DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") amends and forms part of the Replit Terms and Conditions (the "**Agreement**") between Replit, Inc. ("**Company**") and you ("**Customer**"). This DPA prevails over any conflicting term of the Agreement.

1. **Definitions**

1.1. In this DPA:

a) "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in the GDPR;

b) "**Customer Personal Data**" means any Customer Data that constitutes Personal Data, the Processing of which is subject to Data Protection Law, for which Customer or Customer's customers are the Controller, and which is Processed by Company to provide the Services;

c) "**Data Protection Law**" means General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), and their national implementations in the European Economic Area ("**EEA**"), Switzerland and the United Kingdom, each as applicable, and as may be amended or replaced from time to time;

d) "**Data Subject Rights**" means Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making in accordance with Data Protection Law;

e) "**International Data Transfer**" means any transfer of Customer Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom;

f) "**Services**" means the services provided by Company to Customer under the Agreement;

g) "**Subprocessor**" means a Processor engaged by Company to Process Customer Personal Data; and

h) "**Standard Contractual Clauses**" means the clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5-18).

2. **Scope and applicability**

2.1. This DPA applies to Processing of Customer Personal Data by Company to provide the Services. The subject matter, nature and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects are set out in **Appendix 1**.

2.2. Customer is a Controller and appoints Company as a Processor on behalf of Customer. Customer is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.

2.3. Customer acknowledges that Company may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, product development, and compliance with law.

3. **Instructions**

3.1. Company will Process Customer Personal Data to provide the Services and in accordance with Customer's documented instructions. The Controller's instructions are documented in this DPA, the Agreement, and any applicable statement of work.

3.2. Unless prohibited by applicable law, Company will inform Customer if Company is subject to a legal obligation that requires Company to Process Customer Personal Data in contravention of Customer's documented instructions.

4. **Personnel**

4.1. Company will ensure that all personnel authorized to Process Customer Personal Data are subject to an obligation of confidentiality.

5. **Security and Personal Data Breaches**

5.1. 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,

Company will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in **Appendix 2**.

5.2. Company will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data. If Company's notification is delayed, it will be accompanied by reasons for the delay.

6. **Subprocessing**

6.1. Customer hereby authorizes Company to engage Subprocessors. A list of Company's current Subprocessors is [available at URL].

6.2. Company will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law. Company will notify Customer prior to any intended change to Subprocessors. Customer may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Company's notification of the intended change. Customer and Company will work together in good faith to address Customer's objection.

7. **Assistance**

7.1. Taking into account the nature of the Processing, and the information available to Company, Company will assist Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Customer's own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

8. **Audit**

8.1. Company will make available to Customer required information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested by Customer by at least sixty (60) days' notice, and no more than once per calendar year, and performed by an independent auditor as agreed upon by Customer and Company. Any such audit must be conducted during Company's business hours, without disruption to Company's operations, and in compliance with Company's confidentiality obligations.

8.2. Company will inform Customer if Company believes that Customer's instruction under **Section 8.1** infringes Data Protection Law. Company may suspend the audit or inspection, or withhold requested information until Customer has modified or confirmed the lawfulness of the instructions in writing.

9. **International Data Transfers**

9.1. Customer hereby authorizes Company to perform International Data Transfers to any country deemed adequate by the EU Commission; on the basis of appropriate safeguards in accordance with Data Protection Law; or pursuant to the Standard Contractual Clauses referred to in **Section 9.2**.

9.2. By signing this DPA, Customer and Company conclude the Standard Contractual Clauses, which are hereby incorporated into this DPA and completed as follows: the "data exporter" is Customer; the "data importer" is Company; the governing law in Clause 9 and Clause 11.3 of the Standard Contractual Clauses is the law of the country in which Customer is established; Appendix 1 and Appendix 2 to the Standard Contractual Clauses, are **Appendix 1** and **2** to this DPA respectively; and the optional indemnification clause is struck.

10. **Notifications**

10.1. All notices made under this DPA shall be made to Customer via email at the email Customer has used to sign up.

11. **Termination and return or deletion**

11.1. This DPA is terminated upon the termination of the Agreement. Customer may request return of Customer Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Company will delete all remaining copies of Customer Personal Data within one hundred eighty (180) days after returning Customer Personal Data to Customer.

APPENDIX 1

DESCRIPTION OF THE PROCESSING

1. **Data Subjects**

The Customer Personal Data Processed concern the following categories of Data Subjects (please specify):

#	**Category**
1	Users of Replit
2	Paid customers of Replit
3	Prospective customers and users of Replit who contact Replit
4	Job applicants to Replit
5	Visitors to https://repl.it, https://replit.com, and our other web properties

2. **Categories of Customer Personal Data**

The Customer Personal Data Processed concern the following categories of data (please specify):

#	**Category**
1	Contact Information and Identifiers, including name, alias, online identifiers, IP address, email address, or other similar identifiers.
2	Customer Records, including name, telephone number, and financial information (such as payment and bank account number, collected only by our service provider).
3	Commercial Information, including products or services purchased or obtained.
4	Internet or Other Electronic Network Activity Information, including browsing activity, searches, and information regarding a user's interaction with our internet website or application.
5	Visual Information, including profile picture.
6	Professional/Employment Information, including job application or resume information if you apply for a job with us.

3. **Sensitive data**

The Customer Personal Data Processed concern the following special categories of data (please specify):

#	**Category**
1	The Services are not intended to Process special categories of data.

4. **Processing operations**

The Customer Personal Data will be subject to the following basic Processing activities (please specify):

#	**Operation**
1	Collection of Personal Data. We collect data when you provide it to us, we collect it automatically, and when we receive it from others. You give us your information when you sign up. We also collect information through cookies (Replit Cookies, Google Analytics, and Segment).
2	Recording of Personal Data. We record your data if you contact us for support or phone calls and if you attend one of our online events.

3	Structuring of Personal Data. We structure your data to display in the product and to perform analyses on it for business strategy and product development purposes.
4	Storage of Personal Data. We store any and all data that we collect or is shared with us. Stored data is encrypted for security purposes.
5	Adaption or Alteration of Personal Data. We adapt or alter data upon request.
6	Retrieval of Personal Data. Data is retrieved by the product automatically, to conduct analyses for business strategy and product development purposes, and upon any access requests.
7	Consultation of Personal Data. We may discuss and review data for the purposes of business strategy and product development.
8	Use of Personal Data. We use data to provide the product as well as for customer communications, like our newsletter and product updates, and for the purposes of business strategy and product development.
9	Disclosure or Transmission of Personal Data. We share data with the following categories of third parties: ● Other Repl.it users (unless your repls are private, in which case only your profile data, but not your repls, will be shared) ● Third parties integrated with our Services (e.g. GitHub, social sign-on technologies) ● Service provider and vendors ● Third parties for legal matters or safety purposes
10	Destruction of Personal Data. Data will be deleted upon request or if you delete your account.

APPENDIX 2

SECURITY MEASURES

Company will implement the following types of security measures:

1. **Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Customer Personal Data are Processed, include:

- ☐ Establishing security areas, restriction of access paths;
- ☐ Establishing access authorizations for employees and third parties;
- ☐ Access control system (ID reader, magnetic card, chip card);
- ☐ Key management, card-keys procedures;
- ☐ Door locking (electric door openers etc.);
- ☐ Security staff, janitors;
- ☐ Surveillance facilities, video/CCTV monitor, alarm system; and
- ☐ Securing decentralized data processing equipment and personal computers.

2. **Virtual access control**

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- ☐ User identification and authentication procedures;
- ☐ ID/password security procedures (special characters, minimum length, change of password);
- ☐ Automatic blocking (e.g. password or timeout);
- ☐ Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- ☐ Creation of *one* master record per user, user-master data procedures per data processing environment; and
- ☐ Encryption of archived data media.

3. **Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Customer Personal Data in accordance with their access rights, and that Customer Personal Data cannot be read, copied, modified or deleted without authorization, include:

- ☐ Internal policies and procedures;
- ☐ Control authorization schemes;
- ☐ Differentiated access rights (profiles, roles, transactions and objects);
- ☐ Monitoring and logging of accesses;
- ☐ Disciplinary action against employees who access Customer Personal Data without authorization;
- ☐ Reports of access;
- ☐ Access procedure;
- ☐ Change procedure;
- ☐ Deletion procedure; and
- ☐ Encryption.

4. **Disclosure control**

Technical and organizational measures to ensure that Customer Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Customer Personal Data are disclosed, include:

- ☐ Encryption/tunneling;
- ☐ Logging; and
- ☐ Transport security.

5. **Entry control**

Technical and organizational measures to monitor whether Customer Personal Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- ☐ Logging and reporting systems; and
- ☐ Audit trails and documentation.

6. **Control of instructions**

Technical and organizational measures to ensure that Customer Personal Data are Processed solely in accordance with the instructions of the Controller include:

- ☐ Unambiguous wording of the contract;
- ☐ Formal commissioning (request form); and
- ☐ Criteria for selecting the Processor.

7. **Availability control**

Technical and organizational measures to ensure that Customer Personal Data are protected against accidental destruction or loss (physical/logical) include:

- ☐ Backup procedures;
- ☐ Mirroring of hard disks (e.g. RAID technology);
- ☐ Uninterruptible power supply (UPS);
- ☐ Remote storage;
- ☐ Anti-virus/firewall systems; and
- ☐ Disaster recovery plan.

8. **Separation control**

Technical and organizational measures to ensure that Customer Personal Data collected for different purposes can be Processed separately include:

- ☐ Separation of databases;
- ☐ "Internal client" concept / limitation of use;
- ☐ Segregation of functions (production/testing); and
- ☐ Procedures for storage, amendment, deletion, transmission of data for different purposes.