Itslearning AS
P.O. Box 2686
5836 Bergen
Norway

t: +47 55 23 60 70
e: post@itslearning.com

Data Processor Agreement

BETWEEN

[CUSTOMER NAME_____]
ORG.NO. [ORGANISATION NUMBER_____]
(HEREINAFTER "DATA CONTROLLER")

AND

ITSLEARNING AS, IDENTIFIED IN THE STANDARD SERVICE SUBSCRIPTION AGREEMENT
(HEREINAFTER "DATA PROCESSOR")

1. Purpose

The purpose of this agreement is to regulate the rights and duties pursuant to the European Data Protection Legislation, including the GDPR (hereinafter referred to as "Applicable Data Protection Regulation"), applicable to the Data Controller in connection with the Standard Service Subscription Agreement (hereinafter "the Subscription Agreement").

This agreement shall ensure that personal data that are processed in terms of the Subscription Agreement (https://itslearning.com/global/terms-and-conditions) are not used unlawfully or come in the possession of any unauthorised third party.

Notices pursuant to this agreement shall be given to the contact person that is specified in the order from.

Any questions or requests that the Data Controller has regarding the services provided under this agreement may be directed to the Data Processor's DPO, contact-dpo@itslearning.com.

2. Definitions

GDPR means 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.

The other data protection terms and concepts used in this agreement shall have the same content and meaning as those found in GDPR.

3. Processing and primary responsibility

The agreement regulates the Data Processor's processing of personal data on behalf of the Data Controller, including the collection, recording, alignment, storage and disclosure or a combination thereof. Subject matter and details of personal data being processed are detailed in Appendix 1.

The Data Processor itself has no right of disposal over the personal data and cannot process personal data for its own purposes. The personal data shall be solely used to fulfil the purposes of the Subscription Agreement within the limits that the Data Controller has laid down.

If the Data Processor is obliged by law to process personal data in any other manner than as instructed by the Data Controller, the Data Processor must notify the Data Controller before such processing commences, unless applicable legislation or legal process prevents it from providing such notice.

4. The Data Controller's role and responsibilities

The Data Controller is responsible for ensuring that there is a lawful basis for the processing of the personal data, and that the actual processing is in accordance with Applicable Data Protection Legislation.

As part of this responsibility, the Data Controller is responsible for ensuring that system administrator(s) holds the necessary authorisation, prior to processing of personal data on behalf of the Data Controller.

The Data Controller shall also carry out any necessary privacy and data protection impact assessments, i.e. an assessment of the impact of the envisaged processing operations on the protection of personal data, prior to the processing.

The Data Controller is responsible for requests from end users for access to personal data held by the Data Controller or the Data Processor pursuant to the agreement. If such requests is received by the Data Processor, the Data Processor will advise the end user to submit its request to the Data Controller, who is responsible for responding to any such request.

The Subscription Agreement allows for the Data Controller to install and enable additional products from external third parties (including extensions). The Data Controller acknowledges that if it installs, uses, or enables such third party products, which gain access to Personal Data, this data processor agreement does not apply to the processing of data transmitted to or from such external third party products. The Data Controller can enable or disable use of external

third party products, and it is not required to use such products pursuant to the Subscription Agreement.

5. The Data Processor's role and obligations

The Data Processor shall process personal data solely on behalf of the Data Controller and only as instructed by the Data Controller. Incidental processing of personal data by the Data Processor to ensure the security, operational maintenance, analysis or evaluation of the services provided under the Subscription Agreement and not having any adverse impact on the level of data protection of the data subjects, shall not be presumed to constitute processing for the Data Processor's own purposes.

The Data Processor undertakes to give the Data Controller access to all information which is necessary to document compliance with Applicable Data Protection Legislation, and to provide assistance so that the Data Controller can fulfil its responsibilities pursuant to the law and the regulations.

Unless otherwise agreed or pursuant to statutory requirements, the Data Controller has a right of access to personal data that are processed by the Data Processor on behalf of the Data Controller and to all systems that are used for this purpose. The Data Processor undertakes to give assistance in this respect. However, the Data Processor shall not be obliged to disclose any business confidential or commercially sensitive information to the Data Controller. Furthermore, the Data Controller has no right of access where this implies a risk to the security or integrity of the relevant personal data.

The Data Processor, including employees, has a duty of confidentiality regarding documentation and personal data that the Data Processor has access to pursuant to this agreement. This provision also applies after the termination of this agreement. All necessary confidentiality agreements shall be entered into if the employees are not already bound by a statutory duty of confidentiality or secrecy. The duty of confidentiality also includes employees of Sub-Processors who carry out maintenance (or similar tasks) of systems that the Data Processor uses to provide or administer the service.

The Data Processors internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. The Data Processor designs its systems to only allow authorized persons to access data they are authorized to access; and ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. The logs shall be kept by the Data Processor for a minimum of 3 months. The Data Controller shall, upon so requesting, be given access to such logs.

6. Data protection officer

The Data Processor has appointed a data protection officer, in accordance with the requirements of the Applicable Data Protection Legislation.

7. Use of sub-processors and export of data

The Data Processor's use of sub-processors to process personal data shall be agreed in writing with the Data Controller before the processing by the sub-processor commences unless the use of sub-processor already results from the Subscription Agreement. The Data Processor will ensure that any sub-processors only access and use personal data in accordance with the terms of this data processor agreement and that such sub-processors are bound by written agreements that require them to provide at least the level of data protection required by Applicable Data Protection Legislation. The Data Controller may, on reasonable and justifiable grounds, refuse to approve new sub-processors.

The sub-processor's listed on the following website, are hereby approved by the Data Controller: https://itslearning.com/global/gdpr/subprocessors. Should the Data Controller require more detailed information related to processing locations in order to comply with legal requirements or requests from data protection authorities, the Data Processor shall assist the Data Controller to address such compliance needs, provided that, prior to any such provision of information, the Data Controller has entered into appropriate confidentiality obligations where this is deemed necessary by the Data Processor.

Changes concerning an addition or a replacement of an entity listed in the aforementioned list shall be made available to the Data Controller, including by announcing them to the Data Controller through automated notices or other means where appropriate. Within 4 weeks of receiving such notice, the Data Controller may object to any such change or addition solely on reasonable grounds.

The Data Processor is responsible towards the Data Controller for the sub-processor's actions and omissions in the same manner as if these were the Data Processor's own acts or omissions. The Data Processor is responsible for ensuring that the sub-processor is familiar with the Data Processor's contractual and statutory duties, and that the sub-processor performs them in a similar manner vis-à-vis the Data Processor.

The Data Processor, and any potential sub-processor, cannot transfer Personal Data outside the EU/EEA-area or pre-approved third countries without the prior written consent of the Data Controller. Data Controller's access to or use of Personal Data from or in a Third Country shall not, on the account of the Data Processor or any sub-processor, be considered Transfer of Personal Data to such Third Country.

To the extent such transfer of personal data is taking place, either to Data Processor entities or other third party sub-processors located in countries outside the EU/EEA- area, such transfers shall be subject to binding and appropriate transfer mechanisms which provide an adequate level of protection in compliance with Applicable Data Protection Legislation.

8. Security

a. Security measures and documentation

The Data Processor shall fulfil the requirements for security measures stipulated in Applicable Data Protection Legislation. The Data Processor has a duty to document its security measures. Appendix 3 contains an overview of the Data Processors security measures. More detailed documentation can be made available to the Data Controller upon its request.

The Data Processor shall implement and maintain appropriate technical and organisational security measures to ensure a level of security appropriate to the risk involved, including by considering the nature of any cloud service provided to the Data Controller. The measures must protect the personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. The Data Processor shall, in establishing such measures, take into account the confidentiality, integrity, availability and resilience of the information and the processing systems and services.

When processing personal data, appropriate security measures shall include inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

The Data Controller and Data Processor shall take steps to ensure that any person acting under the authority of the Data Controller and Data Processor who has access to personal data does not process them except on instructions from the Data Controller, unless he or she is required to do so by Applicable Data Protection Legislation or other legislation.

b. Overview of processing activities

The Data Processor, and, where applicable, the Data Processor's representative shall set up and maintain a list of all categories of processing activities carried out on behalf of the Data Controller, containing:

a) the name and contact details of the Data Processor and the data protection officer;
b) the categories of processing carried out on behalf of the Data Controller;
c) where applicable, transfers of personal data to a country outside EU/EEA, including the identification of that third country and the documentation of suitable safeguards as when required;
d) where possible, a general description of the technical and organisational security measures applied

The list shall be updated in accordance with clause 9 below. The Data Processor shall make the list available to the relevant data protection authority on request.

c. Notification regarding data breach

In case of a data breach that has compromised the security or privacy of the personal data, this shall be reported to the contact point specified in section 1 in this agreement. Such notification should be issued without undue delay, but in no event later than 72 hours after the Data Processor becoming aware of the data breach.

The notification shall contain:

- A description of the personal data and, when possible, which types and the number of data subjects that are affected as well as which types and quantity of personal data are affected
- The name and contact details of any data protection officer or other contact person
- A description of the likely consequences of the incident
- A description of the measures which are taken or proposed to be taken to address the incident and, where appropriate, the measures to mitigate its possible adverse effects.

The Data Controller is responsible for formally notifying a relevant personal data breach to data protection authorities and, where applicable, to those effected by the data breach.

d. Access management and equipment

The Data Processor must ensure that it has proper security of the service, including servers, databases and other relevant equipment or software, such that no unauthorised person can get access to personal data. The same applies with regard to any print-outs and other physical documents.

The Data Processor shall furthermore have a system for security control in accordance with Applicable Data Protection Legislation. The system shall include – but is not limited to routines for:

- Treatment of non-conformities which includes the provision of notification upon wrong use of the information system, including breach of security
- Security audits

The Data Processor shall establish and maintain those security measures that security and technology risk assessments have revealed a need for.

9. Updates of processing activities and security audits

The list of processing activities, cf. clause 8b) above, shall be subject to verification and updated at least once a year or after substantial changes to the processing activities.

The Data Processor shall regularly, at least once a year or after substantial changes or discrepancies, carry out security audits of systems and anything else which is relevant for the processing of personal data pursuant to this agreement. The security audit shall verify that the technical, physical and organisational security measures which have been established, are complied with and function as planned, as well as identify potential improvements.

The result of the security audit shall be documented and be made available to the Data Controller, inter alia for use in the Data Controller's security audit.

The Data Processor's systems and processes will be regularly audited and certified, and any applicable certifications will be made available to the Data Controller upon request.

Expenses that accrue as a consequence of special audits requested or performed by the Data Controller shall be covered by the Data Controller.

10. Duration of the Agreement

The agreement is valid from 25 May 2018 or from the date when the parties otherwise agreed to these Terms, if such date is after 25 May 2018, and will be in effect as long as the Subscription Agreement is in force, and supersedes any previous Data Processor Agreements of the parties.

Upon breach of this agreement or Applicable Data Protection Legislation, the Data Controller can instruct the Data Processor to stop further processing of Personal Data.

11. Return and deletion upon termination of the agreement

Upon termination of this agreement, the Data Processor shall return, overwrite, delete, cf. routines on deletion included in Appendix 2, and/or properly destroy all documents, storage media and anything else which contains personal data falling within the scope of this agreement. This applies also in respect of any back-up copies. The Data Processor shall document in writing that such action have taken place in accordance with this agreement within a reasonable time after the termination of this agreement.

The Data Controller shall bear all costs in connection with the fulfilment of this clause, unless otherwise specified in the Subscription Agreement.

12. Choice of law and legal venue

Choice of Law and Legal venue is regulated in the Subscription Agreement, or as otherwise agreed between the parties to this agreement.

***

Agreed for and on behalf of **itslearning** (**DATA PROCESSOR**)	Agreed for and on behalf of **Customer** (**DATA CONTROLLER**)
Name of itslearning entity: Itslearning Europe	Name of Customer entity:
Signed: DocuSigned by: 0598113076E1485...	Signed:
Name: Charlotte Møller-Andersen	Name:
Title: VP Europe	Title:
Date: 28-03-2018	Date:

APPENDIX 1

Subject matter and details of personal data being processed
Native and purpose of processing

itslearning as Data Processor is processing personal data received via the Service (i.e. the itslearning software, SkoleIntra or Fronter platforms), on the hosted service for Customer and applications from partners and on the website (http://www.itslearning.com), on behalf of the Data Controller for the following purposes:

- Providing the Services in accordance with the Data Processor Agreement and the Subscription Agreement
- Providing basic and technical support related to the Services in accordance with the Data Processor Agreement and the Service Subscription Agreement
- Secure backup of the Data Controller's data
- Data Processor may collect information on the Data Controller's use of the Service for internal statistical and invoicing purposes

Duration of the Processing

The term in the Subscription Agreement plus the period from the expiry of the term until deletion of all Customer Data by Data Processor in accordance with the term.

Categories of personal data

Data Processor process Personal data that is submitted, stored, imported, sent or received via the Service, by (or at the direction of) the Data Controller and by its Authorised Users. The extent of the data is determined and controlled by these subjects sole discretion. The data include the following categories:

- Contact information (name, email, phone, address, username etc.),
- Contact details of parents or guardians
- Communication (messages between users, discussions, comments to posts, notifications, etc.)
- Course material
- Assessments, assessment results and grades
- Calendar entries and event data
- Documents, presentations, images, homework, tasks, etc.

Data subjects

The Data Processor's processing of personal data via the Service on behalf of Data Controller, may include, but is not limited to personal data relating to the following categories of data subjects:

- the Customer’s employees including teachers, administrators, lecturers, mentors and others
- the Customer's other employees and contractors, and any other Authorised User by the customer who transmits personal data via the Service, including student and parents.

APPENDIX 2 | ROUTINES OF DELETION

Deletion of data upon termination of the agreement

Within 6 months from the termination of the agreement between the Data Controller and Data Processor, all data processed on behalf of the Data Controller will be permanently deleted, including backups.

Decommissioned storage media and erase policy

Storage media/Disks (including HDDs, SSDs, memory sticks and tapes) containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned. Every decommissioned storage media is subject to a series of data destruction processes before leaving Data Processor's premises either for reuse or destruction, according to our "Company policy – Disposal of Storage Media", to ensure that all data is completely and securely wiped off and destructed. The erase results are logged by the decommissioned storage media's serial number for tracking.

APPENDIX 3 | SECURITY MEASURES

itslearning has implemented the security measures set out in this appendix, both organizational and technical measures, in accordance with industry standards. itslearning may update or modify such security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the services. The updated version can be found at https://itslearning.com/global/gdpr/secritymeasures.

Organizational measures

The itslearning management team has been actively involved in developing an information security culture within the company via an ongoing awareness program, and has a management structure in place to manage the implementation of information security in its services with clear roles and responsibilities within the organization.

Operations Management

Multiple industry best-practice processes and policies exist to ensure the best possible confidentiality, availability and integrity of the platform. These policies are built around strict requirements in a number of areas, such as;

- Information security
- Hosting environment security
- Third party access
- Capacity control
- Change management
- Backup and recovery
- Access control
- Documentation
- Logging and monitoring
- Incident response
- Release management

Security team

itslearning have a team of security experts who are responsible for the overall information security of the organization. Their role include responsibility for;

- Coordinating security related tasks
- Securing corporate environment, network and devices
- Security the application (in-house penetration testing and application audits)
- Monitoring and logging
- Process and policy management (disaster recovery, path management etc)
- Training and education of employees, in the field of information security
- Coordinating third-party security audits, and follow up on any findings,
- Reviewing code for potential security vulnerabilities.

Roles and responsibilities

All employees have clear roles within the company, and are only given access to data required for their specific role. A limited number of employees have administrative access to our production environment and their rights are strongly regulated and reviewed at set intervals. Any major change to the application, environment or hardware of the production environment is always verified by a minimum of two individuals.

Personnel security

All itslearning personnel are required to enter into a strict confidentiality agreement. All staff are required to follow corporate policies regarding confidentiality, business ethics and professional standards. Staff involved in securing, handling and processing customer data are required to complete training appropriate for their role.

Access Control

Strict requirements are in place for any employee, hired consultants or third party requesting access to itslearning information systems. Access control is controlled by an authentication system. The user is required to:

- Have management approval for the requested access
- Have strong passwords that are in accordance with the corporate password policy
- Change their password at regular intervals
- Document that the access requested is required for their specific role/task
- Ensure that the device (PC, tablet, cellphone) used is adequately secured, and locked when the user is absent.

itslearning employs automatic temporary lock-out of user terminal if left idle.

Internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Any changes to data is logged to create an audit trail for accountability.

Physical security

a. Data Centers

itslearning operates all its customer services from data centers separated from the corporate office work space. Access to data centers are strictly controlled and protected to reduce the likelihood of unauthorized access, fire, flooding or other damage to the physical environment. Physical access to data centers are limited to a small number of employees within itslearning and/or its hosting center providers. Strict security clearances are required and must be approved by security management prior to entering a data center.

b. Office work space

All of the office work space of itslearning is protected by access control. Only invited visitors and employees can access itslearning's work space. Multiple measures are in place to avoid security issues due to theft or loss of computer equipment. This includes security guidelines and acceptable use policies, authentication systems and encryption of storage units when applicable.

Technical measures

System availability

itslearning has implemented industry standard measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy (including full network, power, cooling, database, server and storage redundancy)
- backup is stored at an alternative site and available for restore in case of failure of the primary system.
- Appropriate denial-of-service protection
- 365/24/7 personnel on duty to monitor and troubleshoot

Data protection

itslearning has implemented a series of industry standard measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during transport or at rest. This is accomplished by various industry standard measures including:

- Use of layered firewalls, VPNs and encryption technologies to protect gateways and pipelines
- HTTPS encryption (also referred to as SSL or TLS connection) with secure cryptographic keys
- Remote access to data centers are protected with a number of layers of network security
- Particular sensitive customer data at rest is protected by encryption and/or hashing (pseudonymisation)
- Every decommissioned disks are subject to a disk erasure process according to our "Disk erase policy", and decommissioning is logged by disk serial number
- Regular third-party security audits (minimum annually), including penetration testing, that are made available to customers

Data centers

itslearning uses only state-of the art data centers, with 365/24/7 on-site security and monitoring operations. The data centers are housed in modern fire-resistant facilities that require electronic card key access, with alarms that are linked to the on-site security operation. Only authorized employees and contractors are permitted to request electronic card key access to these facilities.

System development

itslearning's platform is based on industry standard technologies from well-known vendors, including Microsoft, Linux, Dell, Fujitsu, Amazon, Cloudflare, F5 and Cisco. Systems are periodically patched to

latest version to ensure that the latest security enhancements are applied. The platform is in general updated several times per quarter, and bug-fixes are released swiftly based on priority, following rigorous quality checks.

itslearning has measures in place to minimize the risk of introducing code in its platform that can degrade the security or integrity of the customer services and personal data processed. Measures include:

- Regular training of staff
- Code review by security architects
- QA process for rigorous testing of changes prior to deployment

Sub-processor security

When onboarding sub-processors, itslearning performs an audit of the security and privacy practices of sub-processors to ensure sub-processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. itslearning performs regular security audits of the practices and delivery for existing sub-processors.