



## **Data Processing Agreement GitLabHost B.V.**

This Data Processing Agreement is an appendix to the agreement (hereinafter: **"Agreement"**) by and between Customer (hereinafter: **"Controller"**) and GitLabHost (hereinafter: **"Processor"**). Unless otherwise defined herein, capitalized terms and expressions in this Data Processing Agreement have the meaning set forth in the Agreement. Where the Agreement deviates from this Data Processing Agreement, this Data Processing Agreement prevails.

### **Article 1. Purposes of processing**

- 1.1. Processor hereby agrees under the terms of this Data Processing Agreement to process personal data on behalf of the Controller. Processing shall be done solely for the purpose of the Agreement, in particular for providing webhosting services, and all purposes compatible therewith or as determined jointly.
- 1.2. The personal data to be processed by Processor for the purposes as set out in the previous clause and the categories of data subjects involved are set out in [Appendix 1](#) to this Data Processing Agreement. Processor shall not process the personal data for any other purpose unless with Controller's consent. Controller shall inform Processor of any processing purposes to the extent not already mentioned in this Data Processing Agreement. Processor however is permitted to use personal data for quality assurance purposes, including surveys to data subjects and statistical research purposes regarding the quality of Processor's services.
- 1.3. All personal data processed on behalf of Controller shall remain the property of Controller and/or the data subjects in question.

### **Article 2. Allocation of responsibilities**

- 2.1. Processor shall make available IT facilities to be used by Controller for the purposes mentioned above. Processor shall not itself perform processing operations unless separately agreed otherwise.
- 2.2. Processor shall not process personal data processed on behalf of Controller other than on the relevant Controller documented instructions. For any other processing of personal data, including but not limited to any collection of personal data by Controller, processing for purposes not reported to Processor, processing by third parties and/or for other purposes, the Processor does not accept any responsibility.
- 2.3. Controller represents and warrants that the content, usage and instructions to process the personal data as meant in this Data Processing Agreement are lawful and do not violate any right of any (third) party.

### **Article 3. Processor obligations**

- 3.1. Regarding the processing operations referred to in the previous clause, Processor shall comply with all applicable legislation, including at least all data processing legislation such as the EU General Data Protection Regulation 2016/679 (hereinafter: GDPR).
- 3.2. Upon written request Processor shall inform Controller about any measures taken to comply with its obligations under this Data Processing Agreement.
- 3.3. All obligations for Processor under this Data Processing Agreement shall apply equally to any persons processing personal data under the supervision of Processor, including but not limited to employees in the broadest sense of the term.
- 3.4. Processor shall inform Controller if in its opinion an instruction of Controller would violate the legislation referred to in the first clause of this article.
- 3.5. Processor shall provide reasonable assistance to Controller in the context of any privacy impact assessments to be made by Controller.

### **Article 4. Data transfer**

- 4.1. Processor may process the personal data processed on behalf of Controller in any country within the European Union.
- 4.2. In addition Processor may transfer the personal data to a country outside the European Union, provided that country ensures an adequate level of protection

of personal data and complies with other obligations imposed on it under this Data Processing Agreement and the GDPR.

- 4.3. Processor shall report to Controller of the countries involved. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

#### **Article 5. Involvement of sub-processors**

- 5.1. Processor shall involve third parties in the processing under this Data Processing Agreement on the condition that such parties are reported in advance to the Controller. Controller may object to a specific third party if its involvement would reasonably be unacceptable to it.
- 5.2. Processor will make every reasonable effort to ensure that any third parties are bound to at least the same obligations as agreed between Controller and Processor.

#### **Article 6. Security**

- 6.1. Processor shall use reasonable efforts to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the processing operations involved, against loss or unlawful processing (in particular but limited to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed).
- 6.2. Processor does not warrant that the security is effective under all circumstances. If any security measure explicitly agreed in this Data Processing Agreement is missing, then Processor shall use best efforts to ensure a level of security appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6.3. Controller shall only provide personal data to Processor for processing if it has ensured that the required security measures have been taken. Controller is responsible for the parties compliance with these security measures.

## **Article 7. Notification and communication of data breaches**

7.1. Controller is responsible at all times for notification of any security breaches and/or personal data breaches (which are understood as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed) to the competent supervisory authority, and for communication of the same to data subjects. In order to enable Controller to comply with this legal requirement, Processor shall notify Controller within a reasonable period after becoming aware of an actual or threatened security or personal data breach.

7.2. Notification by Processor under the previous clause shall be made only for actual breaches with severe impact.

7.3. The notification shall include at least the fact that a breach has occurred. In addition, the notification shall:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data;
- breach, including, where appropriate, measures to mitigate its possible adverse effects.

## **Article 8. Data subjects rights**

8.1. In the event a data subject makes a request to exercise his or her legal rights under data protection legislation to Controller, Processor shall pass on such request to Controller, and Controller shall process the request. Processor may inform the data subject of this passing on.

## **Article 9. Confidentiality obligations**

- 9.1. Processor shall keep personal data that Processor receives from Controller and/or collects itself confidential, unless Controller has granted explicit permission to provide the information to third parties, the provision to third parties is reasonably necessary considering the nature of the assignment to Controller or the provision is legally required.

## **Article 10. Audit**

- 10.1. Controller has the right to have audits performed on Processor by an independent third party bound by confidentiality obligations to verify compliance with the security requirements, and all issues reasonably connected thereto.
- 10.2. This audit may be performed in case a substantiated allegation of misuse of personal data has arisen.
- 10.3. The audit findings shall be assessed by Processor and implemented if and to the extent deemed reasonable by Processor.
- 10.4. The costs of the audit shall be borne by Controller.

## **Article 11. Liability**

- 11.1. The liability of Processor for any damages as a result of a reputable failure to comply with this Data Processing Agreement, unlawful acts or otherwise, is excluded. To the extent such liability cannot be excluded, it is limited to direct damages per event (a sequence of successive events counting as one event), up to the amount received by the other Party for all activities under this Data Processing Agreement for the month prior to the event. Any liability of Processor for direct damages shall in any event never be more than € 1.000,00.
- 11.2. Any liability for indirect damages by Processor for indirect damages is excluded. Indirect damages are all damages that are not direct damages, and thus including but not limited to consequential damages, lost profits, missed savings, reductions in goodwill, standstill damages, failure to meet marketing requirements, damages as a result of using data prescribed by Controller, or loss, corruption or destruction of data.
- 11.3. Any liability shall exist only if the other party puts the responsible party on notice of default, including a reasonable term for addressing the failure. The notice shall

contain a (detailed) description of the failure to ensure that the responsible party has a reasonable opportunity to address the failure.

## **Article 12. Term and termination**

- 12.1. This Data Processing Agreement shall become effective upon the date this Data Processing Agreement is signed.
- 12.2. All notices, confirmations and other statements made by Controller in connection with this Data Processing Agreement shall be in writing and shall be sent per e-mail to Processor.
- 12.3. This Data Processing Agreement is entered into for the duration of the Agreement. Obligations with an enduring nature continue to exist between the parties.
- 12.4. Upon termination of the Data Processing Agreement, regardless of reason or manner, Processor shall - at the choice of Controller - return (in original format), delete and/or destroy the personal data processed on behalf of Controller .
- 12.5. This Data Processing Agreement may be changed in the same manner as the Agreement.

## **Appendix 1: Stipulation of personal data and data subjects**

### **Personal data**

Processor shall process the below personal data under the supervision of Controller, as specified in article 1 of the Data Processing Agreement:

- Names and addresses
- Telephone numbers
- Email addresses
- Visitor behavior
- IP addresses
- Social media accounts
- (Portrait) photos
- Civil service numbers
- Resumes
- Dates of birth
- Marital status
- Financial data
- Medical data

All personal data that customers collect and use using the provided webhosting services of the following categories of data subjects:

- Customers
- Personnel
- Suppliers
- Account holders
- Job candidates
- Website visitors
- Patients
- Leads and potential customers
- Members
- Renters

- All people from all data that customers collect and use using the provided webhosting services

*Controller represents and warrants that the description of personal data and categories of data subjects in this Appendix 1 is complete and accurate, and shall indemnify and hold harmless Process for all faults and claims that may arise from a violation of this representation and warranty.*