DATA PROCESSOR ADDENDUM

Effective 9th May 2024

1. Introduction

1.1 This agreement re processing of personal data (the **"Data Processor Agreement**") regulates Poodll's (the **"Data Processor**") processing of personal data on behalf of the client (the **"Data Controller**") and is attached as an addendum to the *Poodll SaaS Terms of Use* agreement (the "**Service Agreement**") in which the parties have agreed the terms for the Data Processor's delivery of services to the Data Controller.

2. Legislation

2.1 The Data Processor Agreement shall ensure that the Data Processor complies with the applicable data protection and privacy legislation (the "Applicable Law"), including in particular The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679)

3. Processing of personal data

3.1 Purpose: The purpose of the processing under the Service Agreement is the provision of the Services by the Data Processor as specified in the Service Agreement.

3.2 In connection with the Data Processor's delivery of the Main Services to the Data Controller, the Data Processor will process certain categories and types of the Data Controller's personal data on behalf of the Data Controller.

3.3 "Personal data" includes "*any information relating to an identified or identifiable natural person*" (the "Data subject") as defined in GDPR, article 4 (1) (1) (the "Personal Data"). The categories and types of Personal Data processed by the Data Processor on behalf of the Data Controller are listed in sub-appendix A. The Data Processor only performs processing activities that are necessary and relevant to perform the Main Services. The parties shall update sub-appendix A whenever changes occur that necessitates an update.

3.4 The Data Processor shall have and maintain a register of processing activities in accordance with GDPR, article 32 (2).

4. Instruction

4.1 The Data Processor may only act and process the Personal Data in accordance with the documented instruction from the Data Controller (the "Instruction"), unless required by law to act without such instruction. The Instruction at the time of entering into this Data Processor Agreement (DPA) is that the Data Processor may only process the Personal Data with the purpose of delivering the Main Services as described in the main Service Agreement. Subject to the terms of this DPA and with mutual agreement of the parties, the Data Controller may issue additional written instructions consistent with the terms of this Agreement. The Data Controller is responsible for ensuring that all individuals who provide written instructions are authorised to do so.

4.2 The Data Controller guarantees to process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. The Data Controller's instructions for the processing of Personal Data shall comply with Applicable Law. The Data Controller will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which it was obtained.

4.3 The Data Processor will inform the Data Controller of any instruction that it deems to be in violation of Applicable Law and will not execute the instructions until they have been confirmed or modified.

5. The Data Processor's obligations

5.1 Confidentiality

5.1.1 The Data Processor shall treat all the Personal Data as strictly confidential information. The Personal Data may not be copied, transferred or otherwise processed in conflict with the Instruction, unless the Data Controller in writing has agreed.

5.1.2 The Data Processor's employees shall be subject to an obligation of confidentiality that ensures that the employees shall treat all the Personal Data under this DPA with strict confidentiality.

5.1.3 Personal Data will only be made available to personnel that require access to such Personal Data for the delivery of the Main Services and this Data Processor Agreement.

5.2 The Data Processor shall also ensure that employees processing the Personal Data only process the Personal Data in accordance with the Instruction.

5.3 Security

5.3.1 The Data Processor shall implement the appropriate technical and organizational measures as set out in this Agreement and in the Applicable Law, including in accordance with GDPR, article 32. The security measures are subject to technical progress and development. The Data Processor may update or modify the security measures from time-to-time provided that such updates and modifications do not result in the degradation of the overall security.

5.4 The Data Processor shall provide documentation for the Data Processor's security measures if requested by the Data Controller in writing.

5.5 Data protection impact assessments and prior consultation

5.5.1 If the Data Processor's assistance is necessary and relevant, the Data Processor shall assist the Data Controller in preparing data protection impact assessments in accordance with GDPR, article 35, along with any prior consultation in accordance with GDPR, article 36.

5.6 Rights of the data subjects

5.6.1 If the Data Controller receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and the correct and legitimate reply to such a request necessitates the Data Processor's assistance, the Data Processor shall assist the Data Controller by providing the necessary information and documentation. The Data Processor shall be given reasonable time to assist the Data Controller with such requests in accordance with the Applicable Law.

5.6.2 If the Data Processor receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and such request is related to the Personal Data of the Data Controller, the Data Processor must immediately forward the request to the Data Controller and must refrain from responding to the person directly.

5.7 Personal Data Breaches

5.7.1 The Data Processor shall give immediate notice to the Data Controller if a breach occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or otherwise processed re the Personal Data processed on behalf of the Data Controller (a "Personal Data Breach").

5.7.2 The Data Processor shall make reasonable efforts to identify the cause of such a breach and take those steps as they deem necessary to establish the cause, and to prevent such a breach from reoccurring.

5.8 Documentation of compliance and Audit Rights

5.8.1 Upon request by a Data Controller, the Data Processor shall make available to the Data Controller all relevant information necessary to demonstrate compliance with this DPA, and shall allow for and reasonably cooperate with audits, including inspections by the Data Controller or an auditor mandated by the Data Controller. The Data Controller shall give notice of any audit or document inspection to be conducted and shall make reasonable endeavours to avoid causing damage or disruption to the Data Processors premises, equipment and business in the course of such an audit or inspection. Any audit or document inspection shall be carried out with reasonable prior written notice of no less than 30 days, and shall not be conducted more than once a year.

5.8.2 The Data Controller may be requested to sign a non-disclosure agreement reasonably acceptable to the Data Processor before being furnished with the above.

5.9 Data Transfers

5.9.1 Ordinarily, the Data Processor will not transfer your data to countries outside the European Economic Area. In some cases, personal data may be saved on storage solutions that have servers outside the European Economic Area (EEA). Only those storage solutions that provide secure services with adequate relevant safeguards will be employed.

6. Sub-Processors

6.1 The Data Processor is given general authorisation to engage third-parties to process the Personal Data ("Sub-Processors") without obtaining any further written, specific authorization from the Data Controller, provided that the Data Processor notifies the Data Controller in writing about the identity of a potential Sub-Processor (and its processors, if any) before any agreements are made with the relevant Sub-Processors and before the relevant Sub-Processor processes any of the Personal Data. If the Data Controller wishes to object to the relevant Sub- Processor, the Data Controller shall give notice hereof in writing within ten (10) business days from receiving the notification from the Data Processor. Absence of any objections from the Data Controller shall be deemed consent to the relevant Sub-Processor.

6.2 In the event the Data Controller objects to a new Sub-Processor and the Data Processor cannot accommodate the Data Controller's objection, the Data Controller may terminate the Services by providing written notice to the Data Processor.

6.3 The Data Processor shall complete a sub-processor agreement with any Sub-Processors. Such an agreement shall at minimum provide the same data protection obligations as the ones applicable to the Data Processor, including the obligations under this Data Processor Agreement. The Data Processor shall on an ongoing basis monitor and control its Sub-Processors' compliance with the Applicable Law. Documentation of such monitoring and control shall be provided to the Data Controller if so requested in writing.

6.4 The Data Processor is accountable to the Data Controller for any Sub-Processor in the same way as for its own actions and omissions.

6.5 The Data Processor is at the time of entering into this Data Processor Agreement using the Sub- Processors listed in sub-appendix B. If the Data Processor initiates sub-processing with a new Sub-Processor, such new Sub-Processor shall be added to the list of Sub-Processors at https://poodll.com/subprocessors.

7. Limitation of Liability

7.1 The total aggregate liability to the Client, of whatever nature, whether in contract, tort or otherwise, of the Data Processor for any losses whatsoever and howsoever caused arising from or in any way connected with this engagement shall be subject to the "Liability" clause set out in the main Service Agreement.

7.2 Nothing in this DPA will relieve the processor of its own direct responsibilities and liabilities under the GDPR.

8. Duration

8.1 The Data Processor Agreement shall remain in force until the main Service Agreement is terminated.

9. Data Protection Officer

9.1 The Data Processor will appoint a Data Protection Officer where such appointment is required by Data Protection Laws and Regulations.

10. Termination

10.1 Following expiration or termination of the Agreement, the Data Processor will delete or return to the Data Controller all Personal Data in its possession as provided in the Agreement except to the extent the Data Processor is required by Applicable law to retain some or all of the Personal Data (in which case the Data Processor will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this DPA will continue to apply to such Personal Data.

Sub-appendix A

1. Personal Data

1.1 The Data Processor processes the following types of Personal Data in connection with its delivery of the Main Services:

1. Data subject may submit Personal Information to the Service, the extent of which is determined and controlled by the Data subject in their sole discretion and which may include, but is not limited to Personal Data.
2. Audio and Video Recordings, and derived data such as AI-generated Transcripts.
3. Information contained within logs of the Main service. This may include
    1. IP address of a Data subject
    2. Date and time of a recording submission
    3. User identifier of a Data subject as determined by Data controller

2. Categories of data subjects

2.1 The Data Processor processes personal data about the following categories of data subjects on behalf of the Client:

1. Users of the Main Service, including Students, Teachers, and Administrators.

Sub-appendix B

1. APPROVED SUB-PROCESSORS

1.1 The following Sub-Processors shall be considered approved by the Data Controller at the time of entering into this Agreement:

Entity Name	Purpose	Location of processing
Assembly AI	Speech to text services	USA
Amazon Web Services	Cloud services including speech processing and file storage	EEA (Ireland and Germany), Australia,Bahrain,Brazil,Canada,Singapore,South Africa,UK,USA,India,Japan
EnglishCentral	English speaking practice and automated feedback.	EEA or USA
Google	Cloud services including speech processing	EEA (Ireland) or USA
Loom	Screen recording and file storage	USA
Open AI	AI services including speech processing and text analysis	EEA or USA

Sub-appendix C

Technical and Organizational Measures

The Data Processor maintains the following technical and organizational security measures to protect Personal Data:

Category	Measure Details
Organizational Controls	The Data Processor maintains direct oversight and strict control over all processing activities. Security policies are formally reviewed annually by the Data Processor's leadership. Access to production systems is restricted exclusively to authorized personnel via multi-factor authentication (MFA).
Encryption & Storage	All data is stored using Amazon Web Services (AWS) S3. Data at rest is encrypted using AES-256 server-side encryption. Data in transit is protected via TLS 1.2 or higher.
Access Control	Leveraging AWS Identity and Access Management (IAM), the principle of least privilege is applied. S3 bucket policies are configured such that direct public access is denied; however, specific files are made public via randomized, unpredictable URLs that are not indexed or searchable, similar to an unlisted video link. Audit logs are maintained via CloudTrail.
Resilience & Recovery	High availability is ensured through AWS multi-AZ deployment. Automated backups and versioning are enabled for data stored in S3 to facilitate rapid recovery from accidental deletion or corruption.