

## Subscription Agreement

This Subscription Agreement (“**Agreement**”) is entered into as of the date set forth in the Order Form or Purchase Order (“**Effective Date**”) between GitLab Federal, LLC with offices at 1775 Tysons, Blvd., Floor 5, Tysons, VA 22102-4285 (“**GitLab**”), and the Ordering Activity under GSA Schedule contracts identified in the Order Form or Purchase Order (“**Customer**”). “Ordering Activity” shall be defined as an entity authorized to order under GSA Schedule contracts, as defined in GSA Order OGP 4800.21, as may be revised from time to time.

### 1. DEFINITIONS

“Acceptance” of an Order Form shall occur at the earliest of the following: (a) execution of an Order Form, (b) reference to an Order Form Quote No. within a purchase order or similar document, or (c) the use of Software.

“Add-On User(s)” are additional Users in excess of those that have been purchased under a Subscription via an executed Order Form or web-portal purchase.

“Affiliate” means any entity(ies) controlling, controlled by, and/or under common control with a party hereto, where “control” means the ownership of more than 50% of the voting securities in such entity.

“Appendix” are inclusions in this Agreement that state the terms by which Software is offered to Customer. The Appendices shall be considered part of the Agreement.

“Authorized Partner” is a reseller or distributor that is enabled and authorized to sell Software.

“Community Edition Software” means the publicly available, community-developed open-source software and components which may be provided with the Software. Community Edition Software is provided as Free Software (as defined herein).

“Contractors” are defined as third parties that Customer has engaged to manage, or otherwise use the Software, solely on behalf of Customer.

“Controlled Subject Matter” is the Software or any software or anything related thereto or any direct product thereof, collectively.

“Customer Content” is all software, information, content and data provided by or on behalf of Customer or made available or otherwise distributed through the use of the Software.

“Customer Records” collectively means books, records, contracts and accounts relating to the payments due GitLab under this Agreement.

“Customer Success Services” means adoption services which are provided as part of the Subscription, as set forth in Appendix 1. Customer Success Services include the collection of Operational Data (as further stated in Appendix 1). Customer Success Services are only available to Customers who are purchasing Software, and are not available for Free Software.

“Customer Support” means technical support of the Software provided by GitLab.

“Designated National” is any person or entity on the U.S. Department of Treasury’s List of Specially Designated Nationals or the U.S. Department of Commerce’s Table of Denial Orders.

“Embargoed Countries” refers collectively to countries to which the United States maintains an embargo.

“Enterprise” means the organization, company, corporation and/or other type of entity which procures the Software to be used on its behalf pursuant to the terms of this Agreement.

“Fees” are those fees set forth within the Order Form, or, fees due immediately when purchasing via the web-portal.

“Free Software” means a feature-limited version of Software provided to a Customer, User, end user, partner, or any other third party at no (or a greatly reduced cost) including but not limited to, the lowest tier offering of Software as made available by GitLab.

“Individual” means a person who uses the Software on their own behalf, and not an Enterprise. An Individual must be over the age of thirteen (13) years old.

“Order Form” is a transactional document agreed to between the parties which states the Software and/or Supplemental Services being purchased, term of use, price, and other applicable transaction details. For the avoidance of doubt, the parties acknowledge and agree the terms and conditions stated within this Agreement and an executed Order Form shall govern with respect to all matters contemplated herein.

“Purchase Order” is a Customer’s processing document, or similar record, which is used by Customer to demonstrate internal approval and /or record of a purchase. Any terms stated within a Purchase Order shall be null and void and are expressly rejected by the parties.

“Software” means software, and other branded offerings made available by GitLab or its Affiliate(s), including but not limited to, GitLab’s DevOps Lifecycle Application Platform.

“Subscription” refers to the applicable services, support and function(s) of the Software as provided. Subscriptions are provided in tiers / levels as described in Appendix 1 and are based on the number of Users.

“Subscription Start Date” is, unless otherwise agreed to in writing: (i) if purchasing directly from GitLab the date, (a) stated on an Order Form, or, the date in which Customer is given access to the Software (whichever is later), or (b) transacted via the Website, (ii) if purchasing through an Authorized Partner, the date in which agreed to between Customer and said Authorized Partner.

“Subscription Term” shall begin on the Subscription Start Date and continue for twelve (12) months, unless otherwise agreed to in an Order Form or web-portal purchase.

“Supplemental Services” means additional capacity, functionality, storage and/or other elements that Customer may procure in addition to the Software. Such Supplemental Services may be purchased by Order Form or web-portal. Supplemental Services purchased will be: (i) provided as a separate line item in an Order Form or web-portal purchase, and (ii) co-termed to the underlying Subscription Term if not purchased on the Subscription Start Date. For the avoidance of doubt, Supplemental Services are not part of the Software, but rather, are provided in addition to the Software and Supplemental Services shall be subject to the terms and conditions of this Agreement.

“User(s)” is defined as the unique and single Individual, or employee, Contractor, or other third party individual authorized by Customer (in accordance with this Agreement) who are able to access the Software purchased under a Subscription, regardless of whether the User actually accesses or the frequency with which they access the Software. A User must be over the age of thirteen (13) years old.

“Website” means GitLab’s website located at [www.gitlab.com](http://www.gitlab.com) and all subdomains, and all content, services, documentation provided on the Website.

## **2. SCOPE OF AGREEMENT**

2.1 This Agreement establishes a framework that will enable GitLab to provide Customer with the Software. Software is provided as part of a Subscription, as described in Appendix 1. Software provided as a hosted solution, or Software-as-a-Service (“SaaS Software”), shall be subject to the attached Appendix 2 entitled “Software as a Service (SaaS) Offering”.

## **3. ORDERING PROCESS**

3.1 This Agreement applies to Software that Customer licenses directly from GitLab, a GitLab Affiliate, or from an Authorized Partner. For the avoidance of doubt, in the event Customer purchases from an Authorized Partner, GitLab shall have no obligations to Customer with respect to any terms and conditions outside of this Agreement unless otherwise agreed to in writing between Customer and GitLab.

3.2 Unless otherwise agreed to between Customer and GitLab in writing, the terms of this Agreement shall govern any and all use of the Software. Purchases of Software may take place by either:

- (i) purchasing via the GitLab Website;
- (ii) executing an Order Form with GitLab or an Affiliate of GitLab; or
- (iii) purchase from an Authorized Partner.

3.3 GitLab and Customer acknowledge and agree that Free Software may be: (i) modified and/or updated, without notice, and (ii) limited in functionality, features, maintenance, support and contain other limitations not present in Software purchased. NOTWITHSTANDING THE “WARRANTY” AND “INDEMNIFICATION” SECTIONS

BELOW, FREE SOFTWARE AND SOFTWARE OFFERED ON A TRIAL BASIS (AS STATED IN AN ORDER FORM OR WEB-PORTAL PURCHASE) ARE PROVIDED “AS-IS” WITHOUT ANY WARRANTY AND GITLAB SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO SUCH FREE SOFTWARE UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW, IN WHICH CASE GITLAB’S LIABILITY WITH RESPECT TO SUCH FREE SOFTWARE SHALL NOT EXCEED \$1,000.00USD.

#### **4. TERM AND TERMINATION**

4.1 The Agreement commences on the Effective Date and continues until it is terminated in accordance with this Section 4.

4.2 Subscriptions may be renewed for successive terms (of the same duration) as the original Subscription Term by executing a written Order Form or Purchase Order for the renewal Subscription Term. Subscriptions must be used during the Subscription Term and any unused Subscriptions will expire.

4.3 When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Gitlab shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

4.4 Reserved.

4.5 Unless otherwise stated herein, termination of this Agreement shall not affect any Subscriptions currently being delivered and this Agreement shall remain in full force and effect until the expiration of the then-current Subscription Term. In the event this Agreement is terminated in accordance with Section 4.3, GitLab will refund Customer any prepaid Fees for the prorated portion of unused Subscription Term. If this Agreement is terminated by GitLab in accordance with this Section 4, Customer will not receive any credits or refunds for any Fees already paid, or due and payable as of the date of termination. For the avoidance of doubt, in no event will termination relieve Customer of its obligation to pay any Fees payable to GitLab for the period prior to the effective date of termination.

#### **5. RESTRICTIONS AND RESPONSIBILITIES**

5.1 Customer will not, and will not permit any third party to:

- (i) use the Software for any purpose other than as specifically authorized in this Agreement;
- (ii) use the Software in such a manner that would enable any third party to access the Software;
- (iii) use the Software for time sharing or service bureau purposes (including without limitation, sublicensing, distributing, selling, reselling any Software);
- (iv) for any purpose other than its and its Affiliates’ own internal use;
- (v) use the Software other than in compliance with all applicable laws and regulations;
- (vi) use the Software in any manner that: (a) is harmful, fraudulent, deceptive, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, or libelous (including without limitation, accessing any computer, computer system, network, software, or data without authorization, breaching the security of another user or system, and/or attempting to circumvent any User authentication or security process); (b) impersonates any person or entity, including without limitation any employee or representative of GitLab; (c) includes content, with respect to the use of SaaS Software, which is illegal or violates the GitLab Community Code of Conduct found here <https://about.gitlab.com/community/contribute/code-of-conduct/>, or (d) contains a virus, trojan horse, worm, time bomb, unsolicited bulk, commercial, or “spam” message, or other harmful computer code, file, or program (including without limitation, password guessing programs, decoders, password gatherers, keystroke loggers, cracking tools, packet sniffers, and/or encryption circumvention programs); and
- (vii) except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile the Software or access it to: (1) build a competitive product or service, (2) build a product or service using similar ideas, features, functions or graphics of the Software, (3) copy any ideas, features, functions or graphics of the Software, or (4) determine whether the Software are within the scope of any patent.

5.2 Nothing in this Agreement shall prohibit Customer from using the Software for benchmark testing or comparative analysis. Customer will comply with all applicable data privacy and security laws and shall have appropriate technological, administrative, and physical controls in place to ensure such compliance.

5.3 In addition to the obligations set forth in Section 5.4, and subject to the rights set forth in Section 5.7, Customer shall ensure the collection of data as required in order to use the Software ("Subscription Data") shall remain unchanged. An overview of the Subscription Data can be found on GitLab's Website.

5.4 In accordance with this Agreement, GitLab has the right to verify electronically (or otherwise), and generate reports related to Customer's installation of, access to, and use of the Software to ensure compliance with the terms of this Agreement. Customer shall maintain Customer Records during the term of this Agreement and for two (2) years thereafter. GitLab may, upon thirty (30) days' prior written notice to Customer and during Customer's normal business hours and subject to industry-standard confidentiality obligations and Government security requirements, hire an independent third-party auditor to audit the Customer Records only to verify the amounts payable under this Agreement with respect to Customer usage of the Software. If an audit reveals underpayment, Customer shall promptly pay the deficiency to GitLab plus late fees pursuant to Section 6. GitLab shall bear the cost of an audit.

5.5 Customer will be responsible for the following:

- (i) maintaining the security of Customer's account, passwords (including, but not limited to, administrative and User passwords) and files, and for all uses of Customer account with or without Customer's knowledge or consent; and
- (ii) any acts or omissions carried out by Contractors on Customer's behalf. Customer shall ensure that Contractors are subject to terms no less stringent than those stated herein.

5.6 Subject to this Agreement and the applicable Order Form, GitLab will provide Customer Support to Customer for the Subscriptions, during the Subscription Term, at no additional cost. Details regarding Customer Support can be found in Appendix 1, as well as on GitLab's Website, as may be non-materially updated from time to time in accordance with GSA Schedule Contract Clause 552.212-4(w)(1)(vi).

5.7 Portions of the Software are governed by underlying open source licenses as described on GitLab's Website. This Agreement and applicable Appendix(es) establish the rights and obligations associated with Subscriptions and Software and are not intended to limit Customer's right to software code under the terms of an open source license.

5.8 Customer acknowledges and agrees that:

- (i) Account names are administered by GitLab on a "first come, first serve" basis;
- (ii) Intentional name squatting, or purchasing, soliciting, or selling of an account name is prohibited; and
- (iii) GitLab reserves the right to remove, rename, or close inactive accounts at its discretion.

5.9 Customer represents and warrants that it has, and shall retain, all right, title and interest (including, without limitation, sole ownership of) relating to Customer Content, and the intellectual property rights related thereto.

## **6. PAYMENT OF FEES**

6.1 With respect to purchases direct from GitLab, all web-portal purchase Fees shall be due and payable immediately.

6.2 With respect to purchases direct from GitLab, the Order Form shall: (i) reference this Agreement; (ii) state the Subscription Term(s) and Subscription(s) that are being purchased; and (iii) state the Fees due for the applicable Subscription(s).

6.3 With respect to purchases direct from GitLab, such Order Form is hereby incorporated into this Agreement by reference. The parties hereby agree to the terms and conditions stated within this Agreement and those found within an Order Form to the exclusion of all other terms. The parties agree that all terms stated within a Purchase Order, or other similar document, shall be null and void and are expressly rejected unless bilaterally negotiated and agreed to in writing by both parties.

6.4 With respect to purchases direct from GitLab, Customer will pay GitLab the applicable Fees, including those for Supplemental Services, without any right of set-off or deduction. All payments will be made in accordance

with the payment details stated within the applicable Order Form. If not otherwise specified: (a) GitLab (or applicable GitLab Affiliate) will invoice Customer for the Fees upon the Acceptance of an Order Form; and (b) all Fees will be due and payable within thirty (30) days of Customer's receipt of an invoice. Except as expressly set forth in this Agreement, all Fees paid or due hereunder (including prepaid amounts) are non-refundable, including without limitation if this Agreement is terminated in accordance with Section 4 herein.

6.5 During the Subscription Term, Customer may, subject to this Agreement, activate and use Add-On Users. For the avoidance of doubt, Customer shall not have the right to report less than the number of Users originally purchased under the Subscription, and all Add-On Users or additional Users shall be co-termed to the underlying Subscription Term.

6.6 With respect to purchases direct from GitLab, at the end of each three (3) month period, commencing up on the Subscription Start Date, (referred to herein as "Quarter" or "Quarterly") during the Subscription Term, GitLab will: (i) per Section 5.3, generate a report of Add-On User(s) deployed during the Quarter ("Quarterly Usage Report"), and (ii) invoice Customer on a prorated basis for the remaining portion of the Subscription Term, with respect to the Add-On User(s) activated and/or used during the Quarter as captured by the Quarterly Usage Report. For the avoidance of doubt, Add-On User(s) will not be invoiced for the Quarter in which they were activated and/or used. A Quarterly Usage Report will be generated during the first three (3) Quarters of a Subscription Term. Upon expiration of the Subscription Term, Customer's renewal of the Software shall be for either: (i) the amount agreed to between Customer and GitLab in an Order Form; or (ii) the number of active Users present in the GitLab Subscription as of the day of Customer's renewal. Add-On User(s) that have been identified within the Quarterly Usage Report, shall be considered due and payable in accordance with this Section 6. In the event a Quarterly Usage Report cannot be generated, Customer shall report and pay for such Overage Users (as defined below) in compliance with Section 6.7. Unless the parties agree to an Effective Price which is less than the List Price and in accordance with the GSA Schedule Pricelist, as set forth in an Order Form or Website purchase, Add-On Users will be invoiced at the List Price in the most recent Order Form or Website purchase. "Effective Price" means the actual price paid by Customer (List Price minus any applicable discount(s)) as set forth on an Order Form or as purchased via the Website. "List Price" means the list price of the GitLab Software excluding (if applicable) any discount(s) set forth in an Order Form or as purchased via the Website.

6.7 In the event a Customer procures Software from an Authorized Partner, or, GitLab is unable to: (a) verify and generate a Quarterly Usage Report, and/or (b) collect payment(s) with respect to Quarterly Add-Ons as provided in the Quarterly Usage Report, Customer shall be obligated to: (i) provide a report no later than twelve (12) months following the Subscription Effective Date ("Annual Report") of all Users from said Subscription Term ("Overage Users"), and (ii) be obligated to pay for such Overage Users, for the previous twelve (12) months, at the then current List Price for the GitLab Software. Overage Users subject to the Annual Report shall not include any pro-ration, set-off and/or deduction to account for term of use, or otherwise. Overage Users that have been identified in an Annual Report shall be considered due and payable in accordance with Section 6. In the event Overage Users are outstanding upon the expiration of a Subscription Term, Customer shall be obligated to pay for such Overage Users in order to renew the Software.

6.8 Any unpaid Fees are subject interest at the interest rate established by the Secretary of the Treasury as provided in [41 U.S.C. 7109](#), which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. Vendor shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with FAR 552.212-4(k).

## **7. CONFIDENTIALITY**

7.1 Each party (the "Receiving Party") understands that the other party (the "Disclosing Party") has disclosed or may disclose information relating to the Disclosing Party's technology or business (hereinafter referred to as "Confidential Information"). Such Confidential Information shall be either: (i) identified as confidential at the time of disclosure; or (ii) the nature of such information and/or the manner of disclosure are such that a reasonable person would understand it to be confidential. Without limiting the foregoing, and subject to applicable open source license(s), the Software is considered GitLab Confidential Information.

7.2 The Receiving Party agrees: (i) not to divulge to any third person any such Confidential Information; (ii) to give access to such Confidential Information solely to those employees with a need to have access thereto for purposes of this Agreement; and (iii) to take the same security precautions to protect against disclosure or

unauthorized use of such Confidential Information that the party takes with its own confidential information, but in no event will a party apply less than reasonable precautions to protect such Confidential Information.

7.3 The Disclosing Party agrees that Section 7.2 will not apply with respect to any information for which the Receiving Party can document: (i) is or becomes generally available to the public without any action by, or involvement of, the Receiving Party; or (ii) was in its possession or known by it prior to receipt from the Disclosing Party; or (iii) was rightfully disclosed to it without restriction by a third party, or (iv) was independently developed without use of any Confidential Information of the Disclosing Party.

7.4 The parties' obligations with respect to the protection of Confidential Information shall remain in force for a period three (3) years following the receipt of such Confidential Information and shall survive any termination or expiration of this Agreement.

7.5 Nothing in this Agreement will prevent the Receiving Party from disclosing Confidential Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing Party, when legally possible, reasonable prior notice of such disclosure to allow the Disclosing Party to contest such order.

7.6 Each party acknowledges and agrees that, to the extent permitted by law, the other may suffer irreparable damage in the event of a breach of the terms of this Section 7 and that such party will be entitled to seek injunctive relief (without the necessity of posting a bond) to cease the other party's activities that are alleged to violate the confidentiality obligations herein.

7.7 Both parties will have the right to disclose Confidential Information in connection with: (i) a required filing to a governmental authority (provided such party will use reasonable efforts to obtain confidential treatment or a protective order), or (ii) disclosures made to potential investors or acquirers, provided that at all times the Confidential Information shall be protected in a manner no less stringent as set forth in this Section 7. Gitlab recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by GitLab.

7.8 GitLab may collect data with respect to, and report on the aggregate response rate and other aggregate measures of, the Software performance and Customer's usage of the Software. Notwithstanding the foregoing, GitLab will not identify Customer to any third party as the source of any such data without Customer's prior written consent.

## **8. INTELLECTUAL PROPERTY RIGHTS**

8.1 Subject to the terms and conditions of this Agreement, GitLab hereby grants to Customer and its Affiliates a limited, non-exclusive, non-transferable, non-sublicensable license for Customer's and its Affiliates' Users to use, reproduce, modify, prepare derivative works based upon, and display the code of Software at the tier level selected by Customer, or as set forth in an Order Form, solely for: (i) its internal use in connection with the development of Customer's and/or its Affiliates' own software; and (ii) the number of Users for which Customer has paid GitLab. Notwithstanding anything to the contrary, Customer agrees that GitLab and/or its licensors (as applicable) retain all right, title and interest in and to all Software incorporated in such modifications and/or patches, and all such Software may only be used, copied, modified, displayed, distributed, or otherwise exploited in full compliance with this Agreement, and with a valid Subscription for the correct number of Users.

8.2 Except as expressly set forth herein, GitLab (and its licensors, where applicable) will retain all intellectual property rights relating to the Software and any suggestions, ideas, enhancement requests, feedback, or other recommendations provided by Customer, its Affiliates, Users or any third party relating to the Software (herein referred to as "Feedback Materials"), which are hereby assigned to GitLab. For the avoidance of doubt, Feedback Materials shall not include Customer Confidential Information or intellectual property owned by Customer. This Agreement does not constitute a sale of the Software and does not convey to Customer any rights of ownership in or related to the Software or any other intellectual property rights. GitLab acknowledges that the ability to use this Agreement and any Feedback Materials provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

8.3 Customer shall not remove, alter or obscure any of GitLab's (or its licensors') copyright notices, proprietary legends, trademark or service mark attributions, patent markings or other indicia of GitLab's (or its licensors') ownership or contribution from the Software.

## **9. WARRANTY**

9.1 During the Subscription Term, GitLab represents and warrants that: (i) it has the authority to enter into this Agreement, (ii) the Software shall be provided in a professional and workmanlike manner by qualified personnel; and (iii) it will use commercial industry standard methods designed to ensure the Software provided to Customer does not include any computer code or other computer instructions, devices or techniques, including without limitation those known as disabling devices, trojans, or time bombs, that are intentionally designed to disrupt, disable, harm, infect, defraud, damage, or otherwise impede in any manner, the operation of a network, computer program or computer system or any component thereof, including its security or User data.

9.2 If at any time GitLab fails to comply with the warranties in this Section 9, Customer may promptly notify GitLab in writing of any such noncompliance. GitLab will, within thirty (30) days of receipt of such written notification, either correct the noncompliance or provide Customer with a plan for correcting the noncompliance. If the noncompliance is not corrected or if a reasonably acceptable plan for correcting the noncompliance is not established during such period, Customer may terminate this Agreement and receive a prorated refund for the unused portion of the Subscription Term as its sole and exclusive remedy for such noncompliance.

9.3 EXCEPT AS SPECIFICALLY SET FORTH IN THIS AGREEMENT, THE SOFTWARE, SUPPLEMENTAL SERVICES AND CONFIDENTIAL INFORMATION AND ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT ARE PROVIDED "AS-IS," WITHOUT ANY WARRANTIES OF ANY KIND. GITLAB AND ITS LICENSORS HEREBY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

## **10. INDEMNIFICATION**

10.1 GitLab will have the right to intervene to defend Customer from any claim, demand, suit or proceeding made or brought against Customer by a third party alleging the Software (excluding Free Software as set forth in Section 3.3) provided by GitLab infringes or misappropriates such third party's patent or copyright (a "Customer Claim"). Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. GitLab will indemnify and hold Customer harmless from any damages, reasonable attorneys' fees and costs finally awarded against Customer as a result of a Customer Claim, or for amounts paid by Customer under a settlement approved (in writing) by GitLab, provided Customer: (i) promptly notifies GitLab in writing of the Customer Claim; (ii) gives GitLab all reasonable assistance at GitLab's expense; and (iii) gives GitLab sole control over defense and settlement thereof except that GitLab may not settle any Customer Claim unless it unconditionally releases Customer of all liability. The foregoing obligations do not apply if: (i) the Customer Claim arises from Software or any part thereof that is modified by Customer, or at Customer's direction, after delivery by GitLab; (ii) the Customer Claim arises from the use or combination of the Software or any part thereof with other products, processes or materials not provided by GitLab where the alleged infringement relates to such combination; (iii) Customer continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement; (iv) the Customer Claim arises from software not created by GitLab, or (v) the Customer Claim results from Customer's breach of this Agreement and/or applicable Order Forms. Notwithstanding the foregoing, in the event of a Customer Claim, GitLab, at its discretion, option and expense, reserves the rights to: (a) modify the Software to make it non-infringing provided there is no material loss of functionality; (b) settle such claim by procuring the right for Customer to continue using the Software; or (c) if in GitLab's reasonable opinion neither (a) or (b) are commercially feasible, terminate the license to the Software and refund a pro-rata portion of the amount paid by Customer for such Software for the unused portion of the Subscription Term.

10.2 When any controversy with the Customer cannot be resolved with the Contracting Officer, this Agreement is subject to 41 U.S.C., Chapter 71, Contract Disputes. Failure of the parties to this Agreement to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this Agreement shall be a dispute to be resolved in accordance with FAR 52.233-1, Disputes, which is incorporated herein by reference.

10.3 This Section 10 (Indemnification) states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against the other party for any third-party claim described in this section.

## **11. LIMITATION OF LIABILITY**

11.1 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY OR THEIR LICENSORS BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES, LOSS

OF REVENUE, ANTICIPATED PROFITS, LOST BUSINESS OR LOST SALES, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR WILLFUL MISCONDUCT; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

11.2 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE TOTAL LIABILITY OF EACH PARTY AND ITS AFFILIATES AND LICENSORS ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, WILL NOT EXCEED, IN THE AGGREGATE, THE TOTAL AMOUNT PAID BY CUSTOMER OR ITS AFFILIATES HEREUNDER IN THE ONE YEAR PERIOD PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE FOREGOING LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY, BUT WILL NOT LIMIT CUSTOMER'S OR ITS AFFILIATES' PAYMENT OBLIGATIONS UNDER THE "PAYMENT OF FEES" SECTION ABOVE.

## **12. U.S. GOVERNMENT MATTERS**

12.1 Notwithstanding anything else, Customer may not provide to any person or export or re-export or allow the export or re-export of Controlled Subject Matter, in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority.

12.2 Without limiting the foregoing, Customer acknowledges and agrees that the Controlled Subject Matter will not be used or transferred or otherwise exported or re-exported to Embargoed Countries, or to or by a national or resident thereof, or to or by Designated Nationals. The lists of Embargoed Countries and Designated Nationals are subject to change without notice. Use of the Software is representation and warranty that the Customer, Customer personnel, or Contractors are not located in, under the control of, or a national or resident of an Embargoed Country or a Designated National.

12.3 The Controlled Subject Matter may use or include encryption technology that is subject to licensing requirements under the U.S. Export Administration Regulations.

12.4 As defined in FAR section 2.101, any software and documentation provided by GitLab are "commercial items" and according to DFAR section 252.227-7014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFAR section 227.7202 and FAR section 12.212, any use modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

## **13. FORCE MAJEURE**

13.1 Excusable delays shall be governed by FAR 52.212-4(f).

13.2 The Non-performing Party will be excused from any further performance of the non-monetary obligations affected by such Force Majeure Event for as long as such Force Majeure Event continues and the Non-performing Party continues to use commercially reasonable efforts to resume performance.

13.3 Except as expressly excused in this Section 13, each party will continue to perform its respective obligations under this Agreement during a Force Majeure Event.

## **14. SECURITY / DATA PROTECTION**

14.1 Without limiting GitLab's obligations as stated in Section 7 (Confidentiality), GitLab shall be responsible for establishing and maintaining a commercially reasonable information security program that is designed to: (i) ensure the security and confidentiality of the Customer Content; (ii) protect against any anticipated threats or hazards to the security or integrity of the Customer Content; (iii) protect against unauthorized access to, or use of, the Customer Content; and (iv) ensure that all subcontractors of GitLab, if any, comply with all of the foregoing. In no case shall the safeguards of GitLab's information security program be less stringent than the information security safeguards used by GitLab to protect its own commercially sensitive data. Customer shall use commercially reasonable security and anti-virus measures when accessing and using the Software and to prevent unauthorized access to, or use of the Software, and notify GitLab promptly of any such unauthorized access or use of which it becomes aware.

14.2 With respect to the protection of information, the GitLab Privacy Policy located on GitLab's Website, and attached hereto as Appendix 3, as may be non-materially updated from time to time, shall apply. If this Agreement is entered into on behalf of an Enterprise, the terms of the data processing addendum attached hereto as Appendix 4 ("DPA"), as may be non-materially updated from time to time, hereby incorporated by reference and shall apply to the extent Customer Content includes Personal Data, as defined in the DPA. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by GitLab, the Standard Contractual Clauses shall apply, as further set forth in the DPA. For the purposes of the Standard Contractual Clauses, Customer and its applicable Affiliates are each the data exporter, and Customer's acceptance of this Agreement, and an applicable Affiliate's execution of an Order Form, shall be treated as its execution of the Standard Contractual Clauses.

14.3 The parties acknowledge and agree that: (i) the Software is not designed for the purpose(s) of storing, processing, compiling or transmitting Sensitive Data (as defined herein), and (ii) Customer shall not use the Software, or otherwise provide to GitLab without prior written consent, Sensitive Data under this Agreement. "Sensitive Data" means: (i) special categories of data enumerated in European Union Regulation 2016/679, Article 9(1) or any successor legislation; (ii) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act (as amended and supplemented) ("HIPAA"); (iii) credit, debit, or other payment card data or financial account information, including bank account numbers or other personally identifiable financial information; (iv) social security numbers, driver's license numbers, or other government identification numbers; (v) other information subject to regulation or protection under specific laws such as the Children's Online Privacy Protection Act or Gramm-Leach-Bliley Act ("GLBA") (or related rules or regulations); or (vi) any data similar to the above protected under foreign or domestic laws. Customer further acknowledges that the Software and related features are not intended to meet any legal obligations for these uses, including HIPAA and GLBA requirements, and that GitLab is not a Business Associate as defined under HIPAA. Therefore, notwithstanding anything else in this Agreement, GitLab has no liability for Sensitive Data processed in connection with Customer's use of the Software.

## **15. MISCELLANEOUS**

15.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

15.2 This Agreement is not assignable, transferable or sublicensable by either party without the other party's prior written consent, not to be unreasonably withheld or delayed; provided that GitLab may seek to novate this Agreement in accordance with FAR 42.1204.

15.3 This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement. All waivers and modifications must be in a writing signed or otherwise agreed to by each party, except as otherwise provided herein.

15.4 No agency, partnership, joint venture, or employment is created as a result of this Agreement and neither party has any authority of any kind to bind the other in any respect whatsoever.

15.5 Equitable relief and the award of attorney's fees, costs, or interest are only allowable to the extent permitted by statute, law or rule.

15.6 All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; and upon receipt, if sent by certified or registered mail (return receipt requested), postage prepaid.

15.7 This Agreement will be governed by the Federal laws of the U.S.A. without regard to its conflict of laws provisions. The United Nations Convention on Contracts for the International Sale of Goods is expressly disclaimed by the Parties with respect to this Agreement and the transactions contemplated hereby.

**GitLab Federal, LLC**

**Signature:**

**Printed Name:**

**Title:**

**Date:**

**Customer:** \_\_\_\_\_

**Signature:**

**Printed Name:**

**Title:**

**Date:**

## APPENDIX 1: GitLab Subscriptions

Fees for the Subscriptions are based upon the number of Users and the applicable level of support and/or functionality of the Software, as set forth in the table below. In the event Customer does not reasonably comply with written specifications or instructions from GitLab’s service engineers, regarding any support issue or request (including without limitation, failure to make backups of Customer Content or versions of Software) (each, a “Support Issue”), GitLab may cease its support obligations to Customer with respect to such Support Issue upon fifteen (15) days written notice and Customer’s inability to cure such noncompliance within the notice period.

### SUBSCRIPTIONS AND LEVELS OF SUPPORT

Subscription*	Level of Support ( <i>First Response Time</i> )	Support Details
Free ( <i>Formerly "Core" or "Free"</i> )	GitLab Community Forum	
Starter ( <i>F.K.A "Basic" or "Bronze"</i> )	GitLab Standard Support	24 x 5 Support Next business day response (24 hour SLA) Submit Tickets at <a href="https://support.gitlab.com">https://support.gitlab.com</a>
Premium ( <i>Formerly Premium or Silver</i> )	Priority Support (Based upon Support Impact **)	See Priority Support Overview <a href="https://support.gitlab.com">https://support.gitlab.com</a>
Ultimate ( <i>Formerly Gold or Ultimate</i> )	Priority Support (Based upon Support Impact**)	See Priority Support Overview <a href="https://support.gitlab.com">https://support.gitlab.com</a>

\*Note: Subscription names are subject to change, however, the applicable Subscription for that tier shall remain the same during a Subscription Term.

\*\*Support Impact categories are defined on GitLab’s Website.

**PRIORITY SUPPORT OVERVIEW:** Please see GitLab’s Website.

### CUSTOMER SUCCESS SERVICES

Customer Success Services include additional assistance with respect to Customer’s use of the GitLab Software. Customer Success Services are provided at no charge, an overview of the Customer Success Services can be found at GitLab’s Website. In order to receive Customer Success Service(s), Customer understands that additional data and information (“Operational Data”) will be collected. An overview of Operational Data can be found on GitLab’s Website.

## **APPENDIX 2: Software as a Service (SaaS) Offering**

With respect to Customer's purchase and/or use of the SaaS Software, the following additional terms shall apply.

### **AVAILABILITY**

Availability to the SaaS Software will be measured, and reported on, by GitLab using instrumentation and observation tools specifically designed to provide a representative measure of service availability. Recent status, references to availability measurement definition, and historical reporting will be available at or linked from the GitLab system status site located on GitLab's Website.

### **RESILIENCY**

GitLab will architect and maintain an underlying cloud infrastructure with commercially reasonable resiliency for all data, compute, and network services. At a minimum, GitLab will maintain the highest documented level of "GitLab Reference Architecture" as detailed on GitLab's Website.

### **BACKUPS**

GitLab will maintain a commercially reasonable system of data backup process and technology to ensure that primary data sources remain recoverable in the event of various system failures.

### **MONITORING AND INCIDENT RESPONSE**

GitLab will employ a system of instrumentation and observation tools to ensure that system behavior which may limit use of the SaaS Software is detected and announced. GitLab will also employ industry reasonable practices to maintain appropriate engineering personnel availability for the purposes of incident response(s).

### **UPDATES AND UPGRADES**

GitLab will update the SaaS Software as updates are available and when reasonably practical to implement said updates. Update timing and process will remain at GitLab's discretion.

### **SCHEDULED SYSTEM MAINTENANCE**

GitLab will occasionally perform scheduled system maintenance which requires limits to the use of part or all of the SaaS Software features, or significantly reduces features and functions during the scheduled system maintenance period. GitLab will provide ten (10) business days notice for all scheduled system maintenance activities. GitLab will take a proactive approach to minimizing the need for such maintenance and will limit scheduled system maintenance to less than four (4) hours per calendar month. Notwithstanding the foregoing, in the event of emergency or urgent issue which may negatively impact GitLab's customers, GitLab has the right to carry out unscheduled maintenance to remedy such instance(s). For the avoidance of doubt, such unscheduled maintenance shall: (i) be limited to only those issues which may negatively impact customers; and (ii) will be carried out in such a manner to provide for the least amount of disruption to customers.

### **SUSPENSION OF SERVICE**

GitLab reserves the right to suspend service to the SaaS Software if: (i) Customer exceeds set application limits, or (ii) requests or usage deemed malicious in nature is identified to be sourced from Customer accounts, personnel, or systems.

## APPENDIX 3: GitLab Privacy Policy

### Introduction

At GitLab, we take the privacy and security of your information seriously. This privacy policy ("Privacy Policy") will explain how GitLab B.V. and GitLab, Inc. ("GitLab", "we", "our", "us") handles your personal data. "Personal Data," as used in this Privacy Policy, is information that identifies or can reasonably be linked directly or indirectly to an identifiable person. The privacy practices and standards detailed in this Privacy Policy apply to all data subjects globally, unless specifically noted otherwise. In particular, this Privacy Policy will touch on the following sections:

- [What Personal Data does GitLab collect about me?](#)
- [What Personal Data is Not Collected by GitLab?](#)
- [How does GitLab use my Personal Data?](#)
- [With Whom does GitLab share my Personal Data?](#)
- [How does GitLab Secure my Personal Data?](#)
- [What are my rights and choices regarding Personal Data?](#)
- [California Privacy Rights](#)
- [Other important privacy information](#)

This Privacy Policy applies to the GitLab websites ("Websites"), GitLab.com ("SaaS"), Self-managed ("Self-managed"), and additional software products and services; collectively "Services."

### What Personal Data does GitLab collect about me?

The categories of Personal Data collected by GitLab change depending on the Services you use and whether those Services are free or paid. We have described below which Services correlate with the processing in each Personal Data category.

#### Information You Provide Directly

We collect the Personal Data you provide to us, for example:

*Account Information:* When you register for an account with GitLab, we collect information that identifies you such as your name, username, email address and password. This is collected for free and paid users of the SaaS product.

*Profile Information:* We collect information that you voluntarily provide in your user profile; this may include your public avatar (which may be a photo), additional email addresses, company/organization name, job title, country, social media handles, and biography. Please note this information may be visible to other users of the Services and to the public depending on the privacy setting you apply. This is collected for free and paid users of the SaaS product.

*Payment Information:* If you purchase a paid subscription from GitLab, we will collect payment information from you that may include your name, billing address and credit card or bank information. We may also use your credit card information to verify your identity and prevent abuse of our pipelines. Please note that GitLab does not directly process or store your entire credit card number, but we do direct that information to our third-party payment processors for processing. This is collected for paid users of the Self-managed and SaaS products.

*Marketing Contact Information:* If you request GitLab to contact you, or sign up for marketing materials or events, GitLab may collect information such as name, address, email address, telephone number, company name, and size of company. This may be collected through the Websites as well as through the use of the Self-managed or SaaS products.

*Licensee Information:* We collect licensee name, email address, and similar information associated with the individual that receives a license key for the paid users of the Self-managed product.

*Content you provide through the use of the Services:* Examples of content we collect and store include but are not limited to: the summary and description added to an issue, your repositories, commits, project contributions, profile metadata, activity data, and comments. Content also includes any code, files and links you upload to the Services. This is collected for the free and paid users of the SaaS product.

*Customer Support and Professional Services:* If you contact GitLab customer support or receive professional services, we will collect information about you related to your account and to the requests you are making or the services being provided. Customer Support information is collected through the Websites, such as the [GitLab Community Forum](#) and the [GitLab Support Portal](#).

*Call Recordings:* We may record and transcribe sales calls hosted on various videoconferencing technologies to enable our sales and support teams to share conversational insights, create training and presentations, and improve their internal processes.

*Other Content You Submit:* We may also collect other content that you submit to our Services. For example: feedback, comments and blog posts, or when you participate in any interactive features, surveys, contests, promotions, prize draws, activities or events. When you participate in interactive channels, we may collect and process information for demographic analysis. Such collection is not tied to any specific products, but may be collected through the Websites.

### **Information About Your Use of the Services We Collect Automatically**

We may collect certain Personal Data automatically through your use of the Services, for example:

*Device Information and Identifiers:* When you access and use our Services, we automatically collect information about your device, which may include: device type, your device operating system, browser type and version, language preference, IP address, hardware identifiers, and mobile IDs. This information may be collected through any use of the Services.

*Subscription Data:* We may automatically collect information about the number of active users, licensing timetables, historical user count, and IP address. This is collected for paid Self-managed and SaaS instances. Subscription Data details can be found in the [Metrics Dictionary](#).

*Services Usage Data:* Services Usage Data is broken into two categories: Optional Data and Operational Data. Optional Data is aggregated metrics regarding activity and feature usage that provide insights into the success of stages and features. Operational Data is aggregated metrics that track how value is delivered through the use of the Services and provide insights into optimal customer implementation. Both categories of Services Usage Data can be tied to the instance hostname, but the information does not contain any other individual user data. This is collected for the free and paid users of the Self-managed and SaaS products. For more information about the data collected and how to set your preferences, please visit [Services Usage Data](#).

*Events Data:* In addition to Services Usage Data, GitLab also uses event analytics, such as browsing duration, page clicks and page views, in a pseudonymized form to gain insights into end-to-end user behavior. This is collected for SaaS and Self-managed products.

*Website Usage Data:* When you visit our Websites, we automatically log information about how you interact with the sites, such as the referring site, date and time of visit, and the pages you have viewed or links you have clicked.

*Cookies and Similar Tracking Technologies:* GitLab uses cookies and similar technologies to provide functionality, such as storing your settings, and to recognize you as you use our Services. In addition, we use cookies to gather information to provide interest-based advertising which is tailored to you based on your online activity. Please review our [Cookie Policy](#) to learn about our practices and the controls we provide you.

*Email marketing:* When we send you emails, they may include technology such as a web beacon, that tells us your device type, email client, and whether you have received and opened an email, or clicked on any links contained in the email.

*Buttons, tools, and content from other companies:* The Services may include links or buttons to third-party services such as Facebook and Twitter. We may collect information about your use of these features. In addition, when you see or interact with these buttons, tools, or content, some information from your browser may automatically be sent to the other company. Please read that company's privacy policy for more information.

### **Information from Third-Parties and Partners**

We may collect Personal Data from other parties in the following ways:

*Vendors and Partners:* We may receive information about you from third-parties such as vendors, resellers, partners, or affiliates. For example, we receive information from our resellers about you and your orders, or we may supplement the data we collect with demographic information licensed from third-parties in order to personalize the Services and our offers to you. Likewise, our sales, marketing, and recruiting teams may receive access to third-party databases containing information to enrich business contacts and other corporate data, or we may receive social listening data from companies that monitor public posts.

*Third-Party sign-in services:* GitLab allows you to sign up for/in to our Services using third-party accounts, such as Facebook or Google. When you give permission for this to happen, GitLab will receive information about you from your third-party account, such as name, email address, location and demographic information.

*Other users of the Services:* Other users of the Services may provide information about you when they submit issues and comments, or we may receive information when you are designated as a representative or administrator on your company's account.

When you are asked to provide personal data, you may decline. And you may use web browser or operating system controls to prevent certain types of automatic data collection. But if you choose not to provide or allow information that is necessary for certain products or features, those products or features may not be available or function correctly.

### **What Personal Data is Not Collected by GitLab?**

GitLab does not intentionally collect sensitive Personal Data, such as social security numbers, genetic data, health information, or religious information. Although GitLab does not request or intentionally collect any sensitive Personal Data, we realize that users might store this kind of information in a GitLab repository.

GitLab does not intentionally collect the Personal Data of individuals that are stored in users' repositories or other free-form content inputs. If Personal Data is stored in a user repository then the repository owner is responsible for its processing.

If you are a child under the age of 13, you may not have an account. With the exception of Educational Licenses, GitLab does not knowingly collect information from, or direct any of our Services to, children under 13. If we learn or have reason to suspect that a user is under the age of 13, we will close the child's account.

### **How Does GitLab use my Personal Data?**

GitLab uses your Personal Data for the following purposes:

- To create your account, identify and authenticate your access to the Services and provide you with the Services you have requested;
- To process your payment for the Services you have purchased;
- To understand how our Services are used and to improve our Services;
- To provide personalized experiences;
- To conduct user research and development;
- To send you important information about the Services;
- To send you information you have requested;

- To send you advertising, marketing content, offers, promotions, newsletters, surveys or other information;
- To provide you a forum to comment on or discuss the Services;
- To create digital productions and manage events;
- To provide trainings and learning opportunities;
- To enable partners to register and track deals;
- To provide workload and code review recommendations through machine-learning;
- To respond to your requests for customer support;
- To improve the security of and troubleshoot our Services, as necessary to perform the contract governing your use of our applications or to communicate with you;
- To detect, prevent, or otherwise address fraud and abuse to protect you, GitLab, and third-parties;
- To enforce the legal terms that govern our Services;
- To comply with our legal obligations;
- To protect the rights, safety and property of GitLab, you, or any third-party; and
- For other purposes, for which we obtain your consent.

#### **Legal Basis for the Processing of your Personal Data**

When our processing is subject to international laws, including but not limited to the General Data Protection Regulation ("GDPR") that governs individuals located in the European Economic Area ("EEA"), we collect and process your Personal Data using one or more of the following legal bases set out by applicable law:

*Performance of a contract:* We use your Personal Data to provide the Services you have subscribed to, and to complete and administer the contract you have entered into with GitLab, which includes the [Subscription Agreement](#), the [Website Terms of Use](#), and any agreement to process payment information.

*Legitimate Interests:* We use your Personal Data for our legitimate interests, such as to provide you with relevant content, communicate with business leads, improve our products and services, and for administrative, security, fraud prevention and legal purposes. You may object to the processing of your Personal Data for these purposes at any time.

*Consent:* We may use your Personal Data, with your consent, for specific purposes such as marketing, surveys, call recordings, and research. You may withdraw your consent for the specific purpose or object to the processing of your Personal Data at any time.

*Compliance with a Legal Obligation:* We may use your Personal Data in connection with legal claims, regulatory compliance, and audits.

#### **With Whom does GitLab share my Personal Data?**

We may share each of the categories of Personal Data we collect with the types of third-parties described below, for the following business purposes:

*Sharing with Users and the Public:* We may share your Personal Data with other users of the Services and with the public if you choose to make your SaaS Profile public. You have control over what information is public. To change your settings, go to [User Settings](#) in your profile. You should also be aware that any information you share as part of a project, blog, website etc. may be publicly available and you should consider this carefully when interacting with the Services.

*Sharing with Managed Accounts and Administrators:* If you have created a GitLab account with your corporate email address, we may share your Personal Data with your Company if your Company enters into a commercial relationship with GitLab. If this happens, then your use of the software and your account is subject to the terms and any data protection agreement between your Company and GitLab.

In the event you change the email address on your account from a corporate email address to a personal email address and, thereafter, your Company enters into a commercial relationship with GitLab, your Personal Data related to that account will not be shared with your Company. GitLab will not link an account to a Company based on retroactive use of a corporate email.

In addition, if you choose to become a member of a project, your username, email address, IP address, the date when access was granted, the date when access expires, and your access role will be shared with the group owners of that project.

*Sharing with Service Providers:* We share your Personal Data with our service providers. These are companies who provide services on our behalf, such as hosting our Services, marketing, advertising, social, analytics, support ticketing, credit card processing, security and other such similar services. These companies are subject to contractual requirements that govern the security and confidentiality of your information.

For example, we use analytics providers, such as Google Analytics, to help us understand the operation and performance of our Services. To learn about how Google uses and shares data it collects through its services, please visit <https://www.google.com/policies/privacy/partners/>. In addition, please visit our [Sub-Processors page](#) to see the list of our Sub-Processors that we use in order to provide customer support and host the Services.

*Sharing with Partners and Resellers:* GitLab works with third-parties who provide sales, consulting, support and technical services for our Services. Where permitted and with your consent (if required), we may share your data with these partners and resellers.

*Sharing with Affiliated Companies:* GitLab will share information collected with [companies owned and operated by us](#).

*Sharing for Fraud and Prevention Abuse:* We may share your information when we have a good faith belief that the disclosure is necessary to prevent fraud, abuse of our services, defend against attacks, and to protect the safety of GitLab and our users.

*Law Enforcement:* GitLab may disclose Personal Data or other information we collect about you to law enforcement if required in response to a valid subpoena, court order, search warrant, a similar government order, or when we believe in good faith that disclosure is necessary to comply with our legal obligations, to protect our property or rights, or those of third-parties or the public at large.

*Merger or Acquisition:* We may share your Personal Data if we are involved in a merger, sale, or acquisition of corporate entities or business units. If any such change of ownership happens, we will ensure that it is under terms that preserve the confidentiality of your Personal Data, and we will notify you on our website or by email before any transfer of your Personal Data.

### **Sharing Personal Data across national borders**

Our Services are hosted in the United States and information we collect will be stored and processed on our servers in the United States. Our employees, contractors, affiliated organizations, service providers, and sub-processors that process Personal Data may be located in the United States or other countries outside of your home country. If you reside in the EEA, United Kingdom, or Switzerland, and we transfer information about you to a jurisdiction that has not been found by the European Commission to have adequate data protections, we will use available safeguards and legal mechanisms to help ensure your rights and protections, including using Standard Contractual Clauses or obtaining your consent.

### **How does GitLab Secure my Personal Data?**

We work hard to protect your Personal Data. We employ administrative, technical, and physical security controls where appropriate, to protect your information. For more information on our security practices please see: [Technical and Organizational Security Measures for GitLab.com](#).

### **Data Retention**

In order to protect your Personal Data, GitLab will only retain your Personal Data for as long as your account is active or as needed to perform our contractual obligations, provide you the Services, comply with legal obligations, resolve disputes, preserve legal rights, or enforce our agreements.

GitLab reserves the right to delete inactive accounts, projects, namespaces, and associated content. GitLab may deem an account, project, or namespace inactive based on various criteria, including, but not limited to, the account creation date, the last time there was a valid log-in, and the date of the last contribution. If we plan to delete your account or projects, we will provide advance notice by sending a message to the email address registered to your account. GitLab encourages you to utilize your account on occasion to avoid the risk of being deemed inactive.

### **What are my rights and choices regarding Personal Data?**

You have the right to access, correct, restrict or delete your Personal Data, and to port your Personal Data to another company. While these rights may vary by jurisdiction, GitLab provides you with the same rights and choices, no matter where you live. We provide these rights free of charge unless your requests are manifestly unfounded and excessive.

You may exercise your choices and rights as follows:

*To opt out of email marketing:* You may opt-out of email marketing by clicking the “unsubscribe” link located at the bottom of any marketing email you receive or by visiting our [preference center](#) and unsubscribing. You may continue to receive transactional email messages about your account and the Service after you have unsubscribed.

*To opt-out of Interest-based advertising:* If you wish to opt-out of interest-based advertising, please visit the Cookie Policy to see your options.

*Request a copy of your information:* You may [request a copy of the Personal Data](#) that GitLab has about you.

*Update your Information:* If you already have an account, you may access, update, or alter your user profile information by logging into your account and updating profile settings.

*To delete your Account:* If you only want to delete your SaaS account, you may do so by logging into your account and going to the “Delete my Account” option in your profile settings. If your intention is to delete your Personal Data across all systems, including your account, you need to fill out a [Personal Data Request Form](#) and select "Account Deletion (full)" in the "Request Type" dropdown menu. If your account is tied to a Company that has entered into a commercial relationship with GitLab, you will have to ask your Company administrator to remove your account from that corporate namespace before we can delete it. Once your account is no longer associated with that corporate namespace, GitLab will process your deletion request according to the process stated herein.

Please note that due to the open source nature of our Services, we may retain limited Personal Data indefinitely in order to provide a transactional history. For example, if you provide your information in connection with a blog post or comment, we may display that information even if you have deleted your account as we do not automatically delete community posts. Also, if you contribute to a public project (not owned by GitLab), and you provide your Personal Data in connection with that contribution, your Personal Data will be embedded and publicly displayed with your contribution, and we will not be able to delete or erase it because doing so would break the project.

One exception to embedded information in a public project occurs when your Personal Data is added by you or someone else to the comments section of a public project. In such a case, your Personal Data will be redacted since removing this information from only the comments section will not break the project.

If you contribute to a GitLab owned project by commenting in, or creating an issue or merge request and you provide your Personal Data in connection with that contribution, your Personal Data associated with your contribution will be deleted and attributed to a ghost user. However, please note that if the content of the contribution contains Personal Data, this information would remain and you will need to submit a specific request to have this information deleted.

*To port your projects:* You may port your projects by either using the [Export functionality](#) provided within the SaaS product which will also include all metadata, or by cloning your repositories. To port your profile information, you may use the [API](#).

*To inform your Supervisory Authority:* In the unlikely event you disagree with our handling of your request, you have the right to file a complaint with the competent supervisory authority in your jurisdiction.

### **California Privacy Rights**

If you are a California resident, please visit the [GitLab California Privacy Notice](#) for a specific description of your privacy rights and collection practices under the California Consumer Privacy Act.

### **Other important privacy information**

#### **Policy Changes**

GitLab may change its Privacy Policy from time to time. When we do, we will update the date at the top of this Policy. If we decide to make a significant change to our Privacy Policy, we will post a notice of the update on the homepage of our Website. We may also provide notification via email of any material changes to our Privacy Policy.

#### **Contact Us**

Your information is controlled by GitLab B.V. and GitLab Inc. If you have questions or concerns about the way we are handling your Personal Data, please email us with the subject line "Privacy Concern" at [DPO@gitlab.com](mailto:DPO@gitlab.com).

#### **APPENDIX 4: GitLab Data Processing Addendum**

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of the GitLab Data Processing Addendum, Standard Contractual Clauses, EU Law including, but not limited to the GDPR, or law of an EU Member State that is inconsistent with the Federal law of the United States.

## 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 EU Member State laws implementing the GDPR, (b) California Consumer Privacy Act of 2018 (“CCPA”) and the California Attorney General Regulations thereof, 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 used in the Service.
  - e. **“Process”, “Processing”, “Processor”, and “Controller”** shall have the meaning as defined under GDPR.
  - f. **“Service(s)”** means the software and services licensed under the Subscription Agreement.
  - g. **“Standard Contractual Clauses”** means Exhibit B located at [https://gitlab.com/gitlab-com/legal-and-compliance/-/raw/master/Exhibit B Standard Contractual Clauses 5 25 22.pdf](https://gitlab.com/gitlab-com/legal-and-compliance/-/raw/master/Exhibit%20B%20Standard%20Contractual%20Clauses%205%2022.pdf), forming part of this DPA pursuant to the European Commission Implementing Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of

the Council, as well as the Switzerland Addendum and the United Kingdom Addendum, which shall prescribe specific amendments to the standard contractual clauses as set forth for application in each of those respective countries. “**Module One**”, “**Module Two**”, and “**Module Three**” shall refer to the respective Modules set forth therein and the relevant terms thereof.

- h. “**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 to the extent Module One or Section 18.a. of the DPA applies.
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 subjects is as set forth in Exhibit A. To the extent the Standard Contractual Clauses, Article 28 of the GDPR, or Article 75 of the UK Data Protection Act apply, further information regarding the nature and purpose of the Processing is as set forth in Exhibit B.
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 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.** 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. 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, 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. 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; and
  - 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 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/> 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 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.
  - i. To the extent applicable for Customers 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 Google LLC and Amazon Web Services, Inc. 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 Products, 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 and objection 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. The parties agree that the Standard Contractual Clauses in Exhibit B will only apply to Personal Data that is transferred outside of the European Economic Area, United Kingdom, or Switzerland to a country that does not ensure an adequate level of protection for Personal Data (as described in the GDPR).
- b. When GitLab, acting as a Controller for the Processing described in Section 18.a., Module One of the Standard Contractual Clauses will apply to the Personal Data transferred by Customer.
- c. When GitLab is acting as a Processor and Customer is acting as a Controller, Module Two of the Standard Contractual Clauses will apply to the Personal Data transferred by Customer.
- d. When GitLab is acting as a Processor and Customer is acting as a Processor, Module Three of the Standard Contractual Clauses will apply to the Personal Data transferred by Customer.
- e. 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.** The following applies where GitLab is processing Personal Data that is within the scope of CCPA. The parties agree that GitLab is a 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. Subject to exceptions under CCPA, GitLab agrees that it will not (a) sell Personal Data, or (b) retain,

use or disclose Personal Data (i) for any purpose other than providing the Services, or (ii) outside its direct business relationship with Customer.

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. 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.

## **EXHIBIT A – DETAILS OF THE PROCESSING**

The following applies where GitLab is a Processor.

### **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