Kami GDPR-compliant Data Processing AGREEMENT under Art. 28 (3) and (4) of Regulation (EU) 2016/679

Last Modified: December 12, 2022

1. **Kami Limited,** Data Processor – Kami is an education software company that provides products and services to learners and institutions. It is situated in 8605 Santa Monica Blvd, PMB 57387, West Hollywood, California 90069-4109 USA. You can contact us here: privacy@kamiapp.com

INTRODUCTION

This Kami Data Processing Agreement ("DPA") reflects the parties' agreement with respect to the terms governing the processing of Personal Data under the Kami standard Terms of Service and the Kami Privacy Policy (together, the "TOS"). This DPA is an amendment to the TOS and is effective upon its incorporation into the TOS, which incorporation may be specified in an Order or an executed amendment to the TOS. Upon its incorporation into the TOS, the DPA will form a part of the TOS.

In all cases Kami ("Processor"), or a third party acting on behalf of Processor, acts as the processor of Personal Data and you ("Controller") remain controller of Personal Data. The term of this DPA shall follow the term of the TOS. Terms not otherwise defined herein shall have the meaning as set forth in the TOS.

. …, Data Controller - …

Named together "Parties"

General provisions

1. The purpose of this Agreement is to ensure compliance with Article 28(3) and (4) 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.

2. This Agreement is prepared in accordance with the Strandard Contractual Clauses, adopted by Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

3. The controllers and processors listed in Annex I have agreed to this Agreement in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3).

4. This Agreement apply to the processing of personal data as specified in Annex II.

5. Annexes I to IV are an integral part of the Agreement.

6. This Agreement is without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.

7. This Agreement do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

8. The Parties undertake not to modify these Clauses, except for adding information to the Annexes or updating information in them. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

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

10. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

11. These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

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

Obligations of the Parties

13. The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

14. 1. The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

14.2. The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

15. The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

16. Processing by the processor shall only take place for the duration specified in Annex II.

17. 1. The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

17.2. The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

18. If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

19.1. The Parties shall be able to demonstrate compliance with these Clauses.

19.2. The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

19.3. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

19.4. The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

19.5. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

Use of sub-processors

20. The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 90 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

21. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

22. At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

23. The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the

processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

International transfers

25. Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

26. The controller agrees that where the processor engages a sub-processor in accordance with this Agreement for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Assistance to the controller

27. The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

28. The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with this Clause and Art.27, the processor shall comply with the controller's instructions.

29. In addition to the processor's obligation to assist the controller pursuant to Art.28, the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data ("personal data protection impact assessment") where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

30. The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Notification of personal data breach

31. In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

Data breach concerning data processed by the controller

32. In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679 shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) 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.

33. Where, and insofar as, it is not possible to provide all this 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.

34. In complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

Data breach concerning data processed by the processor

35. In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

36. Where, and insofar as, it is not possible to provide all this 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.

37. The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

FINAL PROVISIONS

38. Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

39. The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

40. The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

41. Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

1. Name: …

Address: …

Contact person's name, position and contact details: …

Signature and accession date: …

2.

…

Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

1. Name: …

Address: …

Contact person's name, position and contact details: …

Signature and accession date: …

2.

…

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

Students and staff of schools which contract with Kami to provide services.

Categories of personal data processed

Name, email address, password, role, IP address, organisation, user-generated content.

Sensitive data processed (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.

NA

Nature of the processing

Users can open or upload documents in Kami online; can annotate, comment; and can share the document with other Kami users for collaborative working.

Purpose(s) for which the personal data is processed on behalf of the controller

To provide the Kami collaborative document annotation services to users. When teachers share assignments to students, or students share project work for collaborative work, they need to be able to identify or recognize other users in the service. When Kami provide user support, Kami staff need to be able to associate the user and their account. When a user logs into Kami, Kami needs to be able to authenticate the user and identify their organisation.

Duration of the processing

For the duration of the contracted period. User accounts and all user data will be deleted within 30 days of the receipt of an instruction from the user or the customer.

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

- Microsoft – if you choose to log into Kami using your Microsoft account (often referred to as Single Sign-on or “SSO”), your login will be authenticated by Microsoft. If you open/save files on OneDrive, Microsoft will first request authorization for this. You can review Microsoft’s Privacy Policy for use of your Microsoft account here; and update or revoke your permissions as described here.
- Google – if you choose to log into Kami using your Google account, your login will be authenticated by Google. If you open/save files on Google Drive, Google will first request authorization for this. You can review Google’s Privacy Policy for use of your Google account here; and update or revoke your Google Permissions here.
- Groove – Groove is a platform our Support Team use internally to coordinate customer support activities in response to requests from our customers. Our contractual agreement with Groove complies with the terms of this policy.
- Google Analytics & Tag Manager – an analytics service used to help analyze your use of our Website and allow us to improve our Service and provide you information on the Service. Our agreement with Google complies with the terms of this policy.

- Stripe – when you upgrade your account online using a credit card, your payment is securely processed using Stripe's e-payments service. Our contractual agreement with Stripe complies with the terms of this policy.

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

Below is a description of the technical and organisational measures implemented by the Processor (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.

Where applicable this Table will serve as Annex III to the SCCs.

Measure	**Description**
Measures of pseudonymisation and encryption of Personal Data	For the purpose of transfer control, Encryption is used during transit for connections between users' browsers and our backend services. We employ industry best-standard cipher suites and protocols - currently TLS 1.2 with ECDHE_RSA key exchange and AES encryption. For bulk transfer of data or initial data setup we employ a secure folder on Google drive, set up per school to allow data separation, files are uploaded to it encrypted or non encrypted with keys being sent out of band, we also have a Secure file transfer server that usesSSH keys not passwords to share data. All personal data is destroyed as per our data destruction policies when no longer used.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person. To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.

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	Your data is protected using streaming replication to geographically distributed backup servers and log shipping to secure storage. We create daily backups using multiple independent systems and store them across multiple different providers. Our backups are encrypted on dm-crypt encrypted disks with strong passwords. We conduct disaster recovery drills quarterly to ensure we can quickly restore services without data loss in cases of emergency.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	All changes to code and systems relating to customer data is peer reviewed and audited, some automation scripts are run over source code to validate compliance to policy and adherence to industry standards. all aspects of the systems that retain customer data are tested at least annually via an independent third party where defects and recommendations are logged and rectified. staff also have regular (at least annual) process and policy revision as well as security awareness training. Automated tools are running continually auditing the data processing systems with reports generated and critical defect alerted to us 24/7.
Measures for user identification and authorisation	Staff require SSH keys and 2FA-login (via hardware tokens) to access our networks. We implement best-practice protective measures against attacks including XSS, CSRF, and SQL injection. We support both authentication with a username and password, and SSO through Google OAuth. Passwords are stored using bcrypt with a high stretching factor.
Measures for the protection of data during transmission	Data in transit is protected by Transport Layer Security ("TLS"). Encryption is used during transit for connections between users' browsers and our backend services. We employ industry best-standard cipher suites and protocols - currently TLS 1.2 with ECDHE_RSA key exchange and AES encryption. We use HSTS to ensure all HTTP requests through our domains shall always be encrypted and prevent MITM attacks. Data is protected at rest using encryption provided by our cloud services providers (Amazon Web Services and Google Cloud Platform).

Measures for the protection of data during storage	Personal Data is only retained internally on encrypted disks, and on the third party data centre servers, which are covered by Amazon Web Services (AWS) and Google Cloud Platform (GCP) certifications and can be found on their respective sites found on both AWS and Google Cloud Platform. PII students is stored only in our Third party Data centres not locally.
Measures for ensuring physical security of locations at which Personal Data are processed	The Processor utilises third party data centres that maintain current ISO 27001 certifications and/or SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports. The Processor will not utilise third party data centres that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations. The Processor's main office is secured with keyfob entry. When it is not occupied, it is locked securely and covered by a remotely monitored alarm. A central log of keyholders is maintained and access is revoked when an employee is terminated. The Processor's employees that work from home are expected to comply with our security policy in full at all times. Our disciplinary procedure covers failure to meet these standards.
Measures for ensuring events logging	System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted, this is stored in our respective data centres maintained by AWS and GCP
Measures for ensuring system configuration, including default configuration	System configuration is applied and maintained by software tools that ensure the system configurations do not deviate from the specifications, containers are generated from image repositories stored in GCP, we maintain Infrastructure as code as at our core and all changes go via peer review and change control, systems changes are made via a continuous integration (CI) continuous deployment (CD) through non production and promoted in to product via controls and automation (no manual deployments)
Measures for internal IT and IT security governance and management	Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems. The Controller's Personal Data is stored in a way that logically separates it from other customer data.

<table>
<tr><td>Measures for certification/assurance of processes and products</td><td>The Processor utilises third party data centres that maintain current ISO 27001 certifications and/or SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports. The Processor will not utilise third party data centres that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations. Upon the Controller’s written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties. The processor is also independently audited yearly to verify compliance with industry best practice, upon request and executive summary can be obtained.</td></tr>
<tr><td>Measures for ensuring data minimisation</td><td>If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly in accordance with the relevant legal legislation of the country of origin of the requester of known and requested to do so, otherwise personal data is disposed of in accordance with our data destruction policy. Kami only collects data that is used explicitly required to provide and maintain the service to you
<table>
<tr><th>Category</th><th>Elements</th></tr>
<tr><td>Application technology meta data</td><td>IP address, cookies</td></tr>
<tr><td>Application usage statistics</td><td>meta data on interaction with ap</td></tr>
<tr><td>Authentication</td><td>Oauth key</td></tr>
<tr><td>User information</td><td>First name, last name (if enterec email address</td></tr>
<tr><td>User-generated data</td><td>Filenames, annotations, comme A Document itself is only upload servers if shared by the user wit for collaborative annotation. The Documents are fingerprinted anc and are not stored persistently o servers. (The sharing function m be disabled for a given domain)</td></tr>
</table>
</td></tr>
</table>

Measures for ensuring data quality	All of the data that we possess is provided by the Controller. The Processor does not assess the quality of the data provided by the Controller. The Processor provides reporting tools within its product to help the Controller understand and validate the data that is stored. The Controller can at anytime contact the Processor to get data updated after going through the processors identity verification process.
Measures for ensuring limited data retention	All data that is stored is subject to our retention policy, this specifies how each type of data is retained. When a record with Personal Data is deleted then it will be permanently evicted from the Processor’s active databases. The data is retained in the Processor’s backups until they are rotated out by more recent backups per the data retention policy.
Measures for ensuring accountability	All employees that handle sensitive data must acknowledge the information security policies. All employees go through annual training to reinforce and advise of any changes in policies. A disciplinary policy is in place for employees that do not adhere to information security policies.
Measures for allowing data portability and ensuring erasure	The processor has policies in place to allow transfer of personal data you have provided us to another organization this export, you will receive your personal data in a structured, commonly used and machine readable format. In case you provided your consent to the processing of personal data, you may withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. If your personal data are transferred outside the European Economic Area, you have the right to obtain copy of such data as well as indication of the Country/Countries where the personal data have been made available.
Measures to be taken by the (Sub-) processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-processor, to the Data Exporter).	The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union’s data protection requirements, e.g. by employing contracts based on the EU SCCs.

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Google Cloud Platform – cloud hosting, storage and data processing
2. Amazon Web Services – cloud hosting, storage and data processing
3. Groove – user support ticketing platform
4. Stripe – secure credit card payment platform