ANNEX 2. The Data Processing Agreement of OPIQ's Service

This data processing agreement is concluded between the parties mentioned below.

1. Parties

The customer (hereinafter referred to as 'Controller')

and

Star Cloud OÜ (hereinafter 'Processor' or 'OPIQ')

The Controller and the Processor are hereinafter referred to jointly as 'Parties' and separately as 'Party'.

2. Definitions

2.1. **Applicable data protection legislation** – any applicable legislation relating to the protection and security of data, including the directive on privacy and electronic communications (directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) and the General Data Protection Regulation (regulation 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, and repealing Directive 95/46/EC) and their amendments, substitutes, or extensions (collectively: EU legislation), all mandatory national laws implementing EU legislation and other mandatory data protection or data security directives, laws, regulations, and decisions that are in force at the respective time.

2.2. **Personal data** – data related to an identified or identifiable natural person. An identifiable natural person is a person who can be identified, directly or indirectly, on the basis of an attribute.

2.3. **Sub-processor** – processor of personal data involved to the extent necessary for the management and technical operation of OPIQ's services and ancillary services.

3. Background

3.1. The Processor grants the Controller access to the online platform OPIQ on the basis of a service agreement concluded between the Parties (hereinafter referred to as the 'Agreement').

3.2. The purpose of this Data Processing Agreement is to ensure the protection and security of personal data transferred by the Controller to the Processor under the Agreement.

3.3. In connection with the Agreement, the Processor will, on behalf of the Controller, process personal data received from the Controller, for which the Controller is the controller of personal data in accordance with the applicable data protection legislation.

3.4. With regard to the data of the OPIQ e-shop, Star Cloud OÜ is the Processor of personal data and the Processor of data related to payments is Maksekeskus AS for private users and eOppi for legal customers.

3.5. The OPIQStat service is intended for managing generalised usage statistics, for example in the view of a specific work or subject, and does not display user-based statistics.

3.6. OPIQ is an online platform for making e-study materials and related services available. OPIQ and the user of the services contained therein provide us with the information necessary for the convenient use of these services. OPIQ has many personalised e-services, so the system needs to know the respective personal data and their contact information. Without the necessary information, many services are not possible.

4. The obligations of the Controller

4.1. The Controller agrees and confirms that the processing of personal data by the Controller in the framework of the performance of the Agreement is lawful in accordance with the applicable data protection legislation.

4.2. The Controller is responsible for ensuring that the users designated by the Controller have a reasonable basis for accessing OPIQ's service and its content.

4.3. The Controller agrees and confirms that they have authorised and authorise the Processor to process personal data on behalf of the Controller throughout the processing of personal data in connection with the Agreement.

4.4. The Controller agrees to provide the Processor upon request with the necessary information and documentation to fulfil the obligations of the Controller arising from the applicable data protection legislation.

5. The obligations of the Processor

5.1. The Processor ensures that the processing of relevant personal data arising from the Agreement by them complies with the requirements of the applicable data protection legislation, the terms of the Agreement, and this Data Processing Agreement, and that the rights of data subjects are duly protected. The Processor and third parties employed or involved by the Processor may process personal data only in accordance with the requirements of this Data Processing Agreement and the Agreement and following other instructions issued or documented by the Controller as deemed necessary.

5.2. The personal data processed by the Processor on the basis of this Data Processing Agreement, the purposes, deadlines, and security measures are described in Annex A to this Data Processing Agreement.

5.3. The Processor does not process personal data to a greater extent than is necessary for the performance of the Agreement and the Data Processing Agreement by the

Processor. The Processor agrees that, in the absence of explicit written consent, they do not have the right to process personal data for purposes other than those agreed in the Agreement and the Data Processing Agreement. If mandatory European Union or national legislation applicable to the Processor prohibit the Processor from performing the Agreement or the instructions given, or alternatively require further processing beyond the Agreement or the Data Processing Agreement, the Processor will immediately inform the Controller of the relevant legal requirement prior to processing, as reasonably possible, or informs the Controller that the Processor cannot fulfil the Agreement or the given instructions. In addition, the Processor will immediately inform the Controller if they consider that the instruction given by the Controller infringes upon the applicable data protection legislation.

5.4. The Controller will keep the personal data confidential and ensure that all persons authorised to process the personal data are informed of their confidential nature, have received appropriate training on their responsibilities, and are bound by an appropriate or legally binding obligation of confidentiality. The respective obligation of confidentiality remains in force after the termination of this Data Processing Agreement and/or the Agreement.

5.5. The Controller will implement appropriate technical and organisational measures to protect the personal data processed against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure. Such measures ensure a level of security commensurate with the risks of processing.

5.6. Considering the nature of the processing and the information available, the Controller will also assist the Processor in ensuring that the Processor fulfils their obligations regarding the security of personal data, such as data breach notifications, risk and impact assessment, and consultation under applicable data protection legislation.

5.7. In the event of an actual or reasonably suspected breach pertaining to personal data or other threatening enforcement proceedings against the Processor concerning the processing of personal data under the Data Processing Agreement, the Processor will notify the Controller in writing without delay and no later than forty-eight (48) hours after becoming aware thereof. After obtaining the prior approval of the Controller, the Processor will try to resolve the situation quickly and prevent further damage and mitigate the effects of the respective case. In the notification, the Processor will provide the Controller with all data necessary for the Controller to comply with its notification obligation and to eliminate and mitigate the effects of the personal data breach in accordance with the applicable data protection legislation. Where possible and reasonable, the Processor will provide appropriate remedial services to data subjects upon request.

5.8. The Processor will also document the personal data breaches related to the Agreement, outlining the circumstances of the breach, its consequences, and the

corrective measures taken. These documents must enable the supervisory authority to verify compliance with the applicable data protection legislation. The documents may contain only the information necessary for that purpose.

5.9. The Processor will, at the request of the Controller and at no additional cost, cooperate and assist the Controller with information on appropriate technical and organisational measures to ensure the data subject's rights under applicable data protection legislation, including:

5.9.1. submitting a copy of the personal data of the data subject to the Controller;

5.9.2. opening, correcting, deleting personal data, or restricting the processing of personal data.

5.10. The Processor will provide the requested assistance with the necessary documents and information within ten (10) days of the request of the Controller.

5.11. If the data subject, supervisory or government agency, or another third party requests personal data processed by the Processor under the Agreement, the Processor directs the respective request to the Controller. The Processor is not allowed to disclose personal data or other information concerning the processing of personal data without the prior written consent of the Controller unless the Processor is required to disclose such data under mandatory European Union or national legislation. In the latter case, the Processor will immediately notify the Controller of the request to the extent permitted by law.

5.12. The Processor will, without charge to the Controller, provide all data and documentation and provide the assistance necessary for the Controller to comply with all the requirements of the applicable data protection legislation and to prove compliance with these requirements with regard to personal data related to the Agreement. In addition, the Processor will allow and facilitate audits by regulatory and/or supervisory authorities.

5.13. The Processor must always keep and make available up-to-date information on the processing activities, including the name, contact details, representative (including the data protection officer, if applicable), and location of each legal entity acting as a (sub)processor, the types of processing carried out on behalf of the Controller, and, where applicable, on the international transfer of data (including the country (countries) concerned and the documentation on the applicable transfer mechanisms). The Processor will, at the request of the Controller and without undue delay, provide the Controller with the documents provided for in this clause so that the Controller can comply with the applicable data protection legislation.

5.14. The Processor will ensure that the Controller has the right to inspect and audit the premises of the Processor (and ensure that the Processor has equivalent inspection and auditing rights regarding third party sub-processors) to verify that the processing activities and related technical and organisational security measures are in accordance with the obligations set out in the Data Processing Agreement, the

Agreement, or applicable data protection legislation. The following applies to the performance of such audits.

5.15. The Controller has the right to carry out audits during normal business hours, with reasonable prior notice. Such audits must not interrupt the business of the Processor and may be carried out either by employees of the Controller or by employees of another company providing a service to the Controller under contract (professional third party), provided that the third party providing the service under the contract has confidentiality obligations reasonably acceptable to the Processor. The Controller will bear the costs of its audits. However, if the audit reveals an inconsistency or non-compliance caused by the Processor or its affiliates, consultants, subcontractors, or other representatives, the Processor will bear the costs of the audit of the Controller.

6. Transfer of personal data to a third party

6.1. The Processor does not have the right to transfer personal data to a third party or to grant access to a third party, e.g. by granting remote access to personal data, or to involve sub-processors to process personal data (all mentioned transferring and sub-processing activities are collectively referred to as transferring data to a third party) without prior written consent from the Controller. In the case of granting such consent, the same data protection obligations as provided for in this Data Processing Agreement will apply to the respective third party before the transfer of personal data by the Processor. The consent is not required regarding the sub-processors (service providers) listed in Annex A to this Data Processing Agreement.

6.2. This consent is valid until the earliest of the following events: (i) if the Controller notifies the Processor of the withdrawal of the consent; or (ii) if the Processor notifies the Controller that the Processor no longer uses the approved third party for that purpose.

6.3. If the Controller does not consent to the transfer of personal data to a third party for a reason that the Controller deems reasonable, the Processor will continue to perform the Agreement and the Data Processing Agreement until the earliest of the following events: (i) the Parties have agreed upon termination of the Agreement pertaining to the processing of personal data and secured the return (or deletion, as the case may be) of the relevant personal data to the Controller, or have agreed to transfer the Agreement to a new service provider, which in no case takes more than three (3) months from the date of receipt of such a request by the Controller, or (ii) the Parties have agreed on how to proceed with the performance of the Agreement, including relevant costs and in a manner reasonably acceptable to the Controller.

6.4. If the third-party sub-processor does not comply with the applicable data protection legislation or does not comply with the data protection obligations arising from the Agreement with the Processor, the Processor remains fully responsible to the

Controller for the third party's performance of the obligations under applicable data protection legislation and the relevant agreement.

7. Termination of processing of personal data

7.1. If the processing of personal data is no longer necessary under the Agreement or if the respective Agreement is completed or terminated, the Processor will delete or return to the Controller on their discretion all personal data processed by the Processor under the Agreement, unless otherwise required by applicable data protection legislation. Upon deletion of personal data, the Processor will immediately confirm the destruction of personal data at the request of the Controller.

7.2. If the Controller requests the return of personal data, the Processor will return all personal data in the manner and form requested by the Controller and delete all existing copies thereof.

8. Indemnification and liability

8.1. The liability set forth in this clause and its limitations apply in accordance with and in addition to the liability and indemnity clauses of the Parties set forth in the Terms of Service.

8.2. Compensation for the protection of personal data

8.2.1. Notwithstanding the possibly contrary clauses in the Agreement regarding the liability or indemnification obligation of the Processor, it is expressly agreed that if the Processor violates the obligation of confidentiality, security, and/or protection of personal data under the Agreement and/or this Data Processing Agreement) with personal data processed under the Agreement, the Processor will protect the Controller against the following and indemnify the related damage (which is considered direct damage within the meaning of the Data Processing Agreement):

8.2.1.1. fines or penalties for such breaches imposed by governments, regulators, public authorities, or enforcement bodies;

8.2.1.2. amounts paid to third parties whose rights have been infringed on (which may include data subjects, the Controller's customers, employees, managers, and consultants) as damages or conciliation fees as a result of the breach;

8.2.1.3. reasonable costs of providing the required breach notification (and the required notice responses) to the persons whose rights were breached, public authorities, regulatory authorities, and/or other public bodies or agencies.

8.2.2. The above limitations on compensation by the Processor do not apply to damages resulting from wilful misconduct, gross negligence, damage to health, or statutory liability.

8.2.3. The Processor will immediately inform the Controller if proceedings are initiated against them which may result in a claim for damages or a fine under EU legislation or under additional national legislation to the General Data Protection Regulation. When such proceedings are initiated, the Processor will: (a) provide the Controller with details (including specific allegations pertaining to the breach); (b) provide the Controller with the information and assistance requested by the Controller; and (c) not prevent or challenge the active participation of the Controller in the proceedings (using legal aid at their own expense).

8.3. Liability

8.3.1. Notwithstanding the possibly contrary clauses in the Agreement regarding the liability or indemnification obligation of the Processor, it is expressly agreed that the Processor is liable without limitation for all claims, damages, fines, penalties, costs, expenses, amounts, and fees incurred by the Controller to the customer or cooperation partner of the Controller or third party by the activities of the Processor or their employee or subcontractor in violation of this Data Processing Agreement, the Agreement, and/or the applicable data protection legislation, deriving from the Processor's indemnification obligation under the personal data protection compensation provision above.

8.3.2. The obligations set out above will continue to apply after the termination, cancellation, or expiration of this Data Processing Agreement and/or the Agreement.

9. Validity

This Data Processing Agreement is valid as long as the Processor processes personal data on behalf of the Controller under the agreement.

10. Suggestions, questions, complaints

Please send all suggestions, questions, and complaints to the e-mail address info@opiq.fi.

11. Dispute Resolution

Disputes arising out of or in connection with the Terms of Service and the Data Processing Terms will be resolved through negotiations. In case of failure of negotiations, the Parties agree that disputes arising from this Agreement will be settled in Harju County Court pursuant to the legislation in force in the Republic of Estonia.

ANNEX A to the Data Processing Agreement of OPIQ's Service

Description of the categories of personal data, categories of data subjects, processing purposes, sub-processors, data retention periods, and security measures taken by the Processor within the OPIQ's Service and Ancillary Services.

The composition of the list below depends on the services selected for each specific data subject and the details of their use.

1. **Personal data and purposes of their processing**
   - 1.1. The basis for the processing of personal data is the fulfilment of OPIQ's legal obligations, the fulfilment of the contractual service to the customer, OPIQ's legitimate interest, and the consent taken from the user if the law provides for the obligation to seek consent (especially commercial notices).
   - 1.2. The purposes of processing the personal data listed below are the creation and management of a contractual user account, the provision of a contractual service, and provision of its quality and ease of use, user identification, and, if necessary, the required connection to the customer, contacting the user, accounting for royalties, management and accounting of the e-shop orders, statistics, accounting, marketing, user support, compliance with security requirements, operation of the service between service providers.

2. **Personal data to be processed**
   - 2.1. Account creation, account details and related information (first and last name, personal identification code, email address, phone number, hardware, role, subjects, study groups, user institution and class, invitation from another user + inviter details, service usage time, and the user's IP address).
   - 2.2. Stuudium key, social media key on Facebook and Google, E-kool account key, user name, and email address, HarID account key, user name, email address, personal identification code.
   - 2.3. Licence in OPIQ.
   - 2.4. User logs in OPIQ.
   - 2.5. User-added study material (file, text), answers to tasks solved in the study material, notes and comments added to the study material.
   - 2.6. Information about the student's performance (student's answers to the task, automatically checked feedback, teacher feedback in the form of corrections, grades, or other form).
   - 2.7. Created/modified records.
   - 2.8. Information about the finished study material, tasks, and bookmarks in the study material.

2.9. First and last name, email address, place of work (publisher) of the CMS (content management system) author, editor, etc. with whom OPIQ has a contractual relationship.
2.10. Accounting data (invoices paid by private user by name, term of license). When using a payment service, the user's bank account number.
2.11. Usage records, e.g. browsing history, usage history of interactive components.
2.12. Helpdesk contact history.
2.13. Search, query history, browsing history, usage history of interactive components.

3. Data subjects

3.1. Student
3.2. Parent
3.3. Teacher
3.4. Representative of a legal entity (school or local government)
3.5. Private user
3.6. OPIQ's website visitor
3.7. E-shop subscriber/buyer
3.8. Authors, editors, designers, technical editors of the study material

4. Access to personal data

4.1. Access to personal data contained in OPIQ is restricted as follows:
4.1.1. if OPIQ's user is a school through its authorised representative, they have access to the following information: student's name, class teacher's name, subject teacher's name, class (class course), email, and study kits used in the student's OPIQ records;
4.1.2. a schoolteacher who uses OPIQ has access to the following information related to their subject: a list of students in the records, the email addresses of the students in the school, and information about their subject's assignments and their results and performance (statistics);
4.1.3. as a class teacher, a schoolteacher has access to the following information in addition to the teacher's rights related to the teaching of their subject: a list of all records related to their class (later also work and statistics);
4.1.4. students using OPIQ have access to their data, their study materials, sent (assigned) study assignments, and their statistics. It is possible for a student to link parents to their account;
4.1.5. the parent has access to their data, their child's study materials, assigned tasks, and their outcomes. The parent cannot mark or add study materials and cannot solve or send assignments issued to the student.

5. Retention periods for personal data

5.1. Data will be deleted automatically once the purpose of the processing has been fulfilled. As a rule, deletion depends on the agreement entered into with the customer or deletion by the customer.

5.2. Compliance with the requirements arising from the legislation of the Republic of Estonia and therefore the term prescribed by law is applied (e.g. Accounting Act 7 years + current financial year).

5.3. The personal data of OPIQ's user will be deleted 5 years after the end of the study. The purpose of the five-year retention of the account is to enable supporting the learner if they wish to use their data stored in OPIQ after completing general education (e.g. at university, vocational education) or due to school interruptions. It supports the continuation or return of a meaningful learning journey.

5.4. Deletion of personal data will take place immediately on the basis of a written request of the data subject, except for data with a data storage obligation prescribed by law and data requiring permission of the customer (school or local government) to be deleted.

5.5. Where possible, pseudonymisation of data is applied, where the purpose can also be achieved with pseudonymous data.

5.6. Activity logs are kept for 1 year for security purposes.

6. Sub-processors of personal data

6.1. Agile Works AS; www.agileworks.eu.

6.2. Microsoft Azure (Cloud Computing Platform & Services), azure.microsoft.com/en-us/.

6.3. ElasticSearch, www.elastic.co/.

6.4. SendGrid, sendgrid.com.

6.5. Confluent Cloud Kafka, www.confluent.io/.

6.6. Google Analytics, https://analytics.google.com/analytics/web/provision/#/provision.

6.7. Star Cloud as the Controller of personal data (where Star Cloud processes personal data for its own purposes) discloses user information to third parties only in the following cases:

6.7.1. information is required in civil or criminal proceedings;

6.7.2. the transfer of personal data outside the European Union is done according to the requirements of the General Data Protection Regulation. A level of data protection equivalent to that of the European Union is ensured by the standard contractual clauses (SCC) of the Data Protection Agreement.

7. Security measures

OPIQ uses the latest cloud technologies and the highest security standards. Among other things, access management, authentication services, data encryption, security testing, etc. are used. For more information on security measures, please contact Star Cloud.

8. Contact

OPIQ’s service provider is Star Cloud OÜ, commercial registry code 12731921, email info@opiq.fi, phone 5323 7793.