii) Data importer's redundant storage and its procedures for recovering personal data are designed to attempt to reconstruct personal data in its original state from before the time it was lost or destroyed.

(iii) Data importer uses a variety of industry standard systems to protect against loss of personal data due to power supply failure or line interference.

(iv) Data importer backs up copies of personal data at least once a week, unless no personal data has been updated during that period.

(v) Data importer stores backup copies of personal data and recovery procedures in a different place from where the primary computer equipment processing the personal data is located.

(vi) Data importer has specific procedures in place governing access to backup copies.

(vii) Data importer logs personal data restoration efforts, including the person responsible, the description of the restored personal data and which data (if any) had to be input manually in the recovery process.

(viii) Data importer reviews recovery and backup procedures at least every six months.

(ix) Data importer maintains procedures designed to allow for recovery of personal data within seven days.

(b) Examples of availability controls:

Backup security controls

(i) Backups are encrypted to prevent unauthorized disclosure.

(ii) Secure transport to the off-site storage facility is performed by a vetted and authorized security service supplier.

9. Administrative controls

(a) Measures data importer uses to document and track administrative oversight include:

(i) Data importer maintains security documents describing its security measures and setting

out the relevant procedures and responsibilities of data importer's personnel and subcontractors who have access to personal data.

(ii) Data importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering personal data.

(iii) Data importer has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

(iv) Data importer performed a risk assessment before processing the personal data or launching the Service.

(v) Data importer retains its security documents for at least five years after they are no longer in effect.

(b) Examples of administrative controls:

Security policies and standards

(i) Security policies and standards are approved and reviewed annually by executive management.

(ii) Data importer has a team designated to engage on all security incidents to provide triage, remediation, and notification services.

10. Training

(a) Data importer informs its personnel and subcontractors about relevant security procedures and their respective roles. Data importer also informs its personnel and subcontractors of possible consequences of breaching the security rules and procedures. Additionally:

(i) Data importer only uses anonymous personal data in training.

(b) Examples of training materials and programs:

Training requirements

(i) Staff must complete the yearly security training program.

(ii) Security policies and standards are available to all Data importer's personnel and subcontractors.

(iii) Privacy training is made available to engineering, support and operations personnel and subcontractors responsible for privacy compliance.

Signature of Channel Partner appears below.

Attachment 2: Standard Contractual Clauses (UK)

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,

Data exporter and data importer,

each a “party”; together “the parties”,

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

Clause 1: Definitions

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in the General Data Protection Regulation (EU 2016/679) 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 45(2) of the General Data Protection Regulation (EU 2016/679);

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

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

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

Clause 2: Details of the transfer

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

Clause 3: Third-party beneficiary clause

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

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

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

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

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

(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 the General Data Protection Regulation (EU 2016/679);

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

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

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

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

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6: Liability

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

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

successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

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

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

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

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

Clause 8: Cooperation with supervisory authorities

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

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

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

Clause 9: Governing Law.

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

Clause 10: Variation of the contract

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

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same

obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

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

Clause 12: Obligation after the termination of personal data processing services

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

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

Appendix 1 to the Standard Contractual Clauses (UK)

Data exporter: The End Customer is the data exporter.

Data importer: The data importer is Channel Partner acting as a subprocessor of GitHub, Inc.

Data subjects: Data subjects include any individual whose Personal Data is processed by the Service in support of the data processing services, including employees, contractors, collaborators, or customers of the data importer.

Categories of data: The personal data that may be collected and/or processed by the data importer include e-mail, documents and other data in an electronic form, as determined by the data exporter.

Special categories of data (if appropriate): Special categories of data should not be processed.

Processing operations: The data importer will process the personal data to deliver the relevant Service to the data exporter.

Appendix 2 to the Standard Contractual Clauses (UK)

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):

1. Physical Access Controls

(a) Measures that data importer takes to restrict inappropriate access to personal data, and transfer of media and equipment on which personal data is stored, include:

(i) Data importer limits access to facilities where information systems that process personal

data are located to identified authorized individuals.

(ii) Data importer maintains emergency and contingency plans for the facilities in which its information systems that process personal data are located.

(iii) Data importer personnel and subcontractors must obtain authorization prior to storing personal data on portable devices, remotely accessing personal data, or processing personal data outside Data importer's facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing personal data from Data importer's facilities.

(iv) Data importer maintains records of the incoming and outgoing media containing personal data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of personal data they contain.

(v) Data importer uses industry standard processes to delete personal data when it is no longer needed.

(vi) Data importer restricts access to personal data in media leaving data importer's facilities (e.g., through encryption).

(vii) Data importer classifies personal data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption).

(viii) Data importer maintains an inventory of all media on which personal data is stored. Access to the inventories of such media is restricted to data importer's personnel and subcontractors authorized in writing to have such access.

(b) Examples of physical access controls:

(i) Data importer uses a central datacenter access request process with authorized approvers.

(ii) Users must use two-factor authentication (biometrics and access card) to gain entry to sensitive areas.

2. Technical access controls

(a) Measures data importer takes to restrict access to its data-processing systems include:

(i) Data importer uses industry standard practices to identify and authenticate users who attempt to access information systems.

(ii) Data importer maintains and updates a record of personnel and subcontractors authorized to access data importer's systems that contain personal data.

(iii) Data importer uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

(iv) Data importer stores passwords in a way that makes them unintelligible while they are in force.

(v) Data importer identifies those personnel and subcontractors who may grant, alter or cancel authorized access to personal data and resources.

(vi) Data importer ensures that de-activated or expired identifiers are not granted to other individuals.

(vii) Data importer ensures that where more than one individual has access to systems containing personal data, the individuals have separate identifiers/log-ins.

(viii) Data importer maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

(ix) Data importer de-activates authentication credentials that have not been used for six months.

(x) Data importer requires that user sessions with access to personal data are automatically closed in case of non-activity during a pre-determined period of time of no more than ten minutes.

(xi) Data importer instructs users to log-off when leaving data importer-controlled premises or when computers are otherwise left unattended.

(xii) Data importer limits repeated attempts to gain access to the information system using an invalid password.

(xiii) Where authentication mechanisms are based on passwords, data importer requires that the passwords are renewed regularly.

(xiv) Where authentication mechanisms are based on passwords, data importer requires the password to be at least eight characters long.

(b) Examples of technical access controls:

(i) Authentication mechanisms

- Connections to servers require dedicated credentials and the connection must originate from the data importer's controlled premises which has both physical and logical access controls
- Protected network gear and other infrastructure devices requires access using a two-factor security token and password

(ii) Password protections

- All passwords are converted to an obfuscated form using a one-way hash to prevent those with access to the authentication systems from deriving the actual passwords of other users
- Passwords must be changed according to a strict technical policy or they will expire and become unusable.

3. Use controls

(a) Measures data importer uses to restrict individuals from accessing personal data to which they do not have access privileges include:

(i) Data importer maintains a record of security privileges of individuals having access to personal data.

(ii) Data importer restricts access to personal data to only those individuals who require such access to perform their job function.

(iii) Data importer logs access and use of information systems containing personal data, registering the access ID, time, authorization granted or denied, and relevant activity.

(iv) Data importer's security personnel verify the logs every month to propose remediation efforts to identify any irregularities in access or use and propose remediation efforts for such irregularities, if any.

(v) Data importer's personnel and subcontractors with access to personal data are subject to confidentiality obligations.

(b) Measures data importer uses to keep unauthorized individuals from reading, copying, changing or removing personal data during processing and use or after storage include:

(i) Data importer has controls to avoid individuals assuming access rights they have not been assigned to gain access to personal data they are not authorized to access.

(ii) Data importer has anti-malware controls to help avoid malicious software gaining unauthorized access to personal data, in particular malicious software originating from public networks.

(c) Examples of use controls:

(i) Access privileges

- Data importer uses role-based security to establish permissions and access to each set of assets
- Access must be approved and granted by the designated asset owners
- When an employee ceases to be employed by data importer, access is removed on a timely basis

(ii) System Maintenance

- Data importer requires the use of antivirus software which is centrally managed and controlled including the deployment of regular virus definition updates
- Data importer requires security patches to be deployed within 30 days for high priority security patches, or immediately in the case of critical or emergent issues
- Servers are scanned continuously for patch and antivirus compliance

4. Distribution controls

(a) Measures data importer uses that are designed to prevent unauthorized reading, copying, changing or removing of personal data during transmission or storage on media include:

(ii) Data importer encrypts personal data that is transmitted over public networks.

(ii) Data importer tracks disclosures of personal data, including what data has been disclosed, to whom, and at what time.

(iii) Data importer imposes restrictions on printing personal data and has procedures for disposing of printed materials that contain personal data.

(b) Examples of distribution controls:

Asset classification and handling

(i) Print services do not run within the production environment – personal data to be printed must go through centralized security measures including physical access to printers and output material.

(ii) Employees with access to personal data are required to take training on the proper handling of personal data.

5. Input controls

(a) Monitoring and logging measures data importer uses to audit inputs, changes, and deletions from its data-processing systems include:

(i) Data importer logs the use of its data-processing systems containing personal data.

(ii) Logs include ID, time, authorization granted or denied, and relevant activity.

(iii) Data importer's security personnel verify logs every six months to propose remediation efforts to identify any irregularities in access or use and propose remediation efforts for such irregularities.

(b) Examples of input controls:

Logical access controls

(i) Access to all personal data assets is granted through role-based security measures.

(ii) Event logging provides an audit trail regarding access attempts (both successful and failed).

6. Purpose controls

(a) Measures data importer uses to limit processing it performs as a data processor to only processing in accordance with the instructions of the data controller include:

(i) Data importer restricts internal testing efforts with actual personal data.

(ii) When data importer does use actual personal data for testing, it provides, and documents, the relevant level of security for the processing.

(iii) Data importer backs up any actual personal data prior to using it for testing.

(iv) Data importer uses security logs only for their intended security purpose.

(v) When data importer is engaged to process special categories of data, data importer maintains logical separation between this data and other data.

(vi) Technical support personnel and subcontractors only have access to personal data when needed.

(b) Examples of purpose controls:

Separation of environments

(i) Data importer policy requires that test and production environments be physically and logically separated.

(ii) Network access control lists (ACLs) and firewall rules are in place to prevent cross-communication of environments.

7. Availability controls

(a) Measures data importer uses to protect against incidental destruction or loss of personal data include:

(i) Data importer does not initiate any data recovery procedures without the written authorization of the data exporter.

(ii) Data importer's redundant storage and its procedures for recovering personal data are designed to attempt to reconstruct personal data in its original state from before the time it was lost or destroyed.

(iii) Data importer uses a variety of industry standard systems to protect against loss of personal data due to power supply failure or line interference.

(iv) Data importer backs up copies of personal data at least once a week, unless no personal data has been updated during that period.

(v) Data importer stores backup copies of personal data and recovery procedures in a different place from where the primary computer equipment processing the personal data is located.

(vi) Data importer has specific procedures in place governing access to backup copies.

(vii) Data importer logs personal data restoration efforts, including the person responsible, the description of the restored personal data and which data (if any) had to be input manually in the recovery process.

(viii) Data importer reviews recovery and backup procedures at least every six months.

(ix) Data importer maintains procedures designed to allow for recovery of personal data within seven days.

(b) Examples of availability controls:

Backup security controls

(i) Backups are encrypted to prevent unauthorized disclosure.

(ii) Secure transport to the off-site storage facility is performed by a vetted and authorized security service supplier.

8. Administrative controls

(a) Measures data importer uses to document and track administrative oversight include:

(i) Data importer maintains security documents describing its security measures and setting out the relevant procedures and responsibilities of data importer's personnel and subcontractors who have access to personal data.

(ii) Data importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering personal data.

(iii) Data importer has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

(iv) Data importer performed a risk assessment before processing the personal data or launching the Service.

(v) Data importer retains its security documents for at least five years after they are no longer in effect.

(b) Examples of administrative controls:

Security policies and standards

(i) Security policies and standards are approved and reviewed annually by executive management.

(ii) Data importer has a team designated to engage on all security incidents to provide triage, remediation, and notification services.

9. Training

(a) Data importer informs its personnel and subcontractors about relevant security procedures and their respective roles. Data importer also informs its personnel and subcontractors of possible consequences of breaching the security rules and procedures. Additionally:

(i) Data importer only uses anonymous personal data in training.

(b) Examples of training materials and programs:

Training requirements

(i) Staff must complete the yearly security training program.

(ii) Security policies and standards are available to all Data importer's personnel and subcontractors.

(iii) Privacy training is made available to engineering, support and operations personnel and subcontractors responsible for privacy compliance.

Signature of Channel Partner appears below.

Signing the Standard Contractual Clauses (EU/EEA) and the Standard Contractual Clauses (UK), including contained Appendices and Annexes on behalf of the data importer

Name:

Title:

Signature: _____ Company: