DATA PROCESSING AGREEMENT

PROWISE LEARN

1. The educational institution/school named _____, with its address at _____, hereinafter to be referred to as: the "**Data Controller**";

AND

2. **PROWISE UK LIMITED**, a company incorporated under the laws of the United Kingdom, having its registered office in Birmingham at (B24 8HZ) Gravelly Industrial Park, Unit 19, Tyburn Road, the United Kingdom, hereinafter to be referred to as: the "**Data Processor**";

hereinafter together also referred to as: the "Parties",

HEREBY AGREE AS FOLLOWS:

1. Subject matter of this Data Processing Agreement

1.1 This Data Processing Agreement applies exclusively to the processing of personal data that is subject to Data Protection Law in the scope of the agreement between the Parties regarding the web based service called Prowise Learn ("**Services**") (hereinafter to be referred to as: the "**Service Agreement**").

1.2 The term "**Data Protection Law**" shall mean 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 (General Data Protection Regulation; "**GDPR**") and the applicable data protection provisions of the EU or of a member state.

1.3 Terms such as "**Processing**", "**Personal Data**", "**Data Controller**", "**Processor**" and "**Personal Data Breach**" shall have the meaning ascribed to them in the GDPR.

1.4 Insofar as the Data Processor will be processing Personal Data subject to Data Protection Law on behalf of the Data Controller in the course of the performance of the Service Agreement with the Data Controller the terms of this Data Protection Agreement shall apply. An overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed is provided in Annex 2.

2. Nature, scope and purpose of the processing of personal data

2.1 The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Controller's written instructions.

2.2 The Parties have entered into a Service Agreement in order to benefit from the expertise of the Processor in securing and processing the Personal Data for the purposes set forth in Annex 2. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Agreement.

3. Obligations of the Data Processor

3.1 The Data Processor will only process the Personal Data on documented instructions of the Data Controller in such manner as - and to the extent that - this is appropriate for the performance of the Services, except as required to comply with a legal obligation to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless that law explicitly prohibits providing such information to the Data Controller. The Data Processor shall never process the Personal Data in a manner inconsistent with the Data Controller's documented instructions. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the Data Protection Law or other Union or Member State data protection provisions.

3.2 Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1 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, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. The measures which are agreed upon by the Parties are specified in Annex 3.

4.2 The Data Processor shall at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures set forth in Article 4.1.

4.3 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an

on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction.

4.4 Where an amendment to the Service Agreement is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in applicable data protection law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

5. Audit rights

5.1 At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to this Article 4 and shall allow the Data Controller to audit and test such measures. An audit may only take place after the Data Controller has requested and assesses similar audit reports available to the Data Processor and provides reasonable arguments that justify an audit initiated by the Data Controller. Such an audit is justified when the similar audit reports available to the Data Processor give no or insufficient information about compliance with this Data Processing Agreement by the Data Processor.

5.2 The Data Processor has the right to refuse a third party designated by the Data Controller for an audit, if the third party does not have sufficient qualifications according to the Data Processor's assessment or if it is a competitor of the Data Processor. If the Data Processor rejects a third party for the aforementioned reasons, the Data Controller is obliged to nominate another third party for the audit or alternatively can carry out the audit itself.

5.3 Audits by the Data Controller are subject to the following terms:

a. the audit will be pre-scheduled in writing with the Data Processor, at least fourteen (14) days in advance and will be performed not more than once a year (except for an audit following a Personal Data Breach);
b. the auditor will execute a non-disclosure undertaking toward the Data Processor;
c. the auditor will not have access to non-Controller data;
d. the Data Controller will make sure that the audit will not interfere with or damage the business activities and information and network systems of the Data Processor;
e. the Data Controller will bear all costs and assume responsibility and liability for the audit;
f. the Data Controller will receive only the auditor's report, will keep the audit results in strict confidentiality and will use them solely for the specific purposes of the audit under this article;
g. at the request of the Data Processor, the Data Controller will provide it with a copy of the auditor's report.

5.4 The Data Processor may claim compensation for allowing audits by the Data Controller.

6. Data Transfers

6.1 The Data Processor shall immediately notify the Data Controller of any (planned) permanent or temporary transfers of Personal Data to a country outside of the European Economic Area without an adequate level of protection and shall only perform such a (planned) transfer after obtaining authorisation from the Data Controller, which may be refused at its own discretion. Annex 4 provides a list of transfers for which the Data Controller grants its consent upon the conclusion of this Data Processing Agreement.

6.2 To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

7. Information Obligations and Personal Data Breaches

7.1 When the Data Processor becomes aware of an incident that constitutes as a Personal Data Breach, it shall promptly notify the Data Controller about the incident, shall at all times cooperate with the Data Controller, and shall follow the Data Controller's instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

7.2 The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about an incident that constitutes as a Personal Data Breach. Where the incident is reasonably likely to require a data breach notification by the Data Controller under applicable Data Protection Law, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller after having become aware of such an incident.

7.3 Any notifications made to the Data Controller pursuant to this Article 7 shall be addressed to the employee of the Data Controller whose contact details are provided in Annex 1 of this Data Processing Agreement, and shall contain:

a. a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
b. the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;
c. a description of the likely consequences of the incident; and
d. a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

8. Contracting with Sub-Processors

8.1 The Data Controller authorises the Data Processor to engage the sub-processors in the country locations for the Service-related activities specified in Annex 2. The Data Processor shall inform the Data

Controller of any addition or replacement of such sub-processors. The Data Controller shall be entitled to object to such addition or replacement on reasonable grounds relating to data protection in writing within 30 days of the Data processor's notice. If the Data processor still intends to replace or engage a new sub-processor despite the Data Controller's objection, the Data Controller shall be entitled to terminate the Service Agreement with immediate effect within 30 days of the Data processor's notice. Notice of termination shall be given in writing.

8.2 Notwithstanding any authorisation by the Data Controller within the meaning of the preceding paragraph, the Data Processor shall remain fully liable vis-à-vis the Data Controller for the performance of any such sub-processor that fails to fulfill its data protection obligations.

8.3 The consent of the Data Controller pursuant to Article 8.1 shall not alter the fact that consent is required under Article 6 for the engagement of sub-processors in a country outside the European Economic Area without a suitable level of protection.

8.4 The Data Processor shall ensure that the sub-processor is bound by the same data protection obligations of the Data Processor under this Data Processing Agreement, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Law.

9. Returning or Destruction of Personal Data

9.1 After termination of this Data Processing Agreement, the Personal Data will be processed for a period of 12 months. After commencement of 12 months, the Personal Data will be deleted or anonymised.

9.2 Nothwithstanding article 9.1, however, The Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and delete or return any existing copies upon the Data Controller's written request.

10. Assistance to Data Controller

10.1 The Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under the Data Protection Law.

10.2 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to article 4 (Security) and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.

10.3 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

11. Liability

11.1 The Data Controller and the Data Processor are liable to the persons concerned in accordance with the provisions of article 82 GDPR.

12. Inconsistency and amendment of the Data Processing Agreement

12.1 In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Service Agreement, the provisions of this Data Processing Agreement shall prevail.

12.2 If the Parties need to deviate from the clauses of this Data Processing Agreement or wish to supplement them, these deviations and/or additions will be described and substantiated by the Parties in an overview that will be attached to this Data Processing Agreement as Annex 4. The provisions of this paragraph do not apply to additions and/or changes to Annexes 1, 2 and 3.

12.3 In the event of important changes to the Services that influence the Processing of Personal Data, the Data Controller will be informed in clear language about the consequences of these changes before the Data Controller accepts this choice. Important changes are in any case: the addition or change of a functionality that leads to an increase with regard to the Personal Data to be Processed and the purposes for which the Personal Data is Processed. These changes will be included in Annex 2.

12.4 Changes to the clauses of his Data Processing Agreement can only be agreed jointly in writing.

13. Duration and Termination

13.1 This Data Processing Agreement shall come into effect on the date of signing and will be concluded for the same term as the Service Agreement.

13.2 If the Service Agreement is terminated for any reason whatsoever, this Data Processing Agreement stays in full force for as long as the Data Processor processes Personal Data, e.g. in the context of an exit transition, in which case this Data Processing Agreement terminates automatically at the moment the exit transition is concluded.

13.3 Termination or expiration of this Data Processing Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to Article 3.2.

14. Severability

14.1 In the event that any provision of this Data Processing Agreement is or becomes invalid, void or otherwise unenforceable, the remaining provisions of this Data Processing Agreement will remain in full force. In that case, the parties will consult with each other to replace the invalid, void or otherwise unenforceable provision by an enforceable alternative provision. In doing so, the parties will take the utmost account of the purpose and purport of the invalid, annulled or otherwise unenforceable provision.

15. Governing law and competent court

15.1 This Data Processing Agreement is governed by the laws of England. Any disputes arising from or in connection with this Data Processing Agreement shall be brought exclusively before the competent court of England.

The Parties hereto have caused this Data Processing Agreement to be executed by its duly authorized representatives

Data Controller	**Data Processor**
_____	_____
Name:	Name:
Title:	Title:
Date:	Date:

Version 1.1

Last edited on 7 June 2019

Annex 1: Contact information

Contact information of the data protection officer of the Data Controller:

_____
_____
_____
_____
_____
_____

Contact information of the data protection officer/compliance officer of the Data Processor:

Prowise UK Limited
Mr L. Loeff (privacy officer)
(+31) (0) 495 497110
privacy@prowise.com

Annex 2: personal data categories and purposes and sub-(sub-) processors

Categories of data subjects, Personal Data and Processing Operations

In connection with the Data Processor developing, maintaining and hosting the web based service called Prowise Learn (hereinafter: "Services") on behalf of the Data Controller, the Data Controller gives the Data Processor the instruction (or grants consent) to process the following data for the purposes set out below:

1. Data processing purposes

Processing that forms an integral part of the Services

The processing takes place to enable educational institutions to provide education and follow the progress thereof and to be able to follow the progress of pupils and provide them guidance.

When the Services are being used, the following processing takes place:

- the storage of learning and test results;
- receiving back learning and testing results;
- the assessment of learning and testing results in order to obtain learning material and test material that is tailored to the specific learning needs of a pupil;
- the assessment of a pupils learning and test results in relation to the results of a group of pupils to gain insight into how a student performs in relation to this group (for example: percentile scores);
- analysis and interpretation of learning results;
- the delivery/taking into use of the Services;
- obtaining access to the Services, and external information systems, including identification, authentication and authorization;
- the security, control and prevention of abuse and improper use and the prevention of inconsistency and unreliability in the processed Personal Data;
- the continuity and proper functioning of the Services, including having maintenance carried out, making a backup, making corrections after errors or inaccuracies found and receiving support;
- research and analysis on the basis of strict conditions, comparable to existing codes of conduct in the field of research and statistics, for the (optimization of) the learning process, the Services or the policy of the Data Controller;
- being able to make fully anonymised Personal Data available by the Educational Institution for research and analysis purposes in order to improve the quality of education;
- making Personal Data available to the extent necessary to comply with the legal requirements imposed on digital educational resources;

- the implementation or application of another law.

Optional processing:

When using the Services, other forms of processing may also take place, depending on the choices, preferences or setting of the Data Controller:

- the ability to exchange learning and test results with student administration systems of the Data Controller;
- the ability to exchange learning and test results with dashboards that the Data Controller uses;
- some contact details are optional, such as the telephone number of teachers/administrators and the address of pupils;
- Some contact details are optional, such as the telephone number of teachers/administrators and the email address of pupils;
- Processing of the email address for newsletters is optional and is done via opt-in;
- The retention of personal data for research and product optimization projects, see article 2 below for explanation.

2. Retention periods and scientific research

Personal Data of pupils and teachers of educational institutions will be retained for up to 12 months after the end of the subscription to the Services, unless the Data Controller explicitly requests a shorter storage period. This gives educational institutions the opportunity to look back for another year if they still want to know how pupils performed with the Services. If, for example, an educational institution switches to a different learning tool, this also enables the educational institution to compare learning results from the new product with the Services. In addition, it enables educational institutions to go back on their decision to stop using the Services within a period of 12 months and pupils can continue where they left off.

Data is stored for scientific research in completely anonymous form. For scientific research the anonymised data can also be made available to third parties.

3. Specification of personal data categories

Data subjects: Users - administrators / teachers

Category	**Explanation**
Contact details	Name, first names, e-mail address, telephone number (optional)
Education participant number	An administration number that identifies participant
School/institution information	School name, class name
User settings and actions	Number of logins, actions that teacher performs at class level such as game setting

Technical data	- Browser identification (user agent) in order to see which software is used by the customer and to solve problems - IP address for internal purposes (insight into user statistics) and to prevent abuse (network overload)

Data subjects: Users - players (children, pupils, adults)

Category	**Explanation**
Contact details	Name, first names, gender, month of birth, school year, e-mail address (optional)
Education participant number	An administration number that identifies participant
School/institution information	School name, teacher, class name
Learning achievements	Completed exercises including answers and response time Data derived thereof, such as skills scores, learning goals scores and percentile scores
User settings and actions	This includes, among other things, rewards, available games, chosen difficulty levels, number of logins and watched instruction videos
Technical data	- Browser identification (user agent) in order to see which software is used by the customer and to solve problems - IP address for internal purposes (insight into user statistics) and to prevent abuse (network overload)

4. Sub-processors and country location

- Oefenweb.nl B.V., based in the Netherlands (operating the Services)
- Prowise B.V., based in the Netherlands (support/helpdesk/development)

5. sub-sub processors and country location

- Leaseweb, based in the Netherlands (hosting provider)
- Hetzner, based in Germany (hosting provider)

6. Version and amendments

Data Processor may update the content of this Annex 2 from time to time. The most current version is always available on https://www.prowise.com/en/world-of-education/. In the event of important changes, such as adding (sub) processors, Data Processor will actively inform the Data Controller about this (for example by email). After being notified of a (proposed) change, Data Processor has 30 days to object to a change, stating the reasons of the objection. If there is no such notification, the change will be regarded as accepted by Data Controller.

Annex 3: Security measures

1. Access to personal data

The Data Processor makes sure that an authorisation policy is in order to ensure that employees only have access to Personal Data in so far as this is necessary for the purposes of their work.

Employees and data	Actions
Customer services employees have access to information about the subscription and its use.	Administrative actions and end-user support.
Experts in the development and analysis of learning materials have access to sets of results relating to the use of these learning materials.	Analysis of the learning materials aimed at improvement of the material,, development and optimisation of adaptive learning materials, detection and improvement of errors in the operation of the digital learning resources. In some cases, also answering specific questions relating to learning outcomes.
IT and database managers and developers have access to the Services and associated (live) databases.	The actions taken by the IT and database managers are designed to ensure the availability, continuity and optimisation of ICT systems and software.

2. Measures to protect personal data from misuse

Organisation of information security and communication processes

- a Privacy & Security board who identifies risks associated with the processing of personal data, raises awareness of security issues, checks facilities and takes measures which are designed to ensure compliance with the information security policy.
- Information security incidents are documented and used to optimise the information security policy.
- a process for communication around information security incidents is implemented and documented.

Employees

- Confidentiality statements are signed by and information security agreements are concluded with personnel (both internal and external).
- awareness is promoted, education and training in the field of privacy and information security.
- an authorisation policy has been implemented in order to ensure that employees only have access to Personal Data in so far as this is necessary for the purposes of their work.

Physical security and continuity of resources

- Personal data is only processed in a physical environment which is suitably protected against external threats. The data centers of the hosting providers are ISO 27001 certified.

- Geo-redundant backups offer further assurance of the continuity of services and the availability of the Personal Data. In other words, in the event of a serious incident at the primary location (e.g. flooding, attack or fire), the data will be available at an alternative, secure location.
- Regular (encrypted) backups are made to ensure the continuity of services. These backups are treated as confidential and stored in a secure environment.
- The locations where data is processed are periodically tested and maintained and periodically evaluated for security risks.

Network, server and application security and maintenance

- The network environment in which data is processed is strictly secured. Traffic flows are separate and measures have been implemented to prevent misuse and attacks.
- The environment in which Personal Data is processed is monitored in order to detect attacks, break-ins or attempted break-ins as quickly as possible.
- The virtual learning environments in which Personal Data is processed are created on the basis of a multi-stage software development process. Best endeavours are used to ensure that the latter is always implemented in such a way as to prevent security breaches.
- Patch management ensures that the latest (security) patches are periodically installed on systems.
- On local work stations and servers suitable measures are taken to prevent malicious software or functionality being installed.
- Cryptographic measures (hashing), of a quality which is generally regarded within the industry as secure, are applied to passwords in order to ensure that this data is stored securely. The only exception to this is passwords of users which they have not entered themselves in order to facilitate the password management of teachers and managers.
- Login processes use encrypted connections.
- The exchange of Personal Data between the Data Controller and the Services is encrypted.

3. Measures to identify weak spots

Security is periodically reviewed. This includes, amongst others, an internal vulnerability audit and the reviewing of best practices (e.g. OWASP) in the field of security.

Annex 4: Transfer to countries outside the EEA

Transfers to countries outside the European Economic Area without a suitable level of protection for which the Data Controller has granted its authorisation:

NONE