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.


   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, attached to and 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. “**Module One**, **Module Two**, **Module Three**” and “**Module Four**”
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 or Article 28 of the GDPR 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 fulfill 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.

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.** The parties agree that the Standard Contractual Clauses in Exhibit B will 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). 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. GitLab agrees to adopt any supplementary or substitute terms that are deemed mandatory by regulators in the United Kingdom or Switzerland.
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 Section18.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
SECTION I

Clause 1 – Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)

have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

(b) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(c) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 – Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU)

---

1 Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.
2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 – Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 – Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 – Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 – Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose Limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject’s prior consent;
(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

### 8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### 8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage Limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter ‘personal data breach’). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain:

1) A description of the nature of the breach (including, where possible, categories of data subject and categories of personal data affected).

2 This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.
and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive Data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter ‘sensitive data’), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union\(^3\) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

\(^3\) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing
(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data
Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data

4 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.\(^5\)

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

---

\(^5\) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.
On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of
the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In
addition, the data may only be disclosed to a third party located outside the European Union\textsuperscript{6} (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

\textbf{8.9 Documentation and compliance}

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

\textsuperscript{6} The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.
(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the

---

7 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the controller’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s or controller’s request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

8 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter ‘automated decision’), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

---

9 That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.
(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

**MODULE TWO: Transfer controller to processor**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

**MODULE THREE: Transfer processor to processor**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter

**Clause 11 – Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**Clause 12 - Liability**

**MODULE ONE: Transfer controller to controller**
(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 – Supervision

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.
SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;\(^{10}\)

\(^{10}\) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). For Module Three: The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, and, for Module Three, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by, for Module Three: the controller, or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

15.1 Notification
(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

For Module Three: The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). For Module Three: The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal.
When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. For Module Three: The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority, for Module Three: and the controller, of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
(d) *For Modules One, Two and Three:* Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17 - Governing law**

MODULE ONE: Transfer controller to controller  
MODULE TWO: Transfer controller to processor  
MODULE THREE: Transfer processor to processor  

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

**Clause 18 - Choice of forum and jurisdiction**

MODULE ONE: Transfer controller to controller  
MODULE TWO: Transfer controller to processor  
MODULE THREE: Transfer processor to processor  

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.
SWITZERLAND ANNEX TO THE STANDARD CONTRACTUAL CLAUSES

1) The term “Member State” as used in Clause 18.c of the Standard Contractual Clauses shall include Switzerland in cases where Switzerland is the habitual place of residence for data subjects aspiring to bring a legal proceeding under the Clauses.

2) The Standard Contractual Clauses shall also protect the data of legal entities in Switzerland until the entry into force of a revised Swiss Federal Act on Data Protection that does not afford such protections to legal entities.
ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

Data exporter(s): (Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union)

1. Name: Exporter is the entity identified as Customer or Company on any combination of an Order Form, Subscription Agreement, or GitLab.com website purchase.

Address: As listed by Customer in the website purchase portal or as identified on any combination of an Order Form or Subscription Agreement.

Contact person’s name, position and contact details: Exporter’s account administrator or Data Protection Officer, as determined by the Exporter.

Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B. Module One

Signature and date: Signed by Exporter’s representative as of the date of acceptance via purchase through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed, and in each case, where this DPA is incorporated by reference.

Role (controller/processor): Controller

Data importer(s): (Identity and contact details of the data importer(s), including any contact person with responsibility for data protection)

1. Name: Gitlab Inc.

Address: 268 Bush St 350, San Francisco, CA, 94104-3503, USA

Contact person’s name, position and contact details: Data Protection Officer, DPO@gitlab.com

Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B. Module One

Signature and date:

Role (controller/processor): Controller
MODULE TWO: Transfer controller to processor

Data exporter(s): (Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union)

1. Name: Exporter is the entity identified as Customer or Company on any combination of an Order Form, Subscription Agreement, or GitLab.com website purchase.

   Address: As listed by Customer in the website purchase portal or as identified on any combination of an Order Form or Subscription Agreement.

   Contact person’s name, position and contact details: Exporter’s account administrator or Data Protection Officer, as determined by the Exporter.

   Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B. Module Two

   Signature and date: Signed by Exporter’s representative as of the date of acceptance via purchase through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed, and in each case, where this DPA is incorporated by reference.

   Role (controller/processor): Controller

Data importer(s): (Identity and contact details of the data importer(s), including any contact person with responsibility for data protection)

1. Name: Gitlab Inc.

   Address: 268 Bush St 350, San Francisco, CA, 94104-3503, USA

   Contact person’s name, position and contact details: Data Protection Officer, DPO@gitlab.com

   Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B. Module Two

   Signature and date: Signed by Exporter’s representative as of the date of acceptance via purchase through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed, and in each case, where this DPA is incorporated by reference.

   Role (controller/processor): Processor

MODULE THREE: Transfer processor to processor

DocuSign Envelope ID: 0A8F6048-F0B9-490E-8C64-C69E6CF4B49D
Data exporter(s): (Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union)

1. Name: Exporter is the entity identified as Customer or Company on any combination of an Order Form, Subscription Agreement, or GitLab.com website purchase.

   Address: As listed by Customer in the website purchase portal or as identified on any combination of an Order Form or Subscription Agreement.

   Contact person’s name, position and contact details: Exporter’s account administrator or Data Protection Officer, as determined by the Exporter.

   Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B. Module Three

   Signature and date: Signed by Exporter’s representative as of the date of acceptance via purchase through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed, and in each case, where this DPA is incorporated by reference.

   Role (controller/processor): Processor

Data importer(s): (Identity and contact details of the data importer(s), including any contact person with responsibility for data protection)

1. Name: Gitlab Inc.

   Address: 268 Bush St 350, San Francisco, CA, 94104-3503, USA

   Contact person’s name, position and contact details: Data Protection Officer, DPO@gitlab.com

   Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B. Module Three

   Signature and date: Signed by Exporter’s representative as of the date of acceptance via purchase through GitLab.com, or the date an Order Form or Subscription Agreement is fully executed, and in each case, where this DPA is incorporated by reference.

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

Categories of data subjects whose personal data is transferred
Categories of data subjects transferred where GitLab acts as a controller may include, but is not limited to the following:

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

**Categories of personal data transferred**

Categories of Personal Data transferred where GitLab acts as a controller may include, but is not limited to the following:

- Account Management Information, such as license data, historical user data, and account administrator contact information
- Billing Information, such as Customer’s billing address, billing contact, and credit card or banking information
- Product Development Information, such as service usage and activity data
- Security and Fraud Prevention Information, such as log data, device data and IP address

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

GitLab does not collect sensitive Personal Data for the purposes as described in this Annex I.B., Module One.

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

Personal Data is transferred at a frequency appropriate to the nature of the processing and can be one-off or continuous.

**Nature of the processing**

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

**Purpose(s) of the data transfer and further processing**
Purposes of the data transfer are to allow GitLab entities to provide the Services, which are hosted and processed on servers in the United States. In addition, GitLab employees are located in the United States and other countries outside of the European Economic Area.

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

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

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

Personal Data transferred under this Module will be controlled by GitLab Inc.

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Categories of data subjects transferred where GitLab acts as a processor may include, but is not limited to the following:

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

Categories of personal data transferred

Categories of Personal Data transferred where GitLab acts as a processor may include, but is not limited to the following:

- Account Information, such as name, username, email address, and password
- Profile Information, such as name, public avatar or photo, employer, email address, job title, address, social media handles, and biography
- Contact information, such as name, address, email address, and telephone
- Content provided through the use of the Services, such as repositories, issues, commits, project contributions, and comments
- Customer Support Information, such as the request you are making or the services being provided
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

GitLab does not intentionally collect sensitive Personal Data, such as genetic data, health information, or religious information. Although GitLab does not request or intentionally collect any sensitive Personal Data, Customers might submit such data in connection with their use of GitLab Services.

Security measures for all Personal Data, including Sensitive Data, is subject to strict purpose limitations, access restrictions (including access only for staff having followed specialised training), record-keeping of access to the data, restrictions for onward transfers along with additional security measures described in Annex II.

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

Personal Data is transferred at a frequency appropriate to the nature of the processing and can be one-off or continuous.

Nature of the processing

The processing relates to Customers’ use of Gitlab’s SaaS and Self-managed products and services for purposes determined and controlled by Customers in their sole discretion.

Purpose(s) of the data transfer and further processing

Purposes of the data transfer are to allow GitLab entities to provide the Services, which are hosted and processed on servers in the United States. In addition, GitLab employees and sub-processors are located in the United States or other countries outside of the European Economic Area.

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

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

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.
GitLab’s sub-processor importers provide cloud hosting and search functionality services and perform these sub-processing activities in order for GitLab to provide the Services to Customer.

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

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

Categories of data subjects transferred where GitLab acts as a sub-processor may include, but is not limited to the following:

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

Categories of personal data transferred

Categories of Personal Data transferred where GitLab acts as a sub-processor may include, but is not limited to the following:

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

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
GitLab does not intentionally collect sensitive Personal Data, such as genetic data, health information, or religious information. Although GitLab does not request or intentionally collect any sensitive Personal Data, Customers might submit such data in connection with their use of GitLab Services.

Security measures for all Personal Data, including Sensitive Data, is subject to strict purpose limitations, access restrictions (including access only for staff having followed specialised training), record-keeping of access to the data, restrictions for onward transfers along with additional security measures described in Annex II.

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

Personal Data is transferred at a frequency appropriate to the nature of the processing and can be one-off or continuous.

**Nature of the processing**

The processing relates to Customer’s use of Gitlab’s SaaS and Self-managed products and services for purposes determined by the controlling entity for which Customer is processing the Personal Data.

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

Purposes of the data transfer are to allow GitLab entities to provide the Services, which are hosted and processed on servers in the United States. In addition, GitLab employees and sub-processors are located in the United States or other countries outside of the European Economic Area.

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

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

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

GitLab’s sub-processor importers provide cloud hosting and search functionality services and perform these sub-processing activities in order for GitLab to provide the Services to Customer.
Personal data will be retained for the period determined by the controller, including until termination of GitLab’s Subscriptions Agreement with Customer, subject to exceptions allowed by law and under the Subscription Agreement with Customer.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

The data exporter’s competent supervisory authority will be determined in accordance with the GDPR or Swiss Federal Act on Data Protection.
ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

GitLab security measures are described in details in its Customer Assurance Package found at: https://about.gitlab.com/security/cap/, as well as in its Technical and Organizational Security Measures for GitLab.com found at: https://about.gitlab.com/handbook/engineering/security/security-assurance/technical-and-organizational-measures.html. These documents include measures and processes regarding the following:

- Measures for role based access privileges, segregation of access and administrative access based on roles and responsibilities
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation
- Measures for the protection of data during transmission, such as encryption in transit
- Measures for the protection of data during storage, such as encryption at rest
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration, using a configuration management tool that establishes baseline standards
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring data quality
- Measures for ensuring limited data retention, such as the Records Retention Policy and the Records Retention & Disposal Schedule
- Measures for ensuring accountability
• Measures for allowing data portability and ensuring erasure, such as the Export Functionality and the “Delete My Account” option in the profile settings, or submitting a form request.

Sub-Processors will take security measures substantively the same as those above to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.