DATA PROCESSING AGREEMENT

SECTION 1: GENERAL INFORMATION

1. Purpose - Scope of application

The purpose of these sub-contracting clauses ("Data Processing Agreement" or "DPA") is to define the conditions under which LEARN & GO undertakes to carry out, in application of the General Terms and Conditions to which these are annexed ("the Contract"), the personal data processing operations defined below, on behalf of the Customer who will act as data controller.

In the context of their contractual relationship, the parties undertake to comply with the regulations in force applicable to the processing of personal data and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable from 25 May 2018 (hereinafter, "the European Data Protection Regulation" or "EDPR").

This DPA applies exclusively to the processing of personal data under the Contract.

During the term of the Contract, the Data Processor is authorised to process personal data ("Personal Data") on behalf of and on the instructions of the Data Controller in the context of the performance of the Contract with the Data Controller. The Data Controller is, to the exclusion of all others, solely responsible for determining the purposes for which Personal Data will (must) be processed and the manner in which this is done.

2. Interpretation

Where terms defined in Regulation (EU) 2016/679 appear in the clauses of this Agreement, they shall be construed as in the Regulation in question.
These clauses must be read and interpreted in the light of the provisions of the RGPD.
These clauses must not be interpreted in a way that is contrary to the rights and obligations set out in the RGPD or in a way that infringes the fundamental rights or freedoms of the data subjects.

3. Duration of the Agreement

This Agreement shall enter into force retroactively to the date of the Contract concluded between the parties relating to the supply of the Kaligo application and for a duration equal to that of the latter.

4. Language

The governing language of this Agreement is French. Learn & Go has translated this policy into various languages using automatic translation tools, exclusively to enhance accessibility for visitors, prospects, and customers not proficient in French. This translated version is for informational purposes only, and Learn & Go cannot guarantee the quality or accuracy of the translation, nor can it assume any liability. In the event of a dispute concerning this Agreement, only the French version will be considered legally binding and authentic.

SECTION 2: OBLIGATIONS OF THE PARTIES

5. Description of the processing being outsourced

The processor is authorised to process the personal data required to provide the service(s) covered by the Contract on behalf of the data controller.

The nature of the operations carried out on the data relates to its hosting in Cloud mode and, at the Customer's request, access by the Subcontractor's technical and support teams to the data in order to move, restore or delete it.

The purpose(s) of the processing, the personal data processed and the categories of persons concerned in the context of the services covered by the Contract are listed in the register of processing established by the controller on the one hand and the processor on the other, the latter having no control over the data collected and stored.

In order to comply with these conditions, the controller shall provide the processor with the following information in Appendix 1:

- Name and contact details of the data controller
- Name and contact details of the Data Protection Officer

Details of the processing operations, and in particular the categories of personal data and the purposes for which personal data is processed on behalf of the controller, are set out in Annex 2.

6. Instructions

The processor shall process personal data only on the documented instruction of the controller, unless he is required to do so by Union law or the law of the Member State to which he is subject. In this case, the processor shall inform the controller of this legal obligation prior to processing, unless prohibited by law on important public interest grounds. Instructions may also be given subsequently by the controller throughout the processing of personal data. These instructions must always be documented.

The processor shall immediately inform the controller if, in its opinion, an instruction given by the controller constitutes a breach of Regulation (EU) 2016/679 or other provisions of Union or Member State law relating to data protection.

7. Purpose limitation

The processor processes personal data solely for the specific purpose(s) of the processing, as defined in Annex 2, unless further instructions are given by the controller.

8. Duration of processing of personal data

Processing by the processor only takes place for the duration of the Contract as specified in Appendix 2.

9. Treatment safety

The processor shall implement at least the technical and organisational measures specified in Annex 3 to ensure the security of personal data. These measures include the protection of data against any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal 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 and the nature, scope, context and purposes of the processing, as well as the risks to data subjects.

The processor shall only grant members of its staff access to the personal data being processed to the extent strictly necessary for the performance, management and monitoring of the contract. The processor shall ensure

that persons authorised to process personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality.

10. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, as well as genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific limitations and/or additional guarantees.

11. Documentation and compliance

The parties must be able to demonstrate compliance with these clauses.

The processor shall deal promptly and appropriately with requests from the controller concerning the processing of data in accordance with these clauses.

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and arising directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the request of the controller, the processor shall also permit and contribute to audits of the processing activities covered by these clauses at reasonable intervals or where there are indications of non-compliance. When deciding on a review or audit, the controller may take into account relevant certifications in the possession of the processor.

The controller may decide to carry out the audit itself or to appoint an independent auditor. Audits may also include inspections of the processor's premises or physical facilities and, where appropriate, are carried out with reasonable notice.

The parties shall make available to the competent supervisory authority(ies), upon request, the information set out in this clause, including the results of any audit.

12. Use of subsequent subcontractors

The processor shall have the general authorisation of the controller to recruit further processors on the basis of an agreed list. The processor shall inform the controller in advance in writing of any plans to amend this list by adding or replacing sub-processors at least 30 days in advance, thereby giving the controller sufficient time to object to such changes prior to the recruitment of the sub-processor(s) concerned. The processor shall provide the controller with the information necessary to enable him to exercise his right to object. The data controller has a maximum of 5 working days from the date of receipt of this information to present its objections. This sub-contracting may only be carried out if the data controller has not raised any objections within the agreed period.

The list of sub-contractors is included in the data processing register and is made available to the customer on written request.

The subsequent processor is required to comply with the obligations of this contract on behalf of and in accordance with the instructions of the controller. It is the responsibility of the initial processor to ensure that the subsequent processor presents the same sufficient guarantees regarding the implementation of appropriate technical and organisational measures so that the processing meets the requirements of the European Data Protection Regulation.

At the request of the controller, the processor shall provide the controller with a copy of the contract with the sub-processor and any subsequent amendments thereto. To the extent necessary to protect business secrets or other confidential information, including personal data, the processor may redact the text of the contract before distributing a copy.

The processor shall remain fully responsible to the controller for the performance of the obligations of the sub-processor in accordance with the contract concluded with the sub-processor. The processor shall inform the controller of any breach by the sub-processor of its contractual obligations.

13. International transfers :

Any transfer of data to a third country or international organisation by the processor shall only be carried out on the basis of documented instructions from the controller or in order to comply with a specific requirement of Union law or Member State law to which the processor is subject and shall be carried out in accordance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

The Controller agrees that where the Processor engages a sub-processor in accordance with clause 7.7 to carry 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 may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using the standard contractual clauses adopted by the Commission on the basis of Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for using those standard contractual clauses are met.

14. Assistance to the data controller

The processor shall inform the data controller without delay of any request it has received from the data subject. He shall not himself comply with such a request, unless authorised to do so by the data controller.

The processor shall assist the controller in fulfilling its obligation to respond to requests from data subjects to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations, the processor shall comply with the instructions of the controller.

In addition to the processor's obligation to assist the controller pursuant to the previous paragraph, the processor shall also assist the controller in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to the processor:

- the obligation to carry out an assessment of the impact of proposed processing operations on the protection of personal data ("data protection impact assessment") when a type of processing is likely to present a high risk to the rights and freedoms of natural persons;
- the obligation to consult the competent supervisory authority(ies) prior to processing where a data protection impact assessment indicates that the processing would present a high risk if the controller did not take steps to mitigate the risk;
- 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 obsolete;
- the obligations set out in Article 32 of Regulation (EU) 2016/679.

The parties shall define in Annex 3 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 extent of the assistance required.

15. Notification of personal data breaches

In the event of a personal data breach, the processor shall cooperate with and assist the controller in complying with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or Articles 34 and 35 of Regulation (EU) 2018/1725, whichever is applicable, taking into account the nature of the processing and the information available to the processor.

15.1 Data breach in relation to data processed by the controller

In the event of a personal data breach relating to data processed by the controller, the processor shall provide assistance to the controller:
a) for the purpose of notifying the competent supervisory authority(ies) of the personal data breach as soon as possible after the controller becomes aware of the breach, if any (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
(b)for the purposes of obtaining the following information which, in accordance with Article 33(3) of Regulation (EU) 2016/679 must be included in the controller's notification, and include, at least:

- the nature of the personal data, including, if possible, the categories and approximate number of persons affected by the breach and the categories and approximate number of personal data records affected;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any negative consequences.

Where, and to the extent that, it is not possible to provide all the information at the same time, the initial notification shall contain the information available at that time and, as it becomes available, additional information shall be provided thereafter as soon as possible;

(c)for the purposes of fulfilling, in accordance with Article 34 of Regulation (EU) 2016/679, the obligation to communicate the personal data breach to the data subject as soon as possible, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

15.2. Data breach in relation to data processed by the processor

In the event of a personal data breach relating to data processed by the processor, the processor shall notify the controller as soon as possible after becoming aware of the breach. This notification shall contain at least:
(a) a description of the nature of the breach identified (including, where possible, the categories and approximate number of individuals affected by the breach and of personal data records affected);
(b) details of a contact point from which further information may be obtained concerning the personal data breach;
(c) its likely consequences and the steps taken or proposed to be taken to remedy the breach, including mitigation of any adverse consequences.
Where, and to the extent that, it is not possible to provide all the information at the same time, the initial notification shall contain the information available at that time and, as it becomes available, additional information shall be provided thereafter as soon as possible.

SECTION 3 - FINAL PROVISIONS

16. Non-compliance with clauses and termination :

a) Without prejudice to the provisions of Regulation (EU) 2016/679, in the event of a breach by the processor of its obligations under these clauses, the controller may instruct the processor to suspend the processing of the personal data until the processor has complied with these clauses or the contract is terminated. The processor shall promptly inform the controller if it is unable to comply with these clauses for any reason.

b) The data controller shall be entitled to terminate this Agreement insofar as it relates to the processing of personal data in accordance with these clauses if:

- the processing of personal data by the processor has been suspended by the controller in accordance with point a) and compliance with these clauses is not restored within a reasonable period and, in any event, within one month of the suspension;
- the subcontractor is in serious or persistent breach of these clauses or of its obligations under Regulation (EU) 2016/679
- the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority(ies) regarding its obligations under these Clauses or Regulation (EU) 2016/679.

c) The Processor shall be entitled to terminate this Agreement insofar as it relates to the processing of personal data under these clauses where, having informed the Controller that its instructions breach applicable legal requirements in accordance with clause 7.1(b), the Controller insists that its instructions be followed.

d) Following termination of this Agreement, the processor shall, at the choice of the controller, either delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or return all personal data to the controller and destroy existing copies, unless Union or national law requires them to be retained for longer. The processor shall continue to ensure compliance with these clauses until the data is deleted or return

APPENDIX 1 - LIST OF PARTIES

DATA CONTROLLER(S):
The Customer.

SUBCONTRACTOR
LEARN & GO SAS
43 Square de la Mettrie - 35700 RENNES
RCS Rennes 824 814 982
Represented by Mr Benoit Jeannin in his capacity as Chairman

Personal Data Protection Officer :
Mrs. Marie Hombert
legal@learn-and-go.com

APPENDIX 2- TREATMENT DESCRIPTION

Categories of data subjects whose personal data are processed

- Kaligo application users (students and teachers)

Categories of personal data processed

- Content imported by the Customer into the Application (teacher's details, student's name, laterality and classroom etc.)
- No sensitive data may be imported by the Customer.

Access to data imported by the Customer onto the Application by Learn & Go will be strictly limited to members of staff who need access to answer support or maintenance questions.

Type of treatment

- Data hosting
- Access to data by the Subcontractor's technical and support teams only on the Customer's instructions, in order to move, restore or delete them.

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

- Cloud hosting and storage of data imported by the Customer into the Application (retention).
- Provision of corrective and evolutionary maintenance services. (access).

Duration of treatment

- The duration of the contractual relationship.

ANNEX 3 - Technical and organizational measures to ensure data security

In particular, the Sub-Contractor implements the following safety measures:

Physical Measurement :

- Installation of a functional alarm to limit the risk of intruders entering the premises
- Key and code locking system for the premises.

Organisational measures :

- Access to customer accounts and data is restricted to strictly authorised persons whose access is required to carry out maintenance and support services on the instructions of the user (teacher or facility administrator).
- Introduction of a teleworking charter and an IT charter appended to the internal rules to govern the use of digital office tools by employees on site and at home.
- Confidentiality clauses in employee contracts.
- Implementation of a security policy and back-up plan
- Implementation of a personal data breach policy.
- Maintenance of the personal data processing register and the security incident register.
- Raising employee awareness and setting up a mandatory training process.

Technical measures :

- Use of secure protocols (https) when exchanging data between servers or between servers and clients.
- Encryption of customer account passwords and introduction of a requirement for customers to have a strong password that meets various characteristics and prohibits the use of known passwords.
- Implementation of a traceability and logging system for actions (deletion, modification, addition) and connections, or attempted connections.
- Daily backups of data imported by the user into Kaligo
- Data hosting on 2 different servers (redundancy) located on different sites (1 in Gravelines and 1 in Roubaix). Data is hosted on OVH servers. Access, security and server storage measures are detailed in the OVH security policy.