Data processing agreement

pursuant to Article 28 (3) of Regulation 2016/679 of the European Parliament and of the Council (GDPR) with regard to the processing of personal data by the Data Processor

between

Customer

hereinafter referred to as "the data controller"

and

Wittario AS
Org.nr. 915979025
Værftsgata 1 C
1511 Moss
Norway

hereinafter referred to as the "Data Processor", each of which is a "Party" and together constitutes the "Parties". HAVE AGREED to the following Standard Contractual Clauses (the "Terms") with a view to complying with the GDPR and ensuring the protection of the fundamental rights and freedoms of natural persons.

Content

2. Introduction 3
3. Rights and obligations of the controller 3
4. The data processor acts according to instructions 4
5. Confidentiality 4
6. Safety of treatment 4
7. Use of sub-processors 5
8. Transfer to third countries or international organisations 6
9. Assistance to the data controller 7
10. Notification of personal data breaches 8
11. Deletion and return of data 9
12. Auditing, including inspection 9
13. The parties' agreement on other matters 9
14. Entry into force and termination 9
15. Contact persons of the data controller and the data processor 10
Appendix AOncture of the processing 11
Appendix BUnder Data Processors 12
Appendix CInstruks for the processing of personal data 14
Appendix DPart's regulation of other matters 17

1. Introduction

1. These Terms and Conditions set out the rights and obligations of the Controller and the Processor when the Processor carries out the processing of personal data on behalf of the Controller.

2. These Terms and Conditions are designed to ensure the parties' compliance with Article 28(3) 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, and repealing Directive 95/46/EC (GDPR).

3. In connection with the provision of "*Wittario with app/dashboard/web solution*", the data processor processes personal data on behalf of the data controller in accordance with these Terms.

4. The Terms take precedence over any corresponding provisions of any other agreements between the parties.

5. There are four appendices to these Terms, and the appendices form an integral part of the Terms.

6. Appendix A contains further information on the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

7. Appendix B contains the Controller's terms and conditions for the Data Processor's use of sub-processors and a list of sub-processors that the Controller has approved.

8. Appendix C contains the controller's instructions regarding the data processor's processing of personal data, a description of the security measures that the data processor must implement as a minimum, and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions on other activities that are not covered by the Terms.

10. The terms and conditions and associated appendices must be kept in writing, including electronically, by both parties.

11. These Terms do not relieve the Data Processor from any obligations imposed on the Data Processor by the General Data Protection Regulation or other legislation.

2. Rights and obligations of the controller

1. The controller is responsible for ensuring that the processing of personal data is carried out in accordance with the GDPR (see Article 24 of the GDPR), applicable personal data protection provisions in Union or Member State[1] law and these Terms.

[1] References to "Member States" in these Terms shall be understood as referring to states that are part of the European Economic Area (EEA States).

2. The data controller has the right and duty to determine the purpose of the processing of personal data and the means to be used.

3. The data controller is responsible for, among other things, ensuring that there is a legal basis for the processing of personal data that the data processor is instructed to do.

3. The data processor acts according to instructions

1. The Data Processor shall only process personal data on documented instructions from the Data Controller, unless otherwise required by Union or Member State law to which the Data Processor is subject. These instructions shall be specified in Appendices A and C. Subsequent instructions may also be given by the controller while personal data is being processed, but the instructions shall always be documented and kept in writing, including electronically, together with these Terms.

2. The Processor shall promptly notify the Controller if, in the opinion of the Processor, an instruction from the Controller is in breach of the GDPR or applicable personal data protection provisions of Union or Member State law.

4. Confidentiality

1. The Processor may only grant access to Personal Data processed on the Controller's behalf to persons subject to the Data Processor's instructional authority who have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of people who have been granted access will be reviewed continuously. On the basis of such a review, access to personal data may be closed, if it is no longer necessary, and the personal data shall then no longer be available to these persons.

2. The data processor shall, at the request of the data controller, be able to demonstrate that the persons in question, subject to the data processor's authority to instruct, are subject to the above-mentioned duty of confidentiality.

5. Safety of treatment

1. Article 32 of the GDPR states that, taking into account technical developments, the costs of implementation and the nature, scope, purposes and context of the processing, as well as the risks of varying probability and severity to the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to achieve a level of security appropriate to the risk.

   The controller shall assess the risks to the rights and freedoms of natural persons arising from the processing and implement measures to address these risks. Depending on relevance, the measures may include:

   a. pseudonymization and encryption of personal data

   b. the ability to ensure the continued confidentiality, integrity, availability and robustness of the processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, analysing and assessing the effectiveness of the treatment's technical and organisational security measures.

2. According to Article 32 of the GDPR, the data processor – independently of the controller – must also assess the risks to the rights and freedoms of natural persons that the processing poses, and implement measures to address the risks. For the purposes of this assessment, the Controller shall make available to the Processor the necessary information that enables it to identify and assess such risks.

3. The Data Processor shall also assist the Data Controller in complying with the Data Controller's obligations pursuant to Article 32 of the General Data Protection Regulation, by, among other things, making available to the Data Controller the necessary information about the technical and organisational security measures that the Data Processor has already implemented in accordance with Article 32 of the General Data Protection Regulation, as well as all other information necessary for the Data Controller to be able to comply with its obligations cf. Article 32 of the General Data Protection Regulation.

   If, in the opinion of the Controller, addressing the identified risks requires the implementation of additional measures than those already implemented by the Processor, the Controller shall specify these measures in Appendix C.

6. Use of sub-processors

1. The data processor must comply with the conditions set out in Article 28 (2) and (4) of the GDPR in order to make use of another data processor (a sub-processor).

2. Thus, the Data Processor must not use a sub-processor to fulfil the Terms without prior general *written approval* from the Data Controller.

3. The data processor has the data controller's general approval to use sub-processors. The Data Processor shall notify the Controller in writing of any planned changes relating to the addition or replacement of Sub-Processors with at least *30 days'* notice and thereby give the Controller the opportunity to object to such changes before engaging the described Sub-Processor(s). Longer notice deadlines for specific sub-processing services can be specified in Appendix B. The list of sub-processors that the controller has already approved is set out in Appendix B.

4. Where the Processor engages a Subprocessor to carry out specific processing activities on behalf of the Controller, the Subprocessor shall be subject to the same obligations with respect to the protection of personal data as set out in these Terms, by means of an agreement or other legal document under Union or Member State law, providing in particular sufficient guarantees that technical and organisational measures will be implemented measures to ensure that the processing complies with the requirements of this Regulation.

   The Data Processor is therefore responsible for requiring the Sub-Processor to comply with the Data Processor's obligations under these Terms and the General Data Protection Regulation as a minimum.

5. A copy of such Sub-Processing Agreement and any subsequent amendments shall – at the Controller's request – be sent to the Controller, who in this way has the opportunity to ensure that the Sub-Processor is subject to the same obligations with regard to the protection of personal data as set out in these Terms. Commercial provisions that do not affect the personal data protection law content of the sub-data processing agreement are not subject to the requirement for a copy to the data controller.

6. The Data Processor shall include in the Sub-Processing Agreement the Controller as a third-party beneficiary in the event of the Processor's bankruptcy, so that the Controller can step into the Data Processor's rights and assert them against the Sub-Processor, which enables the Controller, for example, to instruct the Sub-Processor to delete or reverse the Personal Data.

7. If the Sub-Processor fails to fulfil its personal data protection obligations, the Processor becomes fully liable to the Controller with regard to the fulfilment of the Sub-Processor's obligations. This does not affect the data subjects' rights under the GDPR – in particular those enshrined in Articles 79 and 82 of the GDPR – vis-à-vis the controller and the data processor, including the sub-processor.

7. Transfer to third countries or international organisations

1. The data processor may only transfer personal data to third countries or international organisations on documented instructions from the data controller, and such transfer must always take place in accordance with Chapter V of the General Data Protection Regulation.

2. Where the transfer of personal data to third countries or international organisations, which the Processor has not been instructed by the Controller to carry out, is required by Union or Member State law to which the Processor is subject, the Processor shall inform the Controller of those legal requirements prior to the processing, unless such a right prohibits such a request for reasons of important public interest notification.

3. Thus, without documented instructions from the Data Controller, the Data Processor may not, within the framework of these Terms:

    a. transfer personal data to a controller or processor in a third country or an international organisation;
    b. entrust the processing of personal data to a sub-processor in a third country;
    c. process the personal data in a third country

4. The controller's instructions with regard to the transfer of personal data to a third country, including the possible basis for transfer in Chapter V of the GDPR on which the transfer is based, shall be set out in Appendix C.6.

5. These Terms are not to be confused with standard contractual clauses as referred to in Article 46 (2) (c) and (d) of the GDPR and these Terms may not constitute a basis for the transfer of personal data under Chapter V of the GDPR.

8. Assistance to the data controller

1. The Processor shall, taking into account the nature of the processing and to the extent possible, by means of appropriate technical and organisational measures, assist the Controller in fulfilling its obligation to respond to requests made by the Data Subject for the purpose of exercising its rights set out in Chapter III of the GDPR.

   This means that the data processor shall, as far as possible, assist the data controller in the data controller's fulfillment of:

   a. The duty to provide information when collecting personal data from the data subject
   b. the duty to provide information if personal data has not been collected from the data subject
   c. The data subject's right of access
   d. The right to rectification
   e. the right to erasure ("the right to be forgotten")
   f. the right to restriction of processing
   g. the duty to notify in connection with the correction or deletion of personal data or restriction of processing;
   h. The right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling;

2. In addition to the Processor's obligation to assist the Controller in accordance with the Terms 6.3., the Processor also assists, taking into account the nature of the processing and the information available to the Processor, the Controller with:

   a. the controller's obligation in the event of a breach of personal data security to without undue delay and whenever possible, no later than 72 hours after becoming aware of it, report the breach of personal data security to the competent supervisory authority, *the Data Protection Authority*, unless the breach is not likely to result in a risk to the rights and freedoms of natural persons;

   b. the controller's obligation to notify the data subject without undue delay of the personal data breach when it is likely that the breach will result in a high risk to the rights and freedoms of natural persons

   c. The controller's obligation to carry out an assessment of the consequences of the planned processing for personal data protection before processing (data protection impact assessment)

   d. the controller's obligation to consult with the competent supervisory authority, *the Norwegian Data Protection Authority*, prior to the processing if a data protection impact assessment indicates that the processing will entail a high risk if the controller does not take measures to reduce the risk.

3. The Parties shall specify in Annex C the appropriate technical and organisational measures through which the Processor shall assist the Controller, as well as the scope and extent of the assistance required. This applies to the obligations arising from Terms 9.1 and 9.2.

9. Notification of personal data breaches

1. In the event of a breach of personal data security, the Data Processor shall notify the Data Controller of the breach without undue delay after becoming aware of it.

2. The data processor's notification to the data controller shall, if possible, take place within *12 hours* after the data processor has become aware of the personal data breach, so that the data controller can comply with its obligation to report the breach to the competent supervisory authority, cf. Article 33 of the GDPR.

3. In accordance with Condition 9 number 2 (a), the Data Processor shall assist the Data Controller in reporting the breach to the competent supervisory authority. This means that the data processor shall assist in obtaining the information listed below, which, according to Article 33 (3) of the GDPR, must be stated in the controller's notification of the breach to the competent supervisory authority:

    a. the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data recordings affected;

    b. the likely consequences of the personal data breach

    c. the measures that the data controller has taken or proposes to take to deal with the personal data breach, including, if relevant, measures to reduce any harmful effects resulting from the breach.

4. The Parties shall set out in Appendix C all information that the Processor shall provide when assisting the Controller in reporting a breach of personal data security to the competent supervisory authority.

10. Deletion and return of data

1. Upon termination of the data processing services, the data processor shall *delete all personal data that has been processed on behalf of the controller and confirm to the controller that the data has been deleted*, unless Union or Member State law requires the retention of the personal data.

11. Auditing, including inspection

1. The Data Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations under Article 28 of the General Data Protection Regulation and these Terms. Furthermore, the Data Processor shall enable and contribute to audits, including inspections, which are carried out by the Data Controller or another auditor authorised by the Data Controller.

2. The procedures for the controller's audits, including inspections, of the processor and sub-processors are specified in Annexes C.7 and C.8.

3. The Data Processor undertakes to give the supervisory authorities, who under applicable legislation have access to the Data Controller's or the Data Processor's premises, or representatives acting on behalf of such supervisory authorities, access to the Data Processor's physical premises upon presentation of appropriate identification.

12. The parties' agreement on other matters

1. The parties may agree on other provisions relating to the data processing services, such as liability, as long as these other provisions do not directly or indirectly conflict with these Terms or are detrimental to the fundamental rights and freedoms of the data subject and the protection afforded by the GDPR.

13. Entry into force and termination

1. The Terms are effective on the date of signature by both parties.

2. Either party may request that the Terms be renegotiated if changes in law or inexpediencies in the Terms warrant this.

3. The terms and conditions apply for the duration of the data processing services. During this period, the Terms cannot be terminated, unless the parties agree on other terms that govern the provision of the data processing services.

4. If the provision of the Data Processing Services ceases, and the Personal Data has been deleted or returned to the Data Controller in accordance with Terms 11.1 and Appendix C.4, the Terms may be terminated with written notice by either party.

5. Signature

   On behalf of the data controller

   Name
   Position
   Phone number
   Email address
   Date
   Signature

   On behalf of the Data Processor

Name	Lars Gunnar Fledsberg
Position	CEO
Phone number	4794019520
Email address	lgf@wittario.com
Date	xx.xx.20xx
Signature	

14. Contact persons of the data controller and the data processor

1. The parties can contact each other via the contact persons below.

2. The parties undertake to inform each other on an ongoing basis about changes that apply to contact persons.

Name
Position
Phone number
Email address

Name	Lars Gunnar Fledsberg
Position	CEO
Phone number	+4794019520
Email address	lgf@wittario.com

Appendix A Information about the processing

A.1. The purposes of the Processor's processing of personal data on behalf of the Controller are:

To provide employees at Customer with training and development through the use of "Wittario with app/dashboard/web solution" which facilitates game-based learning with activity and the goal of increased learning outcomes.

A.2. The Data Processor's processing of personal data on behalf of the Controller shall primarily concern (nature of the processing):

Collecting, storing, organizing, analyzing, and reporting personal data related to employees' learning activities and performance.

Leadership facilitates a learning path by designing creative and self-correcting tasks. This learning path takes the form of a game, where the employees deliver e.g. practical answers via camera images, record audio recordings or by answering quizzes and reflection tasks. The game can be played indoors and outdoors, with or without physical activity. Outdoor games can be added to a predetermined route or with a distance requirement, allowing participants to move around in a physical outdoor setting.

A.3. The processing includes the following types of personal data concerning the data subjects:

- Contact information for the user: Name and e-mail
- Organization affiliation/entity ID
- Password
    i. Not stored in plain text.
- Contact information for the owner of the organization account; Name and contact information
- Organization (such as company, school, association, etc.)
- Results of games played, including responses to the games

A.4. The processing includes the following categories of data subjects:

All employees at the Customer.

A.5. The Processor's processing of personal data on behalf of the Controller may commence after the Terms have entered into force. The duration of the treatment is as follows:

The processing shall last for as long as the Data Processor delivers «Wittario with app/dashboard/web solution» to the Data Controller. Detailed description for «Deletion and return of data» can be found in dots 10.

Appendix B Sub-processors

B.1. Approved sub-processors

Upon entry into force of the Terms, the Controller authorizes the use of the following sub-processors:

NAME	ORG. NO.	ADDRESS	DESCRIPTION OF THE TREATMENT
Google Norway AS	988 588 261	C. J. Hambros place 2 D 0164 OSLO	Wittario stores data in the Google FireStore Database and Firebase Storage. Physical location For the data center, Frankfurt (European West 3).
Microsoft Norway AS	957 485 030	Lysaker torg 45 NO-1366 Lysaker	Wittario stores data in CosmosDb and Azure Storage. Physical location for The database center is Oslo (Norway East). Wittario's AI services process data in the Swedish data centers Sweden Central. The data processing takes place in Sweden Central to leverage specialized AI resources that are not available in Norway East. No data is stored in Sweden Central.
MixPanel			Wittario uses MixPanel to analyze general usage patterns in the product to have a data basis to improve the user experience. Data is stored in EU data centres (Europe-West4): https://docs.mixpanel.com/docs/privacy/eu-residency No direct personal data is stored in MixPanel, but the system uses a pseudonymized identifier (GUID) to distinguish unique users' actions within MixPanel.

NAME	ORG. NO.	ADDRESS	DESCRIPTION OF THE TREATMENT
			Examples of such actions are: *Starting Games* *Creating games* *Create an assignment* Only metadata related to the first action is transferred to MixPanel, none of the users' data (e.g. learning content, game replies, etc.) is transferred. More information about MixPanel as a data processor can be found here: https://mixpanel.com/legal/cdpa/
HubSpot CRM			Customer data is stored in HubSpot's CRM system for the purpose of managing Wittario's customer relationships, support and communication. HubSpot processes data under its DPA and is GDPR compliant: https://legal.hubspot.com/legal-stuff Wittario's data in HubSpot is stored in their European data center in Germany.
Linqur B.V		Nevelgaarde 8, 3466 ZZ Nieuwegein, Netherlands	Serves as provider of SCORM Proxy content. Only applies for customers using distributing courses through SCORM Proxy files. Linqur processes user identifiers (name, e-mail and unique LTI identifiers used for tracking progress from Wittario into the LMS) All data is stored in the Netherlands (EEA). DPA is in place.

Upon the entry into force of the Terms and Conditions, the Data Controller has approved the use of the above-mentioned sub-processors for the processing activity described for the data subject. The Data Processor may not – without the Controller's explicit written consent – use a Sub-Processor for a processing activity other than the one agreed for the person concerned or use another Sub-Processor for the described Processing Activity.

B.2. Notification for approval of sub-processors

See point 6 «Use of sub-processors».

Appendix C Instructions for processing personal data

C.1. Subject-matter/instructions for the processing

The data processor's processing of personal data on behalf of the data controller takes place by the data processor performing the following:

The Data Processor is instructed to collect, store, organize, analyze and report data to facilitate game-based learning in the app/dashboard/web solution. The processing shall be carried out in accordance with the agreement and the applicable privacy policy.

C.2. Information security

The level of security of the processing of personal data shall reflect the risks associated with the processing and the nature of the personal data. This means that the security measures must be proportionate and adapted to both the type of information and the consequences for the data subjects if something goes wrong (e.g. data breach, loss of data or unauthorized access).

Henceforth, the data processor has the right and duty to make decisions about which technical and organisational security measures are to be implemented in order to establish the necessary (and agreed) level of security.

The Data Processor shall nevertheless – under all circumstances and as a minimum – implement the following measures, which have been agreed with the Data Controller:

KIT stands for Confidentiality, Integrity and Availability, and is a key principle in information security and the GDPR (cf. Article 32 of the GDPR on security in the processing of personal data). The level of security shall reflect these principles to ensure a holistic approach to data protection.

- Risk assessment:
  - Regular assessments of security risks related to data processing
  - Testing the system (penetration tests) to uncover vulnerabilities
- Access control:
  - Only authorized users shall have access to the data. This includes:
    - Encrypted logins
    - Strict role and access management
    - Access logging and unauthorized access attempts
- Data protection:
  - Encryption of data both at rest and in transit
  - Control mechanisms to ensure correct storage and transmission of data
  - Regular backups to prevent data loss or corruption
  - Authenticating users entering, modifying, or deleting data
  - System notifications in case of suspicious changes or attempts to change data
  - Redundant servers and solutions to minimize downtime
  - Regular backups that can be restored quickly in case of failure
  - Monitoring system performance to ensure stability
- Privacy Policy Compliance:
  - Implementation of data minimization
  - Securing data during the processing process and during deletion
- Handling security breaches:
  - Notification procedures in the event of a security breach

    - Contingency plan for handling incidents such as data loss, technical failures, or denial-of-service attacks
- Security Level Scaling:
    - If the app or platform starts processing data as defined as special categories of data, the security level must be adjusted accordingly.

C.3 Assistance to the controller

The Data Processor shall, to the extent possible – to the extent and extent described below – assist the Controller in accordance with Terms 9.1 and 9.2 by implementing the following organisational measures:

- Provide data processor employees with the necessary training on information security and GDPR obligations to ensure they handle personal data safely
- Develop and implement internal procedures for processing personal data, including handling data subject requests and reporting security breaches
- Assist the Data Controller in responding to data subject requests under the GDPR, including access, rectification, deletion, and data portability
- Notify the data controller of any security breaches without undue delay, as well as assist with necessary investigations and measures
- Assist with the implementation of risk assessments and impact assessments (DPIAs) where necessary
- Ensure that subcontractors have corresponding technical and organisational measures in place to protect personal data
- Provide the controller with access to the necessary documentation to verify that personal data is processed in accordance with applicable regulations.
- Assist in connection with audits or inspections that the data controller, or supervisory authorities, wish to carry out

C.4 Retention period/deletion procedures

See point 10 About «Deletion and return of data", as well as Appendix A, item A5.

C.5 Location of treatment

Processing of personal data covered by the Terms may not, without the Controller's prior written consent, take place at locations other than the following:

The processing takes place within the EU/EEA, see location specified in Appendix B, item B.1.

C.6 Instructions for the transfer of personal data to third countries

Personal data shall not be transferred to a third country or international organisation. Processing must only take place within the EU/EEA.

C.7 Procedures for the controller's audits, including inspections, of the processing of personal data entrusted to the processor

In order to ensure compliance with the General Data Protection Regulation (GDPR) and the entered into data processing agreement, the Data Controller shall have the right to conduct audits, including inspections, of the Data Processor's processing of personal data. The audits shall be carried out in accordance with the following procedures:

- Notification of revision
    - The Data Controller shall notify the Data Processor in writing for 30 days prior to the audit
    - The notification must contain:

        - The purpose of the audit
        - Scope of the audit
        - Time and duration of the audit
        - What parts of the treatment and systems will be inspected
- Revision frequency and scope:
    - Audits can be carried out annually or more often as needed, e.g. in the event of suspected deviations, security breaches or changes in the data processor's systems.
    - The audit may include:
        - Physical premises where data is processed
        - Systems and technical solutions used for data processing
        - Access management and logging
        - Documentation of implemented technical and organizational security measures
        - Subcontractors' compliance
- Conducting an audit
    - The audit shall be carried out in a manner that does not unnecessarily interfere with the daily operations of the data processor.
    - The audit can be performed:
        - By the data controller himself
        - By a third party (independent auditor), appointed by the Data Controller
    - The Data Processor shall provide the necessary resources to support the audit, including:
        - Provide access to required documentation
        - Provide visibility into systems and processes where personal data is processed
        - Answering questions from the auditor
- Audit results and follow-up
    - After the audit, the data controller must prepare an audit report with findings and recommendations.
    - The report must be shared with the data processor, who:
        - Will review the findings
        - Shall prepare a plan for necessary corrective actions if nonconformities are discovered
        - Shall cooperate with the Data Controller to resolve identified issues within an agreed time limit
- Costs
    - As a general rule, audit costs are borne by the data controller.
    - If the audit reveals material breaches of the agreement or the data protection regulations, the data processor may be obliged to cover part of the costs associated with the audit.
- Third-party audits and certifications
    - If the Data Processor holds third-party certifications (f.eks. ISO 27001), the Data Controller may request a copy of the applicable certification reports as an alternative to physical auditing.
    - Such third-party audits can help reduce the need for extensive inspections.
- Confidentiality
    - The audit process and findings shall be treated as confidential information and not shared with unauthorized persons unless required by law.

Appendix D The parties' regulation of other matters

None.