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 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 EU Member State laws implementing the GDPR, (b) California Consumer Privacy Act of 2018 ("CCPA"), and (c) the UK Data Protection Act 2018.

   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. "**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).

   d. "**Personal Data**" means all information defined in the definition of "personal data" under GDPR, which is controlled by Customer and used in the Service.

   e. **"Process" or "Processing**" shall have the meaning as defined under GDPR.

   f. "**Service**" means the software and services licensed under the Subscription Agreement.

   g. **"Standard Contractual Clauses"** means Exhibit B, attached to and forming part of this DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

2. **Status of the Parties.** This DPA applies when GitLab Processes Personal Data in the provision of the Service. In this context, Customer is the "controller" of Personal Data and GitLab is the "processor" of Personal Data, as each term is defined in the GDPR.

3. **Scope of Data Processing.** The subject-matter of the data processing, along with the nature and purpose of the Processing to be carried out by GitLab under this Agreement, and the types of Personal Data and categories of data subject is as set forth in Exhibit A.

4. **Processing Instructions.** 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 our Technical and Organizational Measures section. Such measures take into account the art and costs of implementation as well as the nature, scope, context and purposes of the Processing. GitLab reserves the right to modify the Technical and Organizational Measures, provided that such changes will maintain or provide better measures.

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.** GitLab will promptly inform Customer of any data subject requests it receives in connection with the Service. Customer is responsible for ensuring such requests are handled in accordance with Applicable Data Protection Laws. GitLab will implement measures to reasonably assist Customer with its obligations in connection with data subject requests.

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 the GDPR 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 the GDPR.

10. **Requests from Authorities.** 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.

11. **Return or Deletion of Personal Data**. Upon termination of the Subscription Agreement or any time upon written notification by Customer, GitLab will, 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 Services will be limited to the extent necessary in order to comply with applicable law. GitLab shall ensure that the post-termination obligations set forth in this section are also required of sub-processors.

12. **Controller Obligations**. Customer agrees that:

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

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

    c. 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.

    d. 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 service provider. 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 13 a. 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 the Standard Contractual Clauses apply, and Customer's audit requirements under the Standard Contractual Clauses cannot reasonably be satisfied through the Reports and self-serve audits set forth above, Customer's 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. Such an audit will be conducted by an independent, accredited third-party audit firm, 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.

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 and such update will serve as notice to Customer. Customer may subscribe at https://about.gitlab.com/privacy/subprocessors/ to receive email notifications of updates to the list. If Customer wishes to object to the approval of a new sub-processor it must provide such objection in writing to GitLab within fourteen (14) 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. Customer can only object to the addition of a new sub-processor on the basis that such addition would cause Customer to violate applicable legal requirements. If Customer does not object within the referred period the respective sub-processor shall be considered approved by Customer.

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 only 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 performing the same data processing services that are being 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.** The parties agree that the Standard Contractual Clauses in Exhibit B will apply when GitLab is Processing Personal Data outside of the European Economic Area, United Kingdom or Switzerland in a country that does not ensure an adequate level of protection for personal data (as described in the GDPR). 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.** If GitLab is processing Personal Data that is within the scope of CCPA, then the parties agree that GitLab is service provider as defined under CCPA, and that any Personal Data provided to GitLab is done for a valid business purpose and for GitLab to perform the Services. GitLab agrees that it will not sell, retain, use or disclose Personal Data for any purpose other than providing the Services.

17. **Limitation of Liability**. 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. Customer acknowledges and agrees that as part of providing the Services, GitLab has the right to use data relating to or obtained in connection with the operation, support, or use of the Services for its legitimate business purposes, such as billing and account management, internal reporting, to administer and deliver the Services, to improve and develop our products and services, to comply with legal obligations, to ensure the security of the Services, and to prevent fraud or mitigate risk. To the extent any such data 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 Section 18.a. GitLab further agrees that it shall be an independent Controller and solely responsible and liable for any of its 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.

GITLAB

By: Brian Robins

Name: Brian Robins

Title: CFO

20201112

Exhibit A

Details of the Processing

Nature and Purpose of Processing

GitLab will Process Personal Data as necessary to perform the Service pursuant to the Subscription Agreement, and as further instructed by Customer in its use of the Service.

Duration of Processing

Subject to Section 11 (Return or Deletion of Personal Data), GitLab will Process Personal Data for the duration of the Subscription Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, Controllers, business partners and vendors of Controller (who are natural persons)
- Employees or contact persons of Controller's prospects, Controllers, business partners and vendors
- Employees, agents, advisors, freelancers of Controller (who are natural persons)
- Controller's users authorized by Controller to use the Services

Type of Personal Data

Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Connection data
- Localization data

Exhibit B

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection:

Customer (hereinafter the “data exporter”)

and

GitLab Inc. (hereinafter the “data importer”)

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

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

CLAUSE 1

Definitions

For the purposes of the Clauses:

a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b) 'the data exporter' means the controller who transfers the personal data;

c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

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

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

f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or

access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

CLAUSE 2

Details of the transfer

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

CLAUSE 3

Third-party beneficiary clause

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

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

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

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

CLAUSE 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

3. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

4. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

5. that it will ensure compliance with the security measures;

6. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

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

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

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

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

CLAUSE 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

3. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

4. that it will promptly notify the data exporter about:

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

ii. any accidental or unauthorized access, and

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

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

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

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

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

9. that the processing services by the subprocessor will be carried out in accordance with Clause 11;

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

CLAUSE 6

Liability

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

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist

in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

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

CLAUSE 7

Mediation and jurisdiction

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

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

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

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

CLAUSE 8

Cooperation with supervisory authorities

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

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

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any

subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

CLAUSE 9

Governing Law

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

CLAUSE 10

Variation of the contract

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

CLAUSE 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses . Where the subprocessor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

CLAUSE 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the

data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

On behalf of the **data importer**:

Name (written out in full): Brian Robins

Position: Chief Financial Officer

Address: 268 Bush Street, #350
San Francisco, CA 94104

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

Signature Brian Robins.....

(stamp of organization)

APPENDIX 1 TO STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is the entity identified as “Customer” in the DPA.

Data importer

The data importer is GitLab, Inc. the provider of a software development and collaboration platform.

Data subjects

Data subjects are defined in Exhibit A of the DPA.

Categories of data

The personal data is defined in Exhibit A of the DPA.

Processing operations

The processing operations are defined in Exhibit A.

DATA IMPORTER

Name:…Brian Robins……

Authorized Signature Brian Robins ……

APPENDIX 2 TO STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organizational security measures implemented by the data importer are as described at https://about.gitlab.com/handbook/engineering/security/security-assurance/technical-and-organizational-measures.html.

DATA IMPORTER

Name:…Brian Robins……

Authorized Signature Brian Robins ……