GitHub Data Protection Agreement

This GitHub Data Protection Agreement forms part of the GitHub Customer Agreement between Customer ("You") and GitHub, Inc., ("GitHub") covering Your legal entity's use of the Online Services. It sets forth the parties' obligations with respect to Customer Personal Data processed by GitHub. Capitalized terms not defined in this document shall have the meaning as provided elsewhere in your GitHub Customer Agreement.

1. Definitions.

A. "CCPA" means the California Consumer Privacy Act (Cal. Civ. Code §1798.100 et seq) and its implementing regulations.

B. "Customer Personal Data" means all data, including all text, sound, video, or image files, and software, that are provided to GitHub by or on behalf of Customer through use of the Online Services.

C. "DPA" means this GitHub Data Protection Agreement.

D. "Data Protection Requirements" means the applicable obligations imposed on GitHub by the GDPR, any subordinate legislation or regulations implementing the GDPR, the CCPA, and any other applicable laws, regulations, and other legal requirements applicable to GitHub and relating to:

i. Privacy and data security; or

ii. The use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

E. "GDPR" means:

i. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; and

ii. Regulation (EU) 2016/679 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 (as may be amended from time to time).

F. "GitHub Affiliate" means any entity that controls GitHub, is controlled by GitHub, or is under common control with GitHub.

G. "GitHub Customer Agreement" or **"Agreement"** means Your agreement(s) for the Online Services.

H. "Instructions" mean the activities you instruct GitHub to perform as Processor acting on Your behalf.

I. "Online Services" means any service or software that GitHub provides You under a written and executed agreement.

J. **"Preview"** means Online Services provided for preview, evaluation, demonstration, or trial purposes, and any beta, technical preview, or other pre-release versions of the Online Services.

K. "**Professional Services**" means training, consulting or implementation services provided by GitHub. Professional Services do not include support.

L. "**Professional Services Data"** means all Customer Personal Data that are provided to GitHub, by or on behalf of a Customer or that Customer authorizes GitHub to obtain from an Online Service or otherwise obtained or processed by or on behalf of GitHub through an engagement with GitHub to obtain Professional Services.

M. **"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data processed by GitHub on Your behalf.

N. "**Standard Contractual Clauses**" or "**SCCs"** means:

   i. where the GDPR applies the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "EU SCCs");

   ii. where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("UK Addendum"); and

   iii. where the Swiss Data Protection Act ("Swiss DPA") applies, the applicable standard data protection clauses issued, approved or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") (the "Swiss SCCs").

O. "**Subprocessor"** means a third-party Processor retained by GitHub to process Your data.

P. **"Subprocessor List"** means the list of Subprocessors identified on the GitHub website at https://github.com/subprocessors or a successor location.

Q. **"Troubleshooting"** means preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the relevant products. Troubleshooting includes fixing software defects and otherwise keeping the Online Services up to date and performant.

R. "**Controller**," "**Data Subject**," "**Personal Data**," "**Process**," and "**Processor**" have the meanings ascribed to them in the GDPR.

2. **Scope and Order of Precedence.**

   A. This DPA applies to all Online Services except:

      i. Products specifically identified as excluded in bespoke GitHub product terms, in which case those terms shall control so long as such terms are compliant with Data Protection Requirements, and

      ii. Previews, unless expressly designated by GitHub as being governed by this DPA. Previews may employ privacy and security measures that are different from those normally provided in Online Services and are offered under Preview Terms. Unless otherwise noted, Customers should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements.

   B. In the event of any other conflict or inconsistency between the terms of this DPA Terms and any other terms in the GitHub Customer Agreement, the terms of this DPA shall prevail. The terms of this DPA shall supersede any conflicting provisions with respect to the processing of Customer Personal Data or Professional Services Data.

3. **Processing Roles and Responsibilities.**

   A. Roles. You are the Controller of Customer Personal Data, and we are the Processor of that data, unless:

      i. You are the Processor of the Customer Personal Data. In that case, GitHub is a Subprocessor;

      ii. GitHub is an independent Controller processing Customer Personal Data for the purposes listed in Section 3.C of this DPA; or

      iii. Otherwise expressly stated in the specific terms applicable to a particular Online Service in accordance with Section 2.A.

   B. Your Processing Instructions to GitHub. You instruct GitHub to perform the following activities as Processor acting on Your behalf:

      i. **Provide Online Services** by:

         a. Providing and updating the Online Services as configured and used by You or Your users, and to make ongoing personalized experiences and recommendations;

         b. Troubleshooting; and

         c. Keeping Online Services up to date and performant, and enhancing user productivity, reliability, efficacy, quality, privacy, accessibility and security.

ii. **Provide Professional Services** by:

a. Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services;

b. Troubleshooting in connection with Professional Services; and

c. Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying product(s) based on issues identified while providing Professional Services, including fixing software defects, and otherwise keeping the Professional Services up to date and performant.

iii. **Process Customer Personal Data** as set out in:

a. Your GitHub Customer Agreement;

b. Annex I to the Standard Contractual Clauses; and

c. any other documented instruction provided by You and acknowledged in writing by GitHub as constituting instructions for purposes of this DPA.

C. GitHub's Independent Processing of Data. GitHub Processes some Customer Personal Data as an independent Controller. GitHub conducts such processing in compliance with Data Protection Requirements generally, and the GDPR specifically, and in a manner consistent with the purposes outlined in the GitHub Privacy Statement. Those exhaustive purposes are restated here for transparency and convenience:

i. account, billing, and customer relationship management and related customer correspondence;

ii. compensation (e.g., calculating employee commissions and partner incentives);

iii. complying with and resolving legal obligations, including responding to Data Subject requests for Personal Data processed by GitHub as Controller (for example website data), tax requirements, agreements, and disputes;

iv. abuse detection, prevention, and protection, virus scanning, and scanning to detect violations of terms of service and,

v. creating aggregated statistical data for internal reporting, financial reporting, revenue planning, capacity planning, and forecast modeling (including product strategy).

GitHub will not use or otherwise process Customer Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, (c) data selling or brokering, or (d) any other purpose, other than for the purposes set out in this section. You agree that GitHub may conduct this Processing.

D. Lawfulness of Instructions.

i. It is Your responsibility to ensure that Your Instructions comply with Data Protection Requirements. GitHub is not responsible for determining what laws or regulations apply to Your business, or for determining whether GitHub's provision of services meets the requirements of such laws.

ii. You will ensure that processing Customer Personal Data in accordance with your Instructions will not cause GitHub to violate any law or regulation, including Data Protection Requirements.

iii. GitHub will inform you if it becomes aware, or reasonably believes, that Your Instructions violate any applicable law or regulation.

E. Additional Instructions. The parties will agree to additional instructions outside the scope of the GitHub Customer Agreement or DPA in writing.

F. Disclosure of Customer Personal Data.

i. GitHub will not disclose or provide access to any Customer Personal Data unless it is:

a. in accordance with Your Instructions; or

b. as described in this DPA; or

c. required by law, in which case the Additional Safeguards Addendum in Annex IV to the Standard Contractual Clauses will apply.

ii. GitHub will not disclose or provide access to any Customer Personal Data to law enforcement unless required by law or compelled by legal process. Requests by law enforcement for Customer Personal Data will be directed to You where possible.

iii. GitHub will contact You if disclosure of Your Customer Personal Data is compelled and provide a copy of the legal process compelling the disclosure, unless we are legally prohibited from doing so.

G. Data Subject Rights. If GitHub receives a request from one of Your Data Subjects pertaining to an Online Service where GitHub functions as Your Processor or Subprocessor, GitHub will redirect the Data Subject to You. Consistent with the functionality of the Online Services and GitHub's role, we will cooperate with You and provide You the necessary means to respond. You are solely responsible for responding to these requests.

4. **Security.** GitHub will implement and maintain appropriate technical and organizational measures and security safeguards as set out in Annex II to the Standard Contractual Clauses. You and GitHub shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate:
    - **A.** the pseudonymisation and encryption of Personal Data;
    - **B.** the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
    - **C.** the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and,
    - **D.** a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

5. **Audit.** GitHub will provide You with security compliance reporting, such as external SOC1 Type 2 and SOC2 Type 2 and ISO 27001 audit reports, upon Your request. Should You be required to respond to a regulatory or supervisory request that requires GitHub's participation, and Your obligations cannot reasonably be satisfied with GitHub's standard security compliance reports, GitHub will promptly respond to Your additional Instructions and requests for information, in accordance with the following terms and conditions:
    - **A.** GitHub will provide access to relevant knowledgeable personnel, documentation, and application software.
    - **B.** You and GitHub will agree in writing upon the scope, timing, duration, control, and evidence requirements.
    - **C.** Unless GitHub is otherwise required by law or a supervisory authority of competent jurisdiction, GitHub will provide such access:
        i. if the regulator or supervisory authority uses an independent and accredited third-party audit firm;
        ii. during regular business hours;
        iii. on 30 days advance written notice; and
        iv. only to Your data and to those GitHub systems or facilities involved in the relevant Online Services. Neither You, Your regulators, or Your regulators' delegates shall have access to any data from GitHub's other customers or to GitHub systems or facilities not involved in the Online Services.
    - **D.** You will compensate GitHub for the expenses incurred by our cooperation, including all out-of-pocket costs and reasonable costs and fees for time GitHub expends, or services GitHub provides, in connection with such cooperation.
    - **E.** Unless prohibited by law from doing so, You will share with GitHub any reports, findings, or recommended actions pertaining to GitHub.

6. **Security Incidents.**
    - **A.** If GitHub becomes aware of a Security Incident, GitHub will without undue delay:
        i. notify You of the Security Incident, in accordance with the notice provisions in this DPA;
        ii. investigate the Security Incident and provide detailed information about it; and,
        iii. take reasonable steps to mitigate its effects and minimize any resulting damage.
    - **B.** GitHub's notification of or response to a Security Incident under this section is not an acknowledgement of any fault or liability.
    - **C.** You are solely responsible for complying with Your obligations under any incident notification laws. GitHub will assist you to the extent required under applicable law in fulfilling Your obligation to notify the relevant authorities and data subjects.
    - **D.** You must notify GitHub promptly about any possible misuse of Your accounts or authentication credentials, or any Security Incident related to an Online Service.
7. **Data Transfers and Location.** You appoint GitHub to transfer Customer Personal Data to the United States or any other country in which GitHub or its Subprocessors operate, and to store and process Customer Personal Data to provide the Online Services, subject to the safeguards below and described elsewhere in this DPA.
    - **A.** GitHub may transfer and process Customer Personal Data to and in the United States, to third-party countries (including those outside of the European Economic Area ("EEA") without an adequacy statement from the European Commission), and to Subprocessors, GitHub Affiliates, and our professional advisors. GitHub shall ensure that such transfers are made in compliance with Data Protection Requirements and this DPA. If you select and use an Online Service where certain data is stored at rest in a specific geographic area, GitHub will store the applicable data based on that instruction.
    - **B.** Any transfer of Customer Personal Data subject to this DPA from member states of the EU, EEA, Switzerland, or the United Kingdom to any countries where the European Commission, the FDPIC, or the UK Information Commissioner's Office has not decided that the third country or more specified sectors within that third country ensures an adequate level of protection, shall be undertaken:
        i. subject to GitHub's self-certification to the EU-US Data Privacy Framework and, as applicable, the UK Extension to the EU-US Data Privacy Framework and/or the Swiss-US Data Privacy Framework; and/or
        ii. through the Standard Contractual Clauses.

C. For the Standard Contractual Clauses, the Parties agree:

i. **Controller to Controller Transfers**. The SCCs shall apply to Personal Data that is protected by the GDPR and processed in accordance with Section 3.C of this DPA, completed as follows:

a. Module One will apply;

b. in Clause 7, the optional docking clause will apply;

c. in Clause 11, the optional language will not apply;

d. in Clause 17, Option 1 will apply, and the New EU SCCs will be governed by the law of the Netherlands; and,

e. in Clause 18(b), disputes shall be resolved before the courts of the Netherlands.

ii. **Controller to Processor/Processor to Processor Transfers**. The SCCs shall apply to Personal Data that is protected by the GDPR and processed in accordance with Section 3.B of this DPA, completed as follows:

a. Module Two or Module Three will apply (as applicable);

b. in Clause 7, the optional docking clause will apply;

c. in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 9 of this DPA;

d. in Clause 11, the optional language will not apply;

e. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the Netherlands; and,

f. in Clause 18(b), disputes shall be resolved before the courts of the Netherlands.

iii. **Transfers from the UK**. In relation to Personal Data that is protected by the UK GDPR, the UK Addendum will apply, completed as follows:

a. The SCCs shall also apply to transfers of such Personal Data, subject to sub-section (b) below;

b. Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the SCCs, completed as set out in Section 7.B.(i)-(ii) of this DPA, and the option “neither party” shall be deemed checked in Table 4; and,

c. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

iv. **Transfers from Switzerland**. In relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply in accordance with Sections 7.B.(i)-(ii) with the following modifications:

a. any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss Federal Data Protection Act;

b. references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as applicable; and,

c. references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the FDPIC and competent courts in Switzerland, unless the SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA, in which event the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in Annexes I and II of this DPA.

8. **Retention and Deletion.** Following the completion of the Services, to the extent that GitHub is a Processor and unless prohibited by law, GitHub will delete or return all the Customer Personal Data to You, whichever you elect, and delete existing copies in accordance with our retention and deletion policy.

9. **Subprocessors**.

A. GitHub may hire Subprocessors of our choosing. The above authorization constitutes Your prior written consent to GitHub subcontracting the processing of Personal Data to any Subprocessor on the Subprocessor List.

B. From time to time, GitHub may engage new Subprocessors. GitHub will give You notice of such engagements by updating the Subprocessor List and providing You with notice of that update (by the means set forth at https://gh.io/subscribe) 30 days before providing that Subprocessor with access to Customer Personal Data.

C. If You do not approve of a new Subprocessor, You may terminate any subscription for the affected Online Services without penalty by providing written notice of termination before the end of the relevant notice period. If the affected Online Service is part of a suite or purchased as part of a bundle, then any termination will apply to the entire suite or bundle.

D. GitHub is responsible for our Subprocessors' compliance with GitHub's obligations in this DPA, and will engage such Subprocessors by written agreements compliant with the requirements of the GDPR governing the use of Subprocessors. GitHub will oversee the Subprocessors to ensure that their contractual obligations are met.

10. CCPA. If and to the extent GitHub is processing Personal Data within the scope of the CCPA on Your behalf and in accordance with Your documented Instructions, GitHub will not:

A. sell the Personal Data as the term "selling" is defined in the CCPA;

B. share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, the Personal Data to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions for cross-context behavioral advertising in which no money is exchanged;

C. retain, use, or disclose the Personal Data for any purpose other than for the business purposes specified in this DPA and the GitHub Customer Agreement, or as otherwise permitted by the CCPA;

D. retain, use, or disclose the Personal Data outside of the direct business relationship with Customer; or

E. combine the Personal Data with personal information that it receives from or on behalf of a third party or collects from California residents, except that GitHub may combine Personal Data to perform any business purpose as permitted by the CCPA or any regulations adopted or issued under the CCPA.

11. Educational Institutions.

A. If You are an educational agency or institution subject to the regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), or similar state student or educational privacy laws (collectively "Educational Privacy Laws"), You shall not provide Personal Data covered by such Educational Privacy Laws to GitHub without obtaining GitHub's prior, written, and specific consent expressly reciting GitHub's agreement to accept Personal Data subject to an Educational Privacy Law, and entering into a separate agreement with GitHub governing the parties' rights and obligations with respect to the processing of such Personal Data by GitHub in connection with the Online Services.

B. Without waiver of the above, or limiting GitHub's remedies in the event of a breach of the above provision, if You breach the above provision by providing GitHub any Personal Data covered by FERPA without such a separate agreement, You agree and acknowledge that, for the purposes of this DPA, GitHub is a "school official" with "legitimate educational interests" in the Personal Data, as those terms have been defined under FERPA and its implementing regulations. You understand GitHub may possess limited or no contact information for Your students and students' parents. Consequently, You are responsible for obtaining any student or parental consent that may be required by applicable law for any end user's use of the Online Services and to convey notification on behalf of GitHub to students (or a student's legal guardian when required) of any judicial order or lawfully issued subpoena requiring the disclosure of Personal Data in GitHub's possession as may be required under applicable law.

12. **CJIS Customer Agreement, HIPAA Business Associate, Biometric Data.** Except with GitHub's prior, written, and specific consent, You shall not provide GitHub any Personal Data:
    - **A.** relating to criminal convictions and offenses or Personal Data collected or otherwise processed by Customer subject to or in connection with FBI Criminal Justice Information Services or the related Security Policy;
    - **B.** constituting protected health information governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) or by state health or medical privacy laws;
    - **C.** collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects; or
    - **D.** covered by state, federal, or foreign biometric privacy laws or otherwise constituting biometric information including information on an individual's physical, physiological, biological, or behavioral characteristics or information derived from such information that is used or intended to be used, singly or in combination with each other or with other information, to establish individual identity.
13. **Breach.** If You believe that GitHub is in breach of our obligations under this DPA, you must provide GitHub with notice of such breach and GitHub shall have 14 business days to cure any such breach.

14. **Notices.**
    - **A. Notices to GitHub.** You will provide notices to GitHub by:
        i. Contacting customer support, or using GitHub's Privacy web form located at https://support.github.com/contact/privacy, with a copy emailed to GitHub's Data Protection Officer at dpo@github.com and a copy mailed to:

            GitHub Privacy
            GitHub, Inc.
            88 Colin P. Kelly Jr. Street
            San Francisco, California 94107 USA

            or

        ii. The method provided for in Your GitHub Customer Agreement.
    - **B. Notices to You**. GitHub may provide notices to You by:
        i. The method provided for in Your GitHub Customer Agreement; or
        ii. Any means of notifying Your administrator(s), including email, that GitHub selects. It is Your obligation to maintain accurate contact information with

GitHub, and You will monitor any contact address provided to GitHub so that You can receive and respond to such Notices.

DPA Attachment 1
ANNEX I to the Standard Contractual Clauses (EU/EEA)

A. LIST OF PARTIES

MODULE ONE: CONTROLLER TO CONTROLLER
MODULE TWO: CONTROLLER TO PROCESSOR
MODULE THREE: PROCESSOR TO PROCESSOR

Data exporter(s) for the above modules:

Name and contact details: as set out in the Agreement.

Activities relevant to the data transferred under these Clauses: as set out in the Agreement.

Signature and date: Annex 1 is deemed to be executed on the date the transfer commenced or the date that the Agreement was executed, whichever is earlier.

Role: MODULE ONE: CONTROLLER, MODULE TWO: CONTROLLER, MODULE THREE: PROCESSOR

Data importer(s):

Name and contact details: as set out in the Agreement.

Activities relevant to the data transferred under these Clauses: as set out in the Agreement.

Signature and date: Annex 1 is deemed to be executed on the date the transfer commenced or the date that the Agreement was executed, whichever is earlier.

Role: MODULE ONE: CONTROLLER, MODULE TWO: PROCESSOR, MODULE THREE: (SUB)PROCESSOR

B. Description of Transfer

MODULE ONE: CONTROLLER TO CONTROLLER
MODULE TWO: CONTROLLER TO PROCESSOR
MODULE THREE: PROCESSOR TO PROCESSOR

Categories of data subjects whose personal data is transferred:

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal data to users of the services provided by data importer. GitHub acknowledges that, depending on Customer's use of the Online Service or Professional Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors, and temporary workers (current, former, prospective) of data exporter;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors, or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users and other data subjects that are users of data exporter's services;
- Partners, stakeholders, or individuals who actively collaborate, communicate, or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter.

Categories of personal data transferred:

The personal data transferred that is included in e-mail, documents, and other data in an electronic form in the context of the Online Services or Professional Services. GitHub acknowledges that, depending on Customer's use of the Online Service or Professional Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth);
- Authentication data (for example username, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Pseudonymous identifiers;
- Device identification (for example IMEI-number, SIM card number, MAC address); or
- Any other personal data identified in Article 4 of the GDPR.

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

GitHub does not request or otherwise ask for sensitive data and receives such data only if and when customers or data subjects decide to provide it.

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

Continuous as part of the Online Services or Professional Services.

Nature of the processing:

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

- Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the applicable GitHub Customer Agreement between data exporter and the data importer. The objective of the data processing is the performance of Online Services and Professional Services.
- Personal Data Access. For the term designated under the applicable GitHub Customer Agreement, data importer will, at its election and as necessary under applicable law, either: (1) provide data exporter with the ability to correct, delete, or block personal data, or (2) make such corrections, deletions, or blockages on its behalf.
- Data Exporter's Instructions. For Online Services and Professional Services, data importer will only act upon data exporter's instructions and the Agreement.

Purpose(s) of the data transfer and further processing:

The scope and purpose of processing personal data is described in DPA Sections 2 and 3 on Scope and Processing Roles. Processing may take place in any jurisdiction where data importer or its subprocessors operate such facilities in accordance with Section 7 on Data Transfers and Locations.

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

Upon expiration or termination of data exporter's use of Online Services or Professional Services, it may extract personal data and data importer will delete personal data, each in accordance with the DPA terms applicable to the agreement.

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

In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain personal data only to deliver the services the data importer has retained them to provide, and they are prohibited from using personal data for any other purpose. Unless a particular subcontractor is replaced ahead of time, the processing will be for the term designated under the applicable GitHub Customer Agreement between data exporter and data importer.

C. COMPETENT SUPERVISORY AUTHORITY
MODULE ONE: CONTROLLER TO CONTROLLER
MODULE TWO: CONTROLLER TO PROCESSOR
MODULE THREE: PROCESSOR TO PROCESSOR

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

DPA Attachment 2
Annex II to the Standard Contractual Clauses (EU/EEA)

MODULE ONE: CONTROLLER TO CONTROLLER
MODULE TWO: CONTROLLER TO PROCESSOR
MODULE THREE: PROCESSOR TO PROCESSOR

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons

1. Data Security Certifications. Data importer holds the following data security certifications as applicable:
    - SOC 1, Type 2;
    - SOC 2, Type 2; and,
    - ISO 27001:2013.
2. Personnel. Data importer's personnel will not process personal data without authorization. Personnel are obligated to maintain the confidentiality of any such personal data and this obligation continues even after their engagement ends.
3. Data Privacy Contact. The data privacy officer of the data importer can be reached at dpo@github.com and the following address: GitHub, Inc. Attn: Privacy, 88 Colin P. Kelly Jr. Street, San Francisco, California 94107 USA
4. Technical and Organization Measures. GitHub implements and maintains the technical and organizational measures and security safeguards listed in Table 1 below for processing Customer Personal Data on behalf and in accordance with Customer Instructions in connection with the Online Services. These measures in conjunction with the security commitments in this DPA are GitHub's only responsibility with respect to the security of that data.
5. Vendor management program - third-party risk program. The data importer has a vendor risk assessment process, vendor contract clauses and additional data protection agreements with vendors. Vendors undergo reassessment when a new business use case is requested. The data importer's vendor risk program is structured so all of data importer's vendors' risk assessments are refreshed two years from the last review date. Vendors deemed high risk, such as data center providers or other vendors storing or processing data in scope for the data importer's regulatory or contractual requirements, undergo reassessment annually.

Table 1: Technical and Organization Measures

Domain	Practices
Access Control	**Access Policy**. GitHub maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** ● GitHub maintains and updates a record of personnel authorized to access GitHub systems that contain Customer Data. ● GitHub identifies those personnel who may grant, alter or cancel authorized access to data and resources. ● GitHub ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins where technically and architecturally feasible, and commercially reasonable. **Least Privilege** ● Technical support personnel are only permitted to have access to Customer Data and Personal Data when needed. ● GitHub restricts access to Customer Data and Personal Data to only those individuals who require such access to perform their job function. GitHub employees are only granted access to production systems based on their role within the organization. **Integrity and Confidentiality** ● GitHub instructs GitHub personnel to disable administrative sessions when computers are left unattended. ● GitHub stores passwords such that they are encrypted or unintelligible while they are in force. **Authentication** ● GitHub uses industry standard practices to identify and authenticate users who attempt to access information systems. ● Where authentication mechanisms are based solely on passwords, GitHub requires the password to be at least eight characters long. ● GitHub ensures that de-activated or expired employee identifiers are not granted to other individuals. ● GitHub monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. ● GitHub maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. ● GitHub uses industry standard password protection practices, including practices designed to maintain the confidentiality and

Domain	Practices
	integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. GitHub has controls to ensure no systems storing Customer Data and Personal Data are part of the same logical network used for GitHub business operations.
Asset Management	**Asset Inventory.** GitHub maintains an inventory of all media on which Customer Personal Data is stored. Access to the inventories of such media is restricted to GitHub personnel authorized to have such access. **Asset Handling** ● GitHub classifies Customer Personal Data to help identify it and to allow for access to it to be appropriately restricted. ● GitHub communicates employee responsibility and accountability for data protection up to and including cause for termination. ● GitHub personnel must obtain GitHub authorization prior to remotely accessing Customer Personal Data or processing Customer Personal Data outside GitHub's facilities.
Business Continuity Management	● GitHub maintains emergency and contingency plans for the facilities in which GitHub information systems that process Customer Data and Personal Data are located. ● GitHub's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Personal Data in its original or last-replicated state from before the time it was lost or destroyed.
Communications and Operations Management	**Operational Policy.** GitHub maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Personal Data. **Data Recovery Procedures** ● On an ongoing basis, but in no case less frequently than once a week (unless no Customer Personal Data has been updated during that period), GitHub maintains multiple copies of Customer Personal Data from which Customer Personal Data can be recovered. ● GitHub stores copies of Customer Personal Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Personal Data is located.

Domain	Practices
	• GitHub has specific procedures in place governing access to copies of Customer Personal Data. • GitHub logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. GitHub has threat detection controls to help identify and respond to anomalous or suspicious access to Customer Personal Data, including malicious software originating from public networks. **Data Beyond Boundaries** • GitHub encrypts, or enables Customer to encrypt, Customer Personal Data that is transmitted over public networks. • GitHub restricts access to Customer Personal Data in media leaving its facilities. **Event Logging**. GitHub logs, or enables Customer to log, access and use of information systems containing Customer Personal Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Human Resources Security	**Security Training.** GitHub requires all new hires to complete security and privacy awareness training as part of initial on-boarding. Participation in annual training is required for all employees to provide a baseline for security and privacy basics.
Information Security Incident Management	**Incident Response Process** • GitHub maintains a record of security incidents with a description of the incidents, the time period, the consequences of the breach, the name of the reporter, and to whom the incident was reported, and details regarding the handling of the incident. • In the event that GitHub Security confirms or reasonably suspects that a GitHub.com customer is affected by a data breach, we will notify the customer without undue delay • GitHub tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring.** GitHub employs a wide range of continuous monitoring solutions for preventing, detecting, and mitigating attacks to the site.

Domain	Practices
Organization of Information Security	**Security Ownership**. GitHub has appointed one or more security officers responsible for coordinating and monitoring the security policies and procedures. **Security Roles and Responsibilities**. GitHub personnel with access to Customer Personal Data are subject to confidentiality obligations. **Risk Management Program.** GitHub performs an annual risk assessment. GitHub retains its security documents pursuant to its retention requirements after they are no longer in effect. **Vendor Management.** GitHub has a vendor risk assessment process, vendor contract clauses and additional data protection agreements with vendors.
Physical and Environmental Security	**Physical Access to Facilities.** GitHub limits access to facilities where information systems that process Customer Personal Data are located to identified authorized individuals. **Physical Access to Components**. GitHub maintains records of the incoming and outgoing media containing Customer Personal Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Personal Data they contain. **Protection from Disruptions.** GitHub uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal.** GitHub uses industry standard processes to delete Customer Personal Data when it is no longer needed.

DPA Attachment 3
ANNEX III– LIST OF SUB-PROCESSORS
to the
Standard Contractual Clauses (EU/EEA)

MODULE ONE: CONTROLLER TO CONTROLLER
MODULE TWO: CONTROLLER TO PROCESSOR
MODULE THREE: PROCESSOR TO PROCESSOR

The Parties rely on general authorization under Clause 9a of the Standard Contractual Clauses (EU/EEA). The list of Subprocessors can be found on the GitHub website at https://github.com/github-subprocessors-list

DPA Attachment 4
ANNEX IV to the Standard Contractual Clauses (EU/EEA)
Additional Safeguards Addendum

This Addendum to the Standard Contractual Clauses ("Addendum") by GitHub provides extra safeguards and redress for data subjects linked to Customer's personal data. It supplements but does not modify the Standard Contractual Clauses.

I. Challenges to Orders: If GitHub receives an order demanding disclosure of personal data transferred under the Standard Contractual Clauses, GitHub will:

a. Redirect the third party to request data from the Customer;
b. Inform the Customer unless legally prohibited, striving to waive this prohibition;
c. Challenge the disclosure order legally.

II. Indemnification of Data Subjects: GitHub shall indemnify a data subject for damages caused by GitHub's disclosure of their data in response to an order from a non-EU/EEA government body.

a. **No Obligation to Indemnify:**
    i. If the data subject has already received compensation for the same damage, GitHub has no obligation to indemnify.
    ii. If GitHub can prove the disclosure did not violate Chapter V of the GDPR, GitHub has no obligation to indemnify.
b. **Conditions of Indemnification:** Indemnification depends on the data subject proving that:
    i. GitHub disclosed the data;
    ii. This led to an official proceeding against them; and
    iii. The disclosure directly caused damage.
c. **Scope of Damages:** Indemnification covers only damages defined in the GDPR, excluding consequential and other damages not due to GitHub's GDPR infringement.

III. Exercise of Rights: Data subjects can enforce their rights under this Addendum against GitHub irrespective of any restrictions in the Standard Contractual Clauses. Claims must be individual, not part of a collective action, and are non-transferable.

IV. Notice of Change: GitHub warrants that the current legislation to which it is subject allows it to fulfill obligations under this Addendum and the Standard Contractual Clauses. If a legal change affecting these obligations occurs, GitHub will notify the Customer, who can then suspend data transfer or terminate the contract.

V. Termination: This Addendum ends if a different lawful transfer mechanism is approved that covers the data transfers of the Standard Contractual Clauses, and doesn't require these additional safeguards.