GitLab Data Processing Addendum

The terms of this Data Processing Addendum ("**DPA**") supplement the Subscription Agreement where Customer is entering into the Subscription Agreement on behalf of an Enterprise. Customer's acceptance of the Subscription Agreement shall be treated as its execution of this DPA and, where applicable, the Standard Contractual Clauses.

The parties agree that this DPA sets forth both parties' obligation with respect to the processing and security of Personal Data, to the extent GitLab processes such Personal Data. The parties hereby enter into this DPA in order to comply with the obligations under Applicable Data Protection Laws (as defined below).

1. **Definitions**. The capitalized terms will have the meanings set forth below:

   a. "**Applicable Data Protection Laws**" means any applicable laws, statutes or regulations as may be amended, extended, re-enacted from time to time, or any successor laws which relate to Personal Data including: (a) the GDPR and any European Economic Area (the "**EEA**") Member State laws implementing the GDPR; (b) the California Consumer Privacy Act of 2018 (the "**CCPA**"), including as modified by the California Privacy Rights Act of 2020 (the "**CPRA**"), and the California Attorney General Regulations thereof; (c) the United Kingdom (the "**UK**") Data Protection Act 2018, as amended, and the GDPR, as incorporated into UK law (the "**UK GDPR**"); and (d) the Swiss Federal Act on Data Protection of 19 June 1992 and the revised version of 25 September 2020 and its corresponding ordinances (the "**Swiss FADP**").

   b. "**Data Breach**" means a confirmed unauthorized access by a third party or confirmed accidental or unlawful destruction, loss or alteration of Personal Data.

   c. "**Customer Product Usage Information**" means aggregated or pseudonymized metrics derived from Customer's use of the Software and which shall not include Customer Content.

   d. "**GDPR**" means the 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).

   e. "**Personal Data**" means all information defined in the definition of "personal data" under GDPR, which is used in the Service.

   f. "**Process**", "**Processing**", "**Processor**", and "**Controller**" shall have the meaning as defined under GDPR.

g. **“Restricted Transfer(s)”** means a transfer of Personal Data from the EEA, the UK or Switzerland to a country that has not received an adequacy decision from the European Commission or the UK or Swiss authorities.

h. “**Service(s)**” means the software and services licensed under the Subscription Agreement.

i. “**Standard Contractual Clauses**” means (i) where the GDPR applies, the contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (the “**EU SCCs**”); (ii) where the UK GDPR applies, the International Data Transfer Addendum issued by the United Kingdom’s Information Commissioner’s Office to the EU Commission's Standard Contractual Clauses available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf (the “**UK SCCs**”); and (iii) where the Swiss FADP applies, those clauses in section 15.d of this DPA (the “**Switzerland Clauses**”).

j. “**Sub-processor(s)**” means any third-party Processor engaged by GitLab to Process Personal Data in order to provide the Services to Customer under the Subscription Agreement.

k. “**Subscription Agreement**” shall mean GitLab’s standard terms of use and delivery with respect to its software and professional services generally made available here: https://about.gitlab.com/terms/ or such separate agreement as agreed to between the parties in writing similarly governing the use and delivery of GitLab’s software and professional services.

2. **Status of the Parties**. This DPA applies when GitLab Processes Personal Data in the provision of the Service. In this context, Customer may be the Controller, or in certain instances the Processor acting on behalf of the Controller, of Personal Data. In the event Customer is a Processor, this DPA will continue to refer to Customer as the Controller because it is unlikely that GitLab will know the identity of the Customer’s Controllers and because GitLab has no direct relationship with the Customer’s Controllers. GitLab is the Processor of Personal Data, except for those Processing activities detailed in section 18.a. of the DPA.

3. **Details of the Processing and Transfer Description**. The subject-matter of the Processing of Personal Data to be carried out by GitLab under the Subscription Agreement, along with the duration of the Processing, the nature and purpose of the Processing, the types of Personal Data, and the categories of data subjects Processed under these terms are further specified in **Exhibit A**. To the extent the Standard Contractual Clauses apply, the information in **Exhibit A** shall set forth the basis for such transfers under the Standard Contractual Clauses.

4. **Processing Instructions**. Where GitLab acts as a Processor, GitLab shall only Process Personal Data on behalf of Customer and only in accordance with documented instructions received from Customer. The parties agree this DPA, the Subscription Agreement, and any features and settings used in the Software shall constitute Customer's documented instructions. GitLab will notify Customer promptly if it considers that an instruction from Customer is in breach of any Applicable Data Protection Laws, and GitLab shall be entitled to suspend execution of the instructions. In the event GitLab is required to Process Personal Data under European Union or Member State law to which it is subject, GitLab shall without undue delay notify Customer of this legal requirement before carrying out such Processing, unless GitLab is prohibited from doing so on important grounds of public interest.

5. **Confidentiality by GitLab Personnel**. GitLab will limit access to Personal Data to personnel who are required to access Personal Data in order to perform the obligations under the Subscription Agreement. GitLab shall impose appropriate contractual obligations upon its personnel to maintain the confidentiality of the Personal Data.

6. **Security Measures**. GitLab will implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed. Those measures are set forth in Exhibit B to this DPA. Such measures take into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing. GitLab reserves the right to modify the measures set forth in Exhibit B, provided that such changes will not result in a material degradation of security.

7. **Data Breach**. In the event that GitLab becomes aware of a Data Breach, GitLab will: (i) notify Customer without undue delay after GitLab becomes aware of the Data Breach; (ii) as part of the notification, provide Customer with information regarding the Data Breach, to the extent such information is available to GitLab, to enable Customer to comply with its notification requirements under the Applicable Data Protection Laws; and (iii) promptly commence an investigation into the Data Breach and take appropriate remedial steps to prevent and minimize any possible harm. For the avoidance of doubt, Data Breaches will not include unsuccessful attempts to, or activities that do not compromise the security of Personal Data. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users.

8. **Data Subject Rights**. Where GitLab is a Processor and it receives a data subject request in relation to Customer, GitLab will either notify the Customer directly or reject the user's request and inform the user to contact Customer. Customer is responsible for ensuring such requests are handled in accordance with Applicable Data Protection Laws. GitLab will assist Customer with its obligations in connection with data subject requests. To the extent GitLab is a Controller and it receives a data subject request, GitLab will comply with the requirements of Applicable Data Protection Laws.

9. **Data Protection Impact Assessments (DPIA) and Prior Consultation**. Upon Customer's request, GitLab shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Applicable Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Service. GitLab shall provide reasonable assistance to Customer in the cooperation or prior consultation with supervisory authorities in the performance of its tasks relating to this section 9, to the extent required under Applicable Data Protection Laws.

10. **Requests from Authorities**.

    a. General Obligations. GitLab shall, unless otherwise prohibited, such as in order to preserve the confidentiality of an investigation by the law enforcement authorities, promptly inform Customer of: (i) any legally binding request for disclosure of Personal Data by a law enforcement authority; and (ii) any relevant notice, inquiry or investigation by a supervisory authority relating to Personal Data.

    b. Obligations for Personal Data Transferred Under the Standard Contractual Clauses. To the extent GitLab is a data importer under the Standard Contractual Clauses and receives a legally binding request for disclosure of Personal Data, GitLab agrees that: (i) it will attempt to obtain a waiver in the event that the country of destination prohibits GitLab from notifying Customer of the legally binding request for disclosure of Personal data; and (ii) provide as much relevant information as possible to Customer, if permitted under the laws of the country, about the requests received. In regards to the Personal Data disclosed, GitLab agrees that: (i) it will challenge the request for disclosure if, after careful assessment, GitLab believes the request is unlawful; and (ii) provide the minimum amount of Personal Data permitted when responding to the request for disclosure.

11. **Return or Deletion of Personal Data**. This section shall apply where GitLab acts as a Processor. Customer may, at any time during the term of the Agreement or upon termination of the Agreement, delete any groups containing Personal Data through the in-product administrative settings or group dashboard. Further, GitLab will, upon request, securely destroy or, at Customer's sole discretion, return all Personal Data (including all copies) and confirm to Customer that it has taken such measures, in each case to the extent permitted by applicable law. GitLab agrees to preserve the confidentiality of any Personal Data retained by it in accordance with applicable law and agrees that any active Processing of such Personal Data after termination of the Subscription will be limited to the extent necessary in order to comply with applicable law. GitLab shall ensure that the obligations set forth in this section are also required of Sub-processors.

12. **Controller Obligations**. Customer, acting as the Controller or on behalf of the Controller, agrees that:

a. It shall comply with all Applicable Data Protection laws, and as between Customer and GitLab, it shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data;

b. It has provided all legally required notices to and obtained all legally required consents from the data subjects whose Personal Data is Processed under the Subscription Agreement;

c. All instructions from Customer to GitLab with respect to Processing of Personal Data shall comply with Applicable Data Protection Laws;

d. It shall promptly inform GitLab of any non-compliance by Customer, its employees or contractors with this DPA or the provisions of the Applicable Data Protection Law relating to the protection of Personal Data Processed under the Subscription Agreement; and

e. It is solely responsible for making an independent determination as to whether the technical and organizational measures for the Service meet Customer's requirements, including any of its security obligations under applicable data protection requirements. Customer acknowledges and agrees that the security practices and policies implemented and maintained by GitLab provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls.

13. **Audit**.

a. GitLab Certification Audits. GitLab uses external auditors to verify the adequacy of its security measures, excluding the physical and environmental security of the third-party physical data centers from which GitLab provides the Services, as those controls are inherited by the third-party Sub-processor. This audit: (a) will be performed at least annually; (b) will be performed according to System and Organization Controls (SOC) 2 Report ISO 27001 standards or such other alternative standards that are substantially equivalent to System and Organization Controls (SOC) 2 Report ISO 27001; (c) will be performed by independent third party security professionals at GitLab's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be GitLab confidential information. At Customer's written request, and provided that the parties have applicable confidentiality terms in place, GitLab will provide Customer with a copy of the Report so that Customer can reasonably verify GitLab's compliance with its obligations under this DPA.

b. GitLab Customer Audits. GitLab shall enable remote self-serve audits of its security program by granting Customer access to the GitLab Customer Assurance Package and GitLab Handbook. The Customer Assurance Package and GitLab Handbook will include documentation evidencing GitLab's policies, procedures and security measures as well as copies of third-party audit reports as listed in section 13a. GitLab reserves the right to refuse to provide Customer (or its representatives) information which would pose a security risk to GitLab or its customers.

c. Feedback. Upon completion of the remote self-serve audit, Customer may submit audit results in writing to GitLab. GitLab may in its sole discretion make commercially reasonable efforts to implement Customer's suggested improvements.

d. Audit Rights Under Standard Contractual Clauses. To the extent GitLab is a Processor and Customer's audit requirements under the Standard Contractual Clauses or Article 28 of the GDPR cannot reasonably be satisfied through the Reports and self-serve audits set forth above, Customer may request an additional audit. Before the commencement of an audit, Customer and GitLab will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit. To the extent needed to perform the audit, GitLab will make the Processing systems and supporting documentation relevant to the Processing of Personal Data by GitLab and its Sub-processors available, including inspections (provided that no access to third party confidential information will be permitted). Such an audit will be conducted by Customer or by an independent, accredited third-party auditor during regular business hours, with reasonable advance notice to GitLab, and subject to reasonable confidentiality procedures. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time GitLab expends for any such audit. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with GitLab. Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

14. **Sub-processors**. To the extent that GitLab acts as a Processor:

a. Customer agrees that GitLab shall be entitled to use the Sub-processors listed at https://about.gitlab.com/privacy/subprocessors/ for the Service. If GitLab wishes to add a new Sub-processor to the list, GitLab will update the list on the website. Customer may subscribe at https://about.gitlab.com/privacy/subprocessors/#sign-up to receive email notifications of updates to the list, which will serve as written notice to Customer. If Customer wishes to object to the approval of a new Sub-processor, meaning an organization or entity not previously listed at https://about.gitlab.com/privacy/subprocessors/, it must provide such objection in writing to GitLab within thirty (30) days after notice has been received. If Customer objects to the change in Sub-processor, the parties will work together in good faith to resolve the objection, including making a commercially reasonable change to Customer's configuration or use of the Services to avoid the Processing of Personal Data by the new Sub-processor. Customer can only object to the addition of a new Sub-processor on the basis that such addition would cause Customer to violate data protection commitments or other applicable legal requirements. If Customer does not object within the referred period the respective Sub-processor shall be considered approved by Customer.

i. To the extent applicable for Customer whose Services include GitLab's Dedicated software with a specified regional hosting location, as may be mutually agreed and described in an Order Form or Subscription Agreement as applicable, that hosting location will be as so designated. Therefore, the cloud hosting location for any cloud hosting Sub-processors listed at https://about.gitlab.com/privacy/subprocessors/#third-party-sub-processors shall be amended to the location as listed and agreed as between Customer and GitLab.

ii. To the extent Customer has purchase Professional Services separate from the Subscription, as that term is defined under the GitLab Professional Services Agreement, and the parties have agreed GitLab will facilitate all or a part of such Professional Services via a subcontractor, Customer agrees that GitLab's use of such subcontractor(s) shall be an approved Sub-processor as listed at https://about.gitlab.com/privacy/subprocessors/#professional-services-sub-processors. If GitLab wishes to add a Sub-processor for Professional Services, it will follow the same notification process as described in section 14.a. of the DPA. All other provisions of this section 14 and the Standard Contractual Clauses, where applicable, will apply to those Sub-processors appointed under this provision.

b. Where a Sub-processor is appointed as described in section 14.a. above: (i) GitLab will restrict the Sub-processor's access to Personal Data to what is necessary to maintain the Service or to provide the Service to Customer in accordance with the documentation, and GitLab will prohibit the Sub-processor from accessing Personal Data for any other purpose; (ii) GitLab will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor is Processing Personal Data to enable the Service provided by GitLab under this DPA, GitLab will impose on the Sub-processor substantially similar contractual obligations that GitLab has under this DPA; and (iii) GitLab will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause GitLab to breach any of GitLab's obligations under this DPA.

15. **International Data Transfers**.

a. If a transfer of Personal Data from Customer to GitLab is a Restricted Transfer, the transfer shall take place on the basis of the EU SCCs and/or the UK SCCs and/or the Switzerland Clauses. In the event GitLab obtains certification under the EU-U.S. Data Privacy Framework (the "EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. Data Privacy Framework, GitLab may also make Restricted Transfers to the United States on the basis of these certifications. The parties agree that the obligations under the Standard Contractual Clauses or the EU-U.S. DPF shall only apply to a Restricted Transfer.

b. To the extent the **EU SCCs** apply, the parties agree that:

   i. where Module One of the EU SCCs applies to the Personal Data transferred for those Processing activities detailed in section 18.a of the DPA, Customer is acting as a Controller and "Data Exporter" and GitLab is acting as independent Controller and "Data Importer";
   ii. where Module Two of the EU SCCs applies to the Personal Data transferred, Customer is acting as a Controller and "Data Exporter" and GitLab is acting as a Processor and "Data Importer";
   iii. where Module Three of the EU SCCs applies to the Personal Data transferred, Customer is acting as a Processor and "Data Exporter" and GitLab is acting as a Processor and "Data Importer";
   iv. Clause 7. The optional docking clause does not apply;
   v. Clause 9(a). The parties select "Option 2 General Written Authorization" under Module Two and Module Three for the engagement of the Sub-processors identified in section 14 of this DPA and the time period for prior written notice of changes shall be thirty (30) days;
   vi. Clause 11. The optional language will not apply;
   vii. Clause 17. Option 2 will apply and the EU SCCs will be governed by the law of the Netherlands;
   viii. Clause 18(b). Disputes shall be resolved before the courts of the Netherlands;
   ix. Annex 1.A and I.B of the EU SCCs shall be deemed complete with the information set out in Exhibit A to this DPA;
   x. Annex I.C of the EU SCCs, where the data exporter is established in the EEA shall be the supervisory authority with responsibility for ensuring compliance by the Data Exporter with GDPR as regards to the data transfer. Where the data exporter is not established in the EEA, but is within the territorial scope of application of the GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1), the supervisory authority shall be the member state in which the representative within the meaning of Article 27(1) is established. If the data exporter is not established in the EEA, but falls within the territorial scope of application of the GDPR without having to appoint a representative pursuant to Article 27(2), the supervisory authority of the Netherlands shall act as the competent supervisory authority.

xi. Annex II of the EU SCCs shall be deemed complete with the information set out in Exhibit B to this DPA; and

xii. Annex III of the EU SCCs shall be deemed complete due to the General Authorization granted to those Sub-processors listed in section 14 of this DPA.

c. To the extent the **UK SCCs** apply, the parties agree that:

i. any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent article or section of the UK GDPR; and references to "EU", "Union" and "Member State law" are all replaced with "UK";

ii. Clause 13(a) of the EU SCCs are not used;

iii. references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;

iv. Clause 17 of the EU SCCs is replaced to state that "*The Clauses are governed by the laws of England and Wales*";

v. Clause 18 of the EU SCCs is replaced to state "*Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may 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

vi. the relevant Annexes of the UK SCCs shall be deemed complete with the information set out in Exhibit A to this DPA.

d. To the extent the **Switzerland Clauses** apply, the parties agree that:

i. the EU SCCs as implemented above will apply provided that “GDPR” shall be interpreted as references to the Swiss FADP;

ii. references to the “EU”, “Union”, and “Member State law” shall be interpreted as references to Switzerland and Swiss law;

iii. the term “member state” shall not exclude data subjects in Switzerland from being able to sue for their rights in their place of habitual residence; and

iv. references to any competent supervisory authority or court shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and courts in Switzerland.

e. Jurisdiction Specific Terms. To the extent GitLab Processes Personal Data originating from and protected by Applicable Data Protection Laws in one of the jurisdictions listed in “Exhibit C Jurisdiction Specific Terms” of this DPA, the terms specified in Exhibit C with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

f. If there is a conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail to the extent of the conflict or inconsistency.

16. **California Consumer Privacy Act and California Privacy Rights Act**. The following applies where GitLab is Processing Personal Data that is within the scope of CCPA or CPRA:

a. The parties agree that GitLab is a service provider as defined under CCPA, and that any Personal Data transferred to GitLab is done for a valid business purpose and for GitLab to perform the Services;

b. Subject to exceptions under CCPA, GitLab agrees that it will not sell Personal Data Processed under the Subscription Agreement, as the term "selling" is defined in the CCPA;

c. GitLab will not share, rent, release, disclose, disseminate, make available, transfer or otherwise communicate orally, in writing or by electronic or other means, the Personal Data, transferred under the Subscription Agreement or to perform the Services, to a third party for cross-contextual behavioral advertising in which no money is exchanged;

d. Customer may monitor GitLab's compliance with this DPA through those measures set forth in section 13, provided Customer will be subject to all requirements and limitations as specified in section 13.d.;

e. GitLab will not use or disclose Personal Data outside its direct business relationship with Customer; and

f. GitLab will not combine the Personal Data transferred under the Subscription Agreement or to perform the Services with information that it receives from or on behalf of a third-party or that it collects independently from California residents, except that GitLab may combine Personal Data to perform a valid business purpose as permitted under the CCPA and/or CPRA.

17. **Limitation of Liability**. To the maximum extent allowed under Applicable Data Protection Laws, the parties intend and agree that each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Subscription Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party under the Agreement and this DPA.

18. **Miscellaneous**.

a. GitLab’s Role as a Controller. Customer acknowledges and agrees that as part of providing the Services, GitLab will Process certain Personal Data as a Controller for the following legitimate business purposes: (i) to manage the relationship with Customer, such as the creation of customer relationship accounts and billing and licensing management; (ii) to conduct internal business operations, such as accounting, audit, tax, and other financial reporting purposes; (iii) to ensure the security of the Services, such as identity verification services and to prevent fraud and mitigate risk; (iv) to comply with our legal or regulatory obligations; and (v) to improve and develop our products and Services through the collection and Processing of Customer Product Usage Information. To the extent any data Processed under this section is Personal Data, GitLab agrees that it will Process such Personal Data in compliance with Applicable Data Protection Laws and only for the purposes that are compatible with those described in this section18.a. Customer Content will not be Processed for any of the purposes listed under this section, unless required under applicable law. GitLab shall be an independent Controller for the Processing listed in this section and will be solely responsible and liable for any such Processing.

b. This DPA, including the Standard Contractual Clauses, constitute the entire agreement and understanding of the parties, and supersedes any prior agreement or understanding between the parties, in each case in respect of the Processing of Personal Data for the purposes specified herein. In case of discrepancies between this DPA and Subscription Agreement, this DPA shall prevail.

EXHIBIT A

Details of the Processing and Transfer Description

A. **Section 2 of this DPA or Modules Two/Three of the EU SCCs**

1. **Data Exporter:** Customer
   Contact Details: As listed by Customer in the website purchase portal or as identified on any combination of an Order Form or Subscription Agreement.
   Signature and Date: Customer is deemed to have signed this DPA and the Restricted Transfer documentation incorporated herein, including their Exhibits, as of the effective date of acceptance via purchase by Customer through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed.
   Role: Controller or Processor

   Data Importer: GitLab, Inc.
   Contact Details: : 268 Bush St 350, San Francisco, CA, 94104-3503, USA; dpo@gitlab.com.
   Signature and Date: GitLab is deemed to have signed this DPA and the Restricted Transfer documentation incorporated herein, including their Exhibits, as of the effective date of acceptance via purchase by Customer through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed.
   Role: Processor or Sub-processor

2. **Categories of data subjects whose Personal Data is transferred**

   - Customer’s prospects, clients, business partners, and vendors (who are natural persons)
   - Customer’s employees, agents, advisors and freelancers (who are natural persons)
   - Customer’s users authorized by Customer to use the Services
   - Any other natural persons who become identifiable through content provided via Customer’s use of the Services

3. **Categories of Personal Data transferred**

   - Account Information, such as name, username, email address, and password
   - Profile Information, such as name, public avatar or photo, employer, email address, job title, address, social media handles, and biography
   - Contact information, such as name, address, email address, and telephone
   - Content provided through the use of the Services, such as repositories, issues, commits, project contributions, comments, and input/output related to AI-powered features
   - Customer Support Information, such as the request you are making or the services being provided

- Product Analytics for Customer to measure engagement by their own users, such as user-level metrics and counts related to interactions with the Software

4. **Sensitive or special categories of Personal Data**

GitLab does not intentionally collect sensitive or special categories of Personal Data, such as genetic data, health information, or religious information. These data elements should not be submitted to the Services without GitLab's consent, pursuant to section 14 of the Subscription Agreement.

In the event Customer submits sensitive or special categories of Personal Data to the Services without Gitlab's consent, such data will be subject to GitLab's technical and organizational security measures set forth in Exhibit B.

5. **Nature of the Processing**

The Processing relates to Customer's use of the Services for purposes determined and controlled by Customer its sole discretion.

6. **Purpose(s) of any data transfer and further Processing**

Purposes of the data transfer are to allow GitLab entities to provide the Services, which are hosted and processed on servers in the United States. Further, GitLab has a globally distributed workforce and a transfer of Personal Data may be necessary to render Customer Support.

7. **The frequency of any data transfer**

Personal Data will be transferred for the duration of the Subscription Term under the Subscription Agreement and this DPA on a continual basis.

8. **The period for which Personal Data will be retained**

Personal data will be retained for the period determined by Customer, including until termination of the Subscription Term, subject to exceptions allowed by law and under the Subscription Agreement with Customer.

9. **Transfers to Sub-processors**

GitLab's Sub-processors import data under the Standard Contractual Clauses or other lawful transfer mechanism for the purposes of cloud hosting, search functionality, application logging and debugging, content delivery, transactional emails, and Customer Support. GitLab uses Sub-processors in order to provide the Services to Customer.

Personal data will be retained for the period determined by Customer, including until termination of the Subscription Term, subject to exceptions allowed by law and under the Subscription Agreement with Customer.

B. **Section 18.a of this DPA or Module One of the EU SCCs**

1. **Data Exporter:** Customer
   Contact Details: As listed by Customer in the website purchase portal or as identified on any combination of an Order Form or Subscription Agreement.
   Signature and Date: Customer is deemed to have signed this DPA and the Restricted Transfer documentation incorporated herein, including their Exhibits, as of the effective date of acceptance via purchase by Customer through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed.
   Role: Controller

   Data Importer: GitLab, Inc.
   Contact Details: : 268 Bush St 350, San Francisco, CA, 94104-3503, USA; dpo@gitlab.com.
   Signature and Date: GitLab is deemed to have signed this DPA and the Restricted Transfer documentation incorporated herein, including their Exhibits, as of the effective date of acceptance via purchase by Customer through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed.
   Role: Controller

2. **Categories of data subjects whose Personal Data is transferred**

   - Customer’s employees, agents, advisors and freelancers (who are natural persons)
   - Customer’s users authorized by Customer to use the Services

3. **Categories of Personal Data transferred**

   - Account Management Information, such as license data, historical user data, and account administrator contact information
   - Billing Information, such as Customer’s billing address, billing contact, and credit card or banking information
   - Customer Product Usage Information, as defined in the DPA, such as feature usage and engagement metrics
   - Security and Fraud Prevention Information, such as log data, device data and IP address

4. **Sensitive or special categories of Personal Data**

GitLab does not collect sensitive or special categories of Personal Data for the purposes as described under this subsection B of Exhibit A.

5. **Nature of the Processing**

The Processing allows for GitLab to understand how the Services are used, to process payments for the Services, to administer the Services, to comply with legal obligations, and to protect the safety and property of GitLab and Customer.

6. **Purpose(s) of any data transfer and further Processing**

GitLab has a globally distributed workforce of employees who may be located in the United States and other countries outside of the European Economic Area, the United Kingdom and Switzerland.

7. **The frequency of any data transfer**

Personal Data will be transferred for the duration of the Subscription Term under the Subscription Agreement and this DPA on a continual basis.

8. **The period for which Personal Data will be retained**

Personal Data will be retained for the described in the Data Retention section of the GitLab Privacy Statement and in accordance with our Records Retention Policy posted at https://handbook.gitlab.com/handbook/legal/record-retention-policy/.

EXHIBIT B

Technical and Organizational Measures to Ensure the Security of Personal Data

GitLab will implement and maintain the following security measures:

- Those Technical and Organizational Security Measures for GitLab cloud services found at https://handbook.gitlab.com/handbook/security/security-assurance/technical-and-organizational-measures/.
- Those policies and certifications found in our Trust Center (https://trust.gitlab.com/).
- Sub-processors will implement and maintain security measures substantively similar to those listed in this Exhibit.

EXHIBIT C
Jurisdiction Specific Terms

1. AUSTRALIA

   The definition of Applicable Data Protection Laws includes the Australian Privacy Principles and the Australian Privacy Act (1988) and any succeeding amendments or accompanying regulations. The definition of Personal Data includes "Personal Information" as defined under the Australian Privacy Principles and the Australian Privacy Act (1988).

2. BRAZIL

   The definition of Applicable Data Protection Laws includes the Brazilian General Personal Data Protection Law of 14 August 2018 (the "**LGPD**"). The EU SCCs will be used for cross-border data transfers to countries not deemed adequate per the LGPD.

3. JAPAN

   The definition of Applicable Data Protection Laws includes the Act on Protection of Personal Information and its amendments and accompanying regulations (the "**APPI**"). The definition of Personal Data includes "Personal Information" as defined under the APPI. Where the APPI applies, GitLab's obligations to Customer are those express obligations on a "Processor" when Processing Personal Data on behalf of a "Business Operator," as defined under the APPI.

4. SINGAPORE

   The definition of Applicable Data Protection Laws includes the Personal Data Protection Act of 2012 of Singapore and its amendments and accompanying regulations (the "**PDPA**"). Where the PDPA applies, GitLab's obligations to Customer are those express obligations imposed by the PDPA on a "Data Intermediary" when Processing Personal Data on behalf of an "Organisation," as defined under the PDPA. Any claims arising from or related to the PDPA will be governed by the laws of Singapore and disputes shall be resolved before a court of general jurisdiction in Singapore.