



GitHub

Data Protection Agreement

Version May, 2022

Table of Contents

<u>INTRODUCTION</u>	3
Applicable DPA Terms and Updates	3
Electronic Notices	3
Prior Versions	3
<u>DEFINITIONS</u>	3
<u>GENERAL TERMS</u>	6
Compliance with Laws	6
<u>DATA PROTECTION TERMS</u>	6
Scope	6
Nature of Data Processing; Ownership	6
Disclosure of Processed Data	7
Processing of Personal Data; GDPR	7
Data Security	8
Security Incident Notification	9
Data Transfers and Location	9
Data Retention and Deletion	9
Processor Confidentiality Commitment	10
Notice and Controls on use of Subprocessors	10
Educational Institutions	10
CJIS Customer Agreement, HIPAA Business Associate, Biometric Data	10
California Consumer Privacy Act (CCPA)	11
How to Contact GitHub	11
<u>APPENDIX A – SECURITY SAFEGUARDS</u>	12
<u>ATTACHMENT 1 – THE STANDARD CONTRACTUAL CLAUSES (EU/EEA)</u>	15
<u>ATTACHMENT 2 – THE STANDARD CONTRACTUAL CLAUSES (UK)</u>	
<u>ATTACHMENT 3 – EUROPEAN UNION GENERAL DATA PROTECTION REGULATION TERMS</u>	22

Introduction

The parties agree that this GitHub Data Protection Agreement (“**DPA**”) sets forth their obligations with respect to the processing and security of Personal Data and, where explicitly stated in the DPA Terms, Customer Data in connection with the Online Services provided by GitHub, Inc. (“**GitHub**”). The DPA (including its Appendix and Attachments) is between GitHub and any customer receiving Online Services from GitHub based on the GitHub Customer Agreement (“**Customer**”), and is incorporated by reference into the GitHub Customer Agreement.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in the GitHub Customer Agreement, the DPA Terms will prevail. The provisions of the DPA Terms supersede any conflicting provisions of the GitHub Privacy Statement that otherwise may apply to processing of Personal Data. For clarity, the Standard Contractual Clauses prevail over any other term of the DPA Terms.

Applicable DPA Terms and Updates

Limits on Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current DPA Terms will apply and will not change during the term of that new subscription for that Online Service.

New Features, Supplements, or Related Software

Notwithstanding the foregoing limits on updates, when GitHub introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), GitHub may provide terms or make updates to the DPA that apply to Customer’s use of those new features, supplements or related software. If those terms include any material adverse changes to the DPA Terms, GitHub will provide Customer a choice to use the new features, supplements, or related software, without loss of existing functionality of a generally available Online Service. If Customer does not use the new features, supplements, or related software, the corresponding new terms will not apply.

Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, GitHub may modify or terminate an Online Service in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects GitHub to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for GitHub to continue operating the Online Service without modification, and/or (3) causes GitHub to believe the DPA Terms or the Online Service may conflict with any such requirement or obligation.

Electronic Notices

GitHub may provide Customer with information and notices about Online Services electronically, including via email, or through a web site that GitHub identifies. Notice is given as of the date it is made available by GitHub.

Prior Versions

The DPA Terms provide terms for Online Services that are currently available. For earlier versions of the DPA Terms, Customer may contact its reseller or GitHub Account Manager.

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the GitHub Customer Agreement. The following defined terms are used in this DPA:

“**CCPA**” means the California Consumer Privacy Act as set forth in Cal. Civ. Code §1798.100 et seq. and its implementing regulations.

“**Customer 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 Service.

“**Data Protection Requirements**” means the GDPR, Local EU/EEA Data Protection Laws, CCPA, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

“**Diagnostic Data**” means data collected or obtained by GitHub from software that is locally installed by Customer in connection with the Online Service. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data, Service Generated Data, or Professional Services Data.

“**DPA Terms**” means both the terms in this DPA and any Online Service-specific terms in the GitHub Customer Agreement that specifically supplement or modify the privacy and security terms in this DPA for a specific Online Service (or feature of an Online Service). In the event of any conflict or inconsistency between the DPA and such Online Service-specific terms, the Online Service-specific terms shall prevail as to the applicable Online Service (or feature of that Online Service).

“GDPR” means 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, and repealing Directive 95/46/EC (General Data Protection Regulation). In connection with the United Kingdom, “GDPR” means 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).

“Local EU/EEA Data Protection Laws” means any subordinate legislation and regulation implementing the GDPR.

“GDPR Related Terms” means the terms in [Attachment 3](#), under which GitHub makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

“GitHub Affiliate” means any entity that directly or indirectly controls, is controlled by or is under common control with GitHub.

“GitHub Customer Agreement” means the service or other agreement(s) entered into by Customer with GitHub for Online Services.

“GitHub Privacy Statement” means the GitHub privacy statement available at <https://docs.github.com/en/github/site-policy/github-privacy-statement>.

“Online Service” means any service or software provided by GitHub to Customer under the GitHub Customer Agreement agreed upon with Customer, including Previews, updates, patches, bug fixes, and technical support.

“Personal Data” means any information relating to 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.

“Preview” means Online Services provided for preview, evaluation, demonstration or trial purposes, or pre-release versions of the Online Services.

“Professional Services Data” means all data, including all text, sound, video, image files or software, 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. Professional Services Data includes Support Data.

“Service Generated Data” means data generated or derived by GitHub through the operation of an Online Service. Service Generated Data does not include Customer Data, Diagnostic Data, or Professional Services Data.

“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 the section of this DPA entitled “Data Transfers and Location” below:

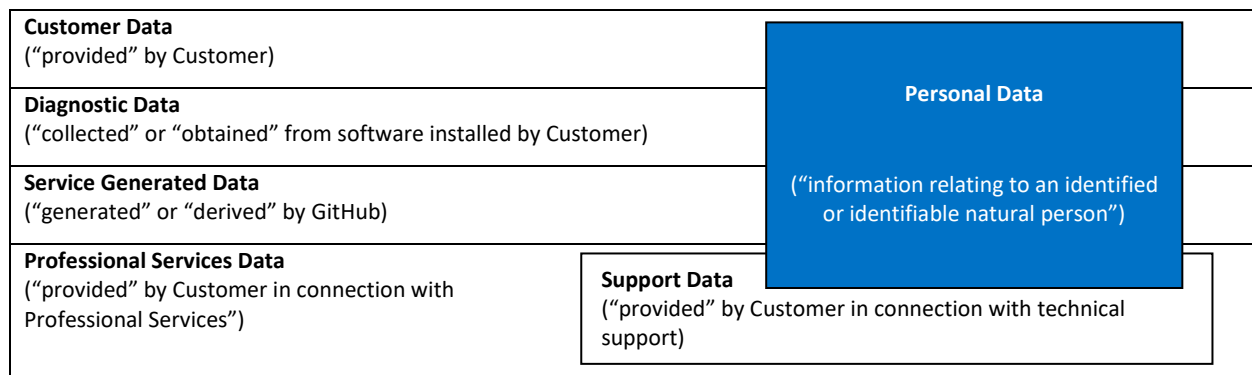
- the Standard Contractual Clauses (MODULE TWO: Transfer controller to processor), dated 4 June 2021, for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as described in Article 46 of the GDPR and approved by European Commission Implementing Decision (EU) 2021/91 (“**Standard Contractual Clauses (EU/EEA)**”) and adopted by the Switzerland Federal Data Protection and Information Commissioner (“Swiss FDPIC”). The Standard Contractual Clauses (EU/EEA) are set forth in [Attachment 1](#).
- the International Data Transfer Addendum to the Standard Contractual Clauses (EU/EEA) as adopted by the United Kingdom Information Commissioner’s Office (“UK ICO”) 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](#).

“Subprocessor” means other processors used by GitHub to process Personal Data on behalf of Customer in connection with the Online Services, as described in Article 28 of the GDPR.

“Support Data” means all data, including all text, sound, video, image files, or software, that are provided to GitHub by or on behalf of Customer (or that Customer authorizes GitHub to obtain from an Online Service) through an engagement with GitHub to obtain technical support for Online Services covered under this agreement. Support Data is a subset of Professional Services Data.

Lower case terms used but not defined in this DPA, such as “personal data breach”, “processing”, “controller”, “processor”, “profiling”, “personal data”, and “data subject” will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms “data importer” and “data exporter” have the meanings given in the Standard Contractual Clauses.

For clarity, and as detailed above, data defined as Customer Data, Diagnostic Data, Service Generated Data, and Professional Services Data may contain Personal Data. For illustrative purposes, please see the chart inserted below:



Above is a visual representation of the data types defined in the DPA. All Personal Data is processed as a part of one of the other data types (all of which also include non-personal data). Support Data is a sub-set of Professional Services Data. Except where explicitly stated otherwise, the DPA Terms exclusively apply to Personal Data.

[Table of Contents](#) / [General Terms](#)

General Terms

Compliance with Laws

GitHub will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law and Data Protection Requirements. However, GitHub is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. GitHub does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Online Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of an Online Service, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Data Processing; Ownership
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
- Data Security
- Security Incident Notification
- Data Transfers and Location
- Data Retention and Deletion
- Processor Confidentiality Commitment
- Notice and Controls on Use of Subprocessors
- Educational Institutions
- CJIS Customer Agreement, HIPAA Business Associate, Biometric Data
- California Consumer Privacy Act (CCPA)
- How to Contact GitHub
- Appendix A – Security Measures

Scope

The DPA Terms apply to all Online Services.

Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. The following terms in this DPA do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and California Consumer Privacy Act.

Nature of Data Processing; Ownership

Except as otherwise stated in the DPA Terms, GitHub will use and otherwise process Customer Data and Personal Data as described and subject to the limitations provided below (a) to provide Customer the Online Service in accordance with Customer's documented instructions, and/or (b) for GitHub's legitimate business operations incident to delivery of the Online Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data. GitHub acquires no rights in Customer Data other than the rights Customer grants to GitHub in this section. This paragraph does not affect GitHub's rights in software or services GitHub licenses to Customer.

Processing to Provide Customer the Online Services

For purposes of this DPA, "to provide" an Online Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (e.g., preventing, detecting, and repairing problems); and
- Ongoing improvement (e.g., installing the latest updates and making improvements to user productivity, reliability, efficacy, and security).

When providing Online Services, GitHub will use or otherwise process Personal Data only on Customer's behalf and in accordance with Customer's documented instructions.

Processing for GitHub's Legitimate Business Operations

For purposes of this DPA, "GitHub's legitimate business operations" consist of the following, each as incident to delivery of the Online Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, abuse, cybercrime, or cyber-attacks that may affect GitHub or Online Services; (5) improving the core functionality of accessibility, privacy or energy-efficiency; (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below); (7) the creation or management of end user accounts and profiles by GitHub for individual users of Customer (except where Customer creates, manages

or otherwise controls such end user accounts or profiles itself); and (8) other purposes pertaining to Personal Data not provided by Customer for storage in GitHub repositories or in connection with Professional Services.

When processing for GitHub's legitimate business operations, GitHub will not use or otherwise process 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.

Disclosure of Processed Data

GitHub will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Personal Data and (c) any other data processed by GitHub in connection with the Online Service that is Customer's confidential information under the GitHub Customer Agreement. All processing of Processed Data is subject to GitHub's obligation of confidentiality under the GitHub Customer Agreement.

GitHub will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts GitHub with a demand for Processed Data, GitHub will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, GitHub will promptly notify Customer and provide a copy of the demand, unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, GitHub will promptly notify Customer unless prohibited by law. GitHub will reject the request unless required by law to comply. If the request is valid, GitHub will attempt to redirect the third party to request the data directly from Customer.

GitHub will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if GitHub is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, GitHub may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR

All Personal Data processed by GitHub in connection with the Online Services is obtained as part of either Customer Data, Professional Services Data (including Support Data), Diagnostic Data, or Service Generated Data. Personal Data provided to GitHub by, or on behalf of, Customer through use of the Online Service is also Customer Data. Pseudonymized identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent GitHub is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Related Terms in [Attachment 3](#) govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and GitHub agree that Customer is the controller of Personal Data and GitHub is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case GitHub is a subprocessor; or (b) as stated otherwise in the GitHub Customer Agreement or this DPA. When GitHub acts as the processor or subprocessor of Personal Data, it will process Personal Data only on Customer's behalf and in accordance with documented instructions from Customer. Customer agrees that its GitHub Customer Agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer's use and configuration of features in the Online Services, are Customer's complete documented instructions to GitHub for the processing of Personal Data. Information on use and configuration of the Online Services can be found at <https://docs.github.com> or a successor location. Any additional or alternate instructions must be agreed to according to the process for amending Customer's GitHub Customer Agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to GitHub that Customer's instructions, including appointment of GitHub as a processor or subprocessor, have been authorized by the relevant controller.

To the extent GitHub uses or otherwise processes Personal Data subject to the GDPR for GitHub's legitimate business operations incident to delivery of the Online Services to Customer, GitHub will comply with the obligations of an independent data controller under GDPR for such use. GitHub is accepting the added responsibilities of a data "controller" under the GDPR for processing in connection with its legitimate business operations to: (a) act consistent with regulatory requirements, to the extent required under the GDPR; and (b) provide increased transparency to Customers and confirm GitHub's accountability for such processing. GitHub employs safeguards to protect Personal Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of Personal Data under this paragraph, GitHub makes the commitments set forth in the Standard Contractual Clauses set forth in [Attachment 1](#) or [Attachment 2](#) (as applicable); for those purposes, (i) any GitHub disclosure of Personal Data, as described in Annex IV to [Attachment 1](#), that has been transferred in connection with GitHub's legitimate business operations is deemed a "Relevant Disclosure" and (ii) the commitments in Annex IV to [Attachment 1](#) apply to such Personal Data.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled “Nature of Data Processing; Ownership” above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Online Service pursuant to Customer’s GitHub Customer Agreement and for GitHub’s legitimate business operations incident to delivery of the Online Service to Customer (as further described in the section of this DPA entitled “Nature of Data Processing; Ownership” above).
- **Categories of Data.** The types of Personal Data processed by GitHub when providing the Online Service include: (i) Personal Data that Customer elects to include in Customer Data or Professional Services Data (including, without limitation, Support Data); and (ii) those expressly identified in Article 4 of the GDPR that may be contained in Diagnostic Data or Service Generated Data. The types of Personal Data that Customer elects to include in Customer Data or Professional Services Data (including, without limitation, Support Data) may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Annex I [to Attachment 1](#).
- **Data Subjects.** The categories of data subjects are Customer’s representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Annex I [to Attachment 1](#).

Data Subject Rights; Assistance with Requests

GitHub will make available to Customer, in a manner consistent with the functionality of the Online Service and GitHub’s role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If GitHub receives a request from Customer’s data subject to exercise one or more of its rights under the GDPR in connection with an Online Service for which GitHub is a data processor or subprocessor, GitHub will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Online Service. GitHub shall comply with reasonable requests by Customer to assist with Customer’s response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires GitHub to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to GitHub and keep it accurate and up-to-date. GitHub may make any such information available to the supervisory authority if required by the GDPR.

Data Security

GitHub will implement and maintain appropriate technical and organizational measures and security safeguards against accidental or unlawful destruction, or loss, alteration, unauthorized disclosure of or access to, Customer Data and Personal Data processed by GitHub on behalf and in accordance with the documented instructions of Customer in connection with the Online Services. GitHub will regularly monitor compliance with these measures and safeguards and will continue to take appropriate steps throughout the term of the GitHub Customer Agreement. [Appendix A – Security Safeguards](#) contains a description of the technical and organizational measures and security safeguards implemented by GitHub.

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures and security safeguards for an Online Service meet Customer’s requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Customer Data and Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons) the technical and organizational measures and security safeguards implemented and maintained by GitHub provide a level of security appropriate to the risk with respect to its Customer Data and Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls.

GitHub will provide security compliance reporting such as external SOC1, type 2 and SOC2, type2 audit reports upon Customer request. Customer agrees that any information and audit rights granted by the applicable Data Protection Requirements (including, where applicable, Article 28(3)(h) of the GDPR) will be satisfied by these compliance reports, and will otherwise only arise to the extent that GitHub’s provision of a compliance report does not provide sufficient information, or to the extent that Customer must respond to a regulatory or supervisory authority audit or investigation.

Should Customer be subject to a regulatory or supervisory authority audit or investigation or carry out an audit or investigation in response to a request by a regulatory or supervisory authority that requires participation from GitHub, and Customers’ obligations cannot reasonably be satisfied (where allowable by Customer’s regulators) through audit reports, documentation, or compliance information that GitHub makes generally available to its customers, then GitHub will promptly respond to Customer’s additional instructions and requests for information, in accordance with the following terms and conditions:

- GitHub will provide access to relevant knowledgeable personnel, documentation, and application software.

- Customer and GitHub will mutually agree in a prior written agreement (email is acceptable) upon the scope, timing, duration, control and evidence requirements, provided that this requirement to agree will not permit GitHub to unreasonably delay its cooperation.
- Customer must ensure its regulator's use of an independent, accredited third-party audit firm, during regular business hours, with reasonable advance written notice to GitHub, and subject to reasonable confidentiality procedures. Neither Customer, its regulators, nor its 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.
- Customer is responsible for all costs and fees related to GitHub's cooperation with the regulatory audit of Customer, including all reasonable costs and fees for any and all time GitHub expends, in addition to the rates for services performed by GitHub.
- If the report generated from GitHub's cooperation with the regulatory audit of Customer includes any findings pertaining to GitHub, Customer will share such report, findings, and recommended actions with GitHub where allowed by Customer's regulators.

Security Incident Notification

If GitHub becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data processed by GitHub on behalf and in accordance with the documented instructions of Customer in connection with the Online Services (each a "**Security Incident**"), GitHub will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means GitHub selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information with GitHub and that Customer's administrators monitor for and respond to any notifications. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

GitHub will make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulations to notify the relevant regulatory or supervisory authority and individual data subjects about a Security Incident.

GitHub's notification of or response to a Security Incident under this section is not an acknowledgement by GitHub of any fault or liability with respect to the Security Incident.

Customer must notify GitHub promptly about any possible misuse of its accounts or authentication credentials or any Security Incident related to an Online Service.

Data Transfers and Location

Personal Data that GitHub processes on behalf and in accordance with the documented instructions of Customer in connection with the Online Services may not be transferred to, or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints GitHub to transfer Personal Data to the United States or any other country in which GitHub or its Subprocessors operate and to store and process Personal Data to provide the Online Services, except as may be described elsewhere in these DPA Terms.

All transfers of Personal Data out of the European Union, European Economic Area, or Switzerland to provide the Online Services shall be governed by the Standard Contractual Clauses (EU/EEA) in [Attachment 1](#). All transfers of Personal Data out of the United Kingdom to provide the Online Services shall be governed by the Standard Contractual Clauses (UK) in [Attachment 2](#). For the purposes of the Data Protection Law of Switzerland, Standard Contractual Clauses (EU/EEA) in [Attachment 1](#), shall be interpreted as follows:

- i. references to the "European Union," "EU," "European Economic Area," "EEA" or a "Member State" shall be interpreted to refer to "Switzerland"
- ii. references to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the "Data Protection Law of Switzerland".
- iii. References to "supervisory authority" shall be interpreted to refer to the "Swiss FDPIC".

GitHub will abide by the requirements of applicable European Union, European Economic Area, United Kingdom and Swiss data protection law, and other Data Protection Requirements, in each case regarding the transfer of Personal Data to recipients or jurisdictions outside such jurisdiction. All such transfers of Personal Data will, where applicable, be 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.

Subject to the safeguards described above, GitHub may transfer, store and otherwise process Personal Data to or in jurisdictions and geographic locations worldwide as it, subject to its sole discretion, considers reasonably necessary in connection with the Online Services.

Data Retention and Deletion

Upon Customer's reasonable request, unless prohibited by law, GitHub will return or destroy all Customer Data and Personal Data processed by GitHub on behalf and in accordance with the documented instructions of Customer in connection with the Online Services at all locations where it is stored within 30 days of the request, provided that it is no longer needed for providing the Online Services or the purposes for which a data subject

had authorized the processing of their Personal Data. GitHub may retain Customer Data or Personal Data to the extent required by the applicable Data Protection Requirements or other applicable law, and only to the extent and for such period as required by the applicable Data Protection Requirements or other applicable law, provided that GitHub will ensure that the Customer Data or Personal Data is processed only as necessary for the purpose specified in the applicable Data Protection Requirements or other applicable law and no other purpose, and the Customer Data or Personal Data remains protected by the Applicable Data Protection Requirements or other applicable law.

Processor Confidentiality Commitment

GitHub will ensure that its personnel engaged in the processing of Customer Data and Personal Data on behalf of Customer in connection with the Online Services (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. GitHub shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data and Personal Data in accordance with applicable Data Protection Requirements or other applicable law and industry standards.

Notice and Controls on Use of Subprocessors

GitHub may hire Subprocessors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to GitHub Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by GitHub of the processing of Personal Data if such consent is required under applicable law, the Standard Contractual Clauses or the GDPR Related Terms.

GitHub is responsible for its Subprocessors' compliance with GitHub's obligations in this DPA. GitHub makes available information about Subprocessors on the GitHub website <https://github.com/subprocessors> (or a successor location). When engaging any Subprocessor, GitHub will ensure via a written contract that the Subprocessor may access and use Customer Data or Personal Data only to deliver the services GitHub has retained them to provide and is prohibited from using Customer Data or Personal Data for any other purpose. GitHub will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of GitHub by the DPA, including the limitations on disclosure of Personal Data. GitHub agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, GitHub may engage new Subprocessors. GitHub will give Customer notice (by updating the website at <https://github.com/github-subprocessors-list> (or a successor location) and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor in advance of providing that Subprocessor with access to Customer Data. If GitHub engages a new Subprocessor for a new Online Service, GitHub will give Customer notice prior to availability of that Online Service.

If Customer does not approve of a new Subprocessor, then Customer may terminate any subscription for the affected Online Service without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit GitHub to re-evaluate any such new Subprocessor based on the applicable concerns. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, GitHub will remove payment obligations for any subscriptions for the terminated Online Service from subsequent invoices to Customer or its reseller.

Educational Institutions

If Customer is 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**"), Customer shall not provide Personal Data covered by such Educational Privacy Laws to GitHub without obtaining GitHub's prior, written and specific consent 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.

Subject to the above, if Customer intends to provide to GitHub Personal Data covered by FERPA, the parties 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. Customer understands that GitHub may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any student or parental consent for any end user's use of the Online Services that may be required by applicable law and to convey notification on behalf of GitHub to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) 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.

CJIS Customer Agreement, HIPAA Business Associate, Biometric Data

Except with GitHub's prior, written and specific consent, Customer shall not provide to GitHub any Personal Data

- 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.
- 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.

- 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 (Common Rule).
- 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.

California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

If and to the extent GitHub is processing Personal Data on behalf and in accordance with the documented instructions of Customer within the scope of the CCPA, GitHub makes the following additional commitments to Customer. GitHub will process the Personal Data on behalf of Customer and will not

- sell the Personal Data as the term "selling" is defined in the CCPA.
- 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.
- retain, use or disclose the Personal Data for any purpose other than for the business purposes specified in the DPA Terms and the GitHub Customer Agreement, including retaining, using or disclosing the Personal Data for a commercial purpose other than the business purposes specified in the DPA Terms or the GitHub Customer Agreement, or as otherwise permitted by the CCPA.
- retain, use or disclose the Personal Data outside of the direct business relationship with Customer.
- 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.

How to Contact GitHub

If Customer believes that GitHub is not adhering to its privacy or security commitments, Customer may contact customer support or use GitHub's Privacy web form, located at <https://support.github.com/contact/privacy>. GitHub's mailing address is:

GitHub Privacy

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

GitHub B.V. is GitHub's data protection representative for the European Economic Area. The privacy representative of GitHub B.V. can be reached at the following address:

GitHub B.V.

Vijzelstraat 68-72
1017 HL Amsterdam
The Netherlands

Appendix A – Security Safeguards

GitHub has implemented and will maintain for Customer Data and Personal Data processed by GitHub on behalf and in accordance with the documented instructions of Customer in connection with GitHub services the following technical and organizational measures and security safeguards, which in conjunction with the security commitments in this DPA (including the GDPR Related Terms), are GitHub’s only responsibility with respect to the security of that data:

Domain	Practices
Organization of Information Security	<p>Security Ownership. GitHub has appointed one or more security officers responsible for coordinating and monitoring the security policies and procedures.</p> <p>Security Roles and Responsibilities. GitHub personnel with access to Customer Data and Personal Data are subject to confidentiality obligations.</p> <p>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.</p> <p>Vendor Management. GitHub has a vendor risk assessment process, vendor contract clauses and additional data protection agreements with vendors.</p>
Asset Management	<p>Asset Inventory. GitHub maintains an inventory of all media on which Customer Data and Personal Data is stored. Access to the inventories of such media is restricted to GitHub personnel authorized to have such access.</p> <p>Asset Handling</p> <ul style="list-style-type: none"> • GitHub classifies Customer Data and 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 Data and Personal Data or processing Customer Data and Personal Data outside GitHub’s facilities.
Human Resources Security	<p>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.</p>
Physical and Environmental Security	<p>Physical Access to Facilities. GitHub limits access to facilities where information systems that process Customer Data and Personal Data are located to identified authorized individuals.</p> <p>Physical Access to Components. GitHub maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data and Personal Data they contain.</p> <p>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.</p> <p>Component Disposal. GitHub uses industry standard processes to delete Customer Data and Personal Data when it is no longer needed.</p>

<p>Communications and Operations Management</p>	<p>Operational Policy. GitHub maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.</p> <p>Data Recovery Procedures</p> <ul style="list-style-type: none"> • On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data and Personal Data has been updated during that period), GitHub maintains multiple copies of Customer Data and Personal Data from which Customer Data and Personal Data can be recovered. • GitHub stores copies of Customer Data and Personal Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Personal Data is located. • GitHub has specific procedures in place governing access to copies of Customer 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. <p>Malicious Software. GitHub has threat detection controls to help identify and respond to anomalous or suspicious access to Customer Data, including malicious software originating from public networks.</p> <p>Data Beyond Boundaries</p> <ul style="list-style-type: none"> • GitHub encrypts, or enables Customer to encrypt, Customer Data and Personal Data that is transmitted over public networks. • GitHub restricts access to Customer Data and Personal Data in media leaving its facilities. <p>Event Logging. GitHub logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.</p>
---	---

Access Control	<p>Access Policy. GitHub maintains a record of security privileges of individuals having access to Customer Data.</p> <p>Access Authorization</p> <ul style="list-style-type: none"> • 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. <p>Least Privilege</p> <ul style="list-style-type: none"> • 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. <p>Integrity and Confidentiality</p> <ul style="list-style-type: none"> • 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. <p>Authentication</p> <ul style="list-style-type: none"> • 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 integrity of passwords when they are assigned and distributed, and during storage. <p>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.</p>
Information Security Incident Management	<p>Incident Response Process</p> <ul style="list-style-type: none"> • 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. <p>Service Monitoring. GitHub employs a wide range of continuous monitoring solutions for preventing, detecting, and mitigating attacks to the site.</p>

Business Continuity Management	<ul style="list-style-type: none">• 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.
--------------------------------	--

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

Controller to Processor

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.
- (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.

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.

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 90 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 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.

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

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.
- (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

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.

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)

A. LIST OF PARTIES

Data exporter(s): Customer is the data exporter

Name: see GitHub Customer Agreement

Address: see GitHub Customer Agreement

Contact person's name, position and contact details: see GitHub Customer Agreement

Activities relevant to the data transferred under these Clauses:

The data exporter is a user of Online Services or Professional Services as defined in the DPA and GitHub Customer Agreement.

Signature and date: see GitHub Customer Agreement (the DPA and the Standard Contractual Clauses (EU/EEA) are incorporated into the GitHub Customer Agreement)

Role (controller/processor): controller (unless otherwise agreed in the Customer Agreement).

Data importer(s):

Name: GitHub, Inc.

Address: 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA

Contact person's name, position and contact details: Frances Wiet, Head of Privacy, fwiet@github.com

Activities relevant to the data transferred under these Clauses:

GitHub, Inc. is a global producer of software and services

Signature and date: see GitHub Customer Agreement (the DPA and the Standard Contractual Clauses (EU/EEA) are incorporated into the GitHub Customer Agreement)

Role (controller/processor): processor or, depending on the agreements set forth in the Customer Agreement, subprocessor.

B. DESCRIPTION OF TRANSFER

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 user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example IP addresses, employee number, student number);
- Pseudonymous identifiers;
- Photos, video and audio;
- Internet activity (for example browsing history, search history, reading and viewing activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);

- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- Special categories of data as voluntarily provided by data subjects (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); 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.

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

The scope and purpose of processing personal data is described in the “Processing of Personal Data; GDPR” section of the DPA. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities in accordance with the “Security Practices and Policies” section of the DPA.

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

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

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

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

**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:
 - SOC 1, Type 2;
 - SOC 2, Type 2;
 - NIST, to the extent incorporated for FedRAMP Low-Impact / Tailored ATO.
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 the following address:

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

4. Technical and Organization Measures. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect personal data, as defined in the Security Practices and Policies section of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the Data Security section of the DPA are hereby incorporated into this Annex II to Attachment 1 by this reference and are binding on the data importer as if they were set forth in this Annex 2 to Attachment 1 in their entirety.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

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.

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

MODULE TWO: Transfer controller 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>

ANNEX IV to the Standard Contractual Clauses (EU/EEA)

Additional Safeguards Addendum

By this Additional Safeguards Addendum to Standard Contractual Clauses (EU/EEA) (this “Addendum”), GitHub, Inc. (“GitHub”) provides additional safeguards to Customer and additional redress to the data subjects to whom Customer’s personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses (EU/EEA).

1. Challenges to Orders. In addition to Clause 15.1 of the Standard Contractual Clauses (EU/EEA), in the event GitHub receives an order from any third party for compelled disclosure of any personal data that has been transferred under the Standard Contractual Clauses (EU/EEA), GitHub shall:

- a. use every reasonable effort to redirect the third party to request data directly from Customer;
- b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and
- c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable Member State law.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. Indemnification of Data Subjects. Subject to Sections 3 and 4, GitHub shall indemnify a data subject for any material or non-material damage to the data subject caused by GitHub’s disclosure of personal data of the data subject that has been transferred under the Standard Contractual Clauses (EU/EEA) in response to an order from a non-EU/EEA government body or law enforcement agency (a “Relevant Disclosure”). Notwithstanding the foregoing, GitHub shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from GitHub or otherwise.

3. Conditions of Indemnification. Indemnification under Section 2 is conditional upon the data subject establishing, to GitHub’s reasonable satisfaction, that:

- a. GitHub engaged in a Relevant Disclosure;
- b. the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and
- c. the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. through c.

Notwithstanding the foregoing, GitHub shall have no obligation to indemnify the data subject under Section 2 if GitHub establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

4. Scope of Damages. Indemnification under Section 2 is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from GitHub’s infringement of the GDPR.

5. Exercise of Rights. Rights granted to data subjects under this Addendum may be enforced by the data subject against GitHub irrespective of any restriction in Clauses 3 or 12 of the Standard Contractual Clauses (EU/EEA). The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.

6. Notice of Change. In addition to Clause 14 of the Standard Contractual Clauses (EU/EEA), GitHub agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the data exporter and its obligations under this Addendum or the Standard Contractual Clauses (EU/EEA) 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 this Addendum or the Standard Contractual Clauses (EU/EEA), it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

7. Termination. This Addendum shall automatically terminate if the European Commission, a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the data transfers covered by the

Standard Contractual Clauses (EU/EEA) (and if such mechanism applies only to some of the data transfers, this Addendum will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Addendum.

Attachment 2 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Table 1: Parties

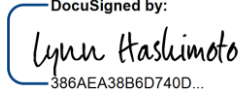
Start date	As indicated in the applicable GitHub Customer Agreement.	
The Parties	Exporter (who sends the Restricted Transfer) Customer as indicated in the applicable GitHub Customer Agreement	Importer (who receives the Restricted Transfer) GitHub, Inc.
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier): <u>Exporter details as included in Annex I to Attachment 1 of this Addendum.</u>	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier): <u>Importer details as included in Annex I to the Attachment 1 of this Addendum.</u>
Key Contact	Full Name (optional): Job Title: Contact details including email: <u>Exporter details as included in Annex I to Attachment 1 of this Addendum.</u>	Full Name (optional): Job Title: Contact details including email: <u>Importer details as included in Annex I to the Attachment 1 of this Addendum.</u>
Signature (if required for the purposes of Section 2)	Execution of the GitHub Customer Agreement by Customer includes execution of this Attachment 2, which is countersigned by GitHub, Inc.	DocuSigned by:  386AEA38B6D740D... Lynn Hashimoto Head of Product and Regulatory Legal GitHub, Inc. 88 Colin P. Kelly Jr. Street, San Francisco, California 94107 USA

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		<input checked="" type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	Module Two (Controller to Processor)	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 1.A	Optional language in Clause 11 shall not apply.	General Authorization	30 days	N/A

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As described in Annex I to the Schedule 3 of this Addendum.

Annex 1B: Description of Transfer: As described in Annex I to the Schedule 3 of this Addendum.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described in Annex II to the Schedule 3 of this Addendum.

Annex III: List of Sub processors (Modules 2 and 3 only): List of Subprocessors can be found at <https://github.com/github-subprocessors-list>

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer
---	---

	<input checked="checked" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	---

Part 2: Mandatory Clauses

Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

- Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

“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”;

c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
 - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
 - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
 - a its direct costs of performing its obligations under the Addendum; and/or
 - b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
--------------------------	---

Attachment 3 – European Union General Data Protection Regulation Terms

GitHub makes the commitments in these GDPR Related Terms, to all customers effective May 25, 2018. These commitments are binding upon GitHub with regard to Customer regardless of (1) the version of the GitHub Customer Agreement and DPA that is otherwise applicable to any given Online Services subscription or (2) any other agreement that references this attachment.

For purposes of these GDPR Related Terms, Customer and GitHub agree that Customer is the controller of Personal Data and GitHub is the processor of such data, except when Customer acts as a processor of Personal Data, in which case GitHub is a subprocessor. These GDPR Related Terms apply to the processing of Personal Data, within the scope of the GDPR, by GitHub on behalf of Customer. These GDPR Related Terms do not limit or reduce

any data protection commitments GitHub makes to Customer in the GitHub Customer Agreement or other agreement between GitHub and Customer. These GDPR Related Terms do not apply where GitHub is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. GitHub shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, GitHub shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))

2. Processing by GitHub shall be governed by these GDPR Related Terms under European Union (hereafter “Union”) or Member State law and are binding on GitHub with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer’s licensing agreement, including these GDPR Related Terms. In particular, GitHub shall:

- (a) process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which GitHub is subject; in such a case, GitHub shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- (b) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) take all measures required pursuant to Article 32 of the GDPR;
- (d) respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;
- (e) taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer’s obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
- (f) assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to GitHub;
- (g) at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;
- (h) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

GitHub shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

3. Where GitHub engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Related Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, GitHub shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

4. 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, Customer and GitHub shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia 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 organisational measures for ensuring the security of the processing. (Article 32(1))

5. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed (Article 32(2)).

6. Customer and GitHub shall take steps to ensure that any natural person acting under the authority of Customer or GitHub who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law (Article 32(4)).

7. GitHub shall notify Customer without undue delay after becoming aware of a Personal Data breach (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to GitHub.