GDPR – customer documentation - product

Introduction

A summary of what data we process, your rights as a customer and how data protection is built into our development processes

Fronter – an itslearning LMS

Fronter is now an LMS provided as a software-as-a-service by the itslearning company. The Fronter GDPR customer documentation is therefore based on the same documentation as itslearning LMS, with adaptions in some areas where Itslearning and Fronter are different, for example due to different technical solutions. We have used the Itslearning brand where the information relates to itslearning as a company, but we use the Fronter name when information relates directly to the LMS.

Terms used in this document:

In general, the terms and concepts used in this document have the same content and meaning as those found in GDPR.

- *GDPR* – General Data Protection Regulation, EU legislation regulating use of Personal Data
- *Data controller* – the itslearning customer, meaning typically a school, university, district or municipality.
- *Data processor* – itslearning, including the Fronter LMS
- *Data subject* – a natural person, in this context an itslearning user
- *Data Processor Agreement (DPA)* – contains further details on role and responsibilities of the Data Controller and Data Processor

itslearning as a Data Processor

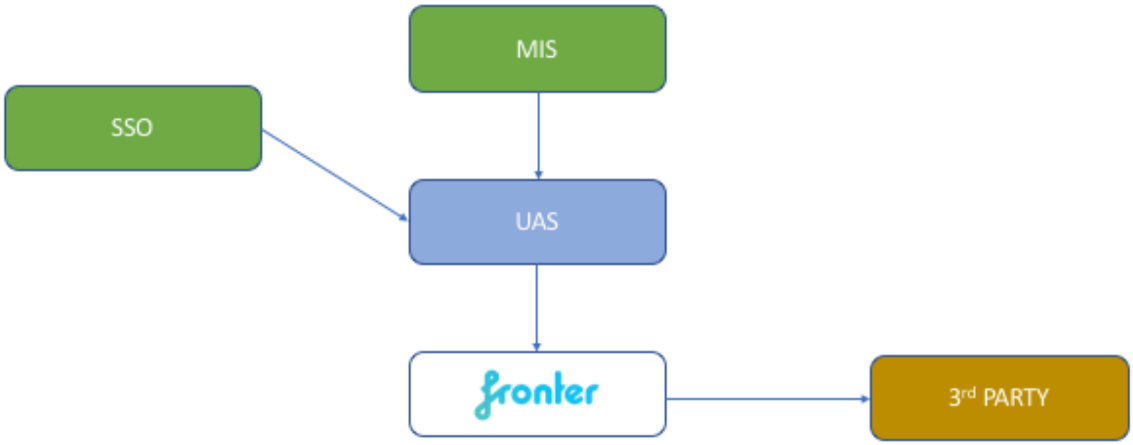
For the cloud services we provide to our customers and their end users, itslearning is what both existing and new EU regulation defines as a Data Processor. As a Data Processor we do not decide the purpose or lawfulness of the processing, we merely process data on our customers' behalf. The GDPR regulations force stricter requirements upon all processors of data. We will fully comply with these requirements for all of our services, including itslearning.

Itslearning does not independently obtain user data to our services. User data can either be submitted to the platform by customers' representatives, through an integration with a third-party system, or in some cases by the users themselves. Most commonly, personal data in itslearning comes from student information systems under the control of our customers. We only import data from third-party systems on the instruction from our customers.

Further details on role and responsibilities of the Data Controller and Data Processor can be found in the DPA (Data Processor Agreement). This, and more information about itslearning and GDPR can be found on our website (https://itslearning.com/global/gdpr).

From a high level, Data can be entered into the Fronter LMS in 2 main ways:

1. Imported through a MIS - Management Information System. The MIS is a 3rd party system provided by the schools/school owners. The schools/school owners (municipalities) are responsible for the data provided to Fronter by the MIS. These data will be handled inside the UAS – User Administration Tool – that also handles SSO (Single Sign On) solutions.



2. Data can be entered directly into Fronter. Normally, Data Subjects are imported from the SIMS. But personal data can be updated inside Fronter as well, by system administrators and in some cases by the users/data subjects themselves.

Details of personal data being processed

Which data is collected and how it is processed in Fronter, depends on how our customers use our system. This document contains a general description. The DPA can be updated to contain a specific description for each customer.

Data subjects

In Fronter, the Data Subject does not have roles in the system, but have **rights** that give the subject

a) access to certain parts of the system (buildings, corridors, rooms etc.)
b) ability to perform certain actions (based on Read, Write, Delete)

Even if there is a "flat" structure in Fronter, the data subjects normally fall into one of three groups:

1. Staff (Administrator, Tutor, Teacher…)
2. Students
3. Parents

Collection and processing of data

itslearning as Data Processor is processing personal data received via the Fronter platform, on the hosted service for the customer and applications from partners. Processing is done on behalf of the Data Controller for the following purposes:

- Providing the Services in accordance with existing agreements
- Providing basic and technical support related to the Services in accordance with the Data Processor Agreement and the Service Subscription Agreement
- Ensuring security, do maintenance, analyse or evaluate how well the service works

The duration of processing is 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

The information that may be submitted to itslearning (depending on how a customer has chosen to configure and implement the service) about a Data Subject falls into several categories, these are given below with examples of each:

Category	Examples
Personal information (contact information)	- User name - Email - Phone number - Contact details of parents or guardians - IP-addresses - Activity logs
Communication	- Messages (IM / Old messages) - Discussion (could also be seen as student response) - Bulletins + comments
Course material (produced by user in context of teaching)	- Assignment - Test - Note - Uploaded document
Assessments (given by teacher to student)	- Assessments (grades, descriptive feedback) - Attendance comments - Behaviour comments
Calendar entries	- Events
Student responses	- Answer to assignment (including uploaded files) - Test attempt - Crossword answer
Internal logic	- Last used selection in dropdowns some places - Personal settings: language, simplified tree structure, accessibility ++ - Cookies

How to satisfy the right of the data subject

Roles and responsibilities

Under GDPR, the Data Subject rights are between him and the Data Controller. Any Data Subject requests from end users to itslearning will be handed over to the customer. itslearning will cooperate in good faith with customers to ensure they can exercise the rights of the Data Subjects in a prompt manner. The rights of the Data Subject are described in Chapter 3 of GDPR (https://gdpr-info.eu/chapter-3/).

All requests should go from the Data Subject to the Data Controller, who in turn may or may not use our functionality or ask itslearning for help to exercise the right for the Fronter platform. **Each individual**

request needs consideration and processing before action is taken. The rights of the Data Subject are not absolute and should be processed in the context of both GDPR and local regulations.

Please note that according to GDPR there are exceptions to exercising the rights of the data subject when the data is considered necessary…

* … to exercise right of freedom of expression and information of other data subjects

* … to comply with legal obligations or the performance of a task carried out in public interest

* … for archiving, historical or statistical purposes

Under GDPR, the data subject rights are between him and the Data Controller. Any data subject requests from end users to itslearning will be handed over to the customer. itslearning will cooperate in good faith with customers to ensure they can exercise the rights of the data subjects in a prompt manner.

In addition to administrative and other functionality already available in the Fronter system, the itslearning Data Protection Officer (DPO) and our service team are available to help our customers as Data Controllers, satisfy the right of the Data Subject.

Below is a description of how some of the rights can be exercised with the help of itslearning.

Performing actions to satisfy the rights of the data subject

To help our Fronter customers satisfy the rights of the Data Subject, we have created a script that will either

- Delete the data subject and all its personal data permanently
- Export (access) the data (the right of access)

Deleting data from Fronter according to GDPR regulations

This script to delete data will be run by itslearning staff upon request from the Data Controller's system administrator, to its learning support. **It is important for the Data Controller to be aware that to be able to delete data from Fronter in accordance with the GDPR regulations – they will have to contact itslearning.** The data will then be permanently removed from the system, and this action cannot be reverted.

If your intention is to "clean" the system to hide irrelevant data, you can use the existing delete functionality inside the Fronter platform. The data controller should also note that when the business agreement between itslearning (Data Processor) and its customer (Data Controller) is terminated – all data will be permanently deleted, according to the GDPR regulations.

Details about what data that will be deleted can be provided upon request from system administrator to itslearning support staff.

The right of access

The Data Subject has the right to obtain information from the Data Controller about what personal data are processed, how and why. This is described in the DPA, and categories of data can also be found on page 2 of this document for easy reference.

More details about this right can be found in Article 15 of GDPR (https://gdpr-info.eu/art-15-gdpr/).

To access the specific information stored in Fronter related to a Data Subject, the system administrator can contact itslearning support staff.

Details about what data that will be exported can be provided upon request from system administrator to itslearning support staff.

More details about this right can be found in Article 20 of GDPR (https://gdpr-info.eu/art-20-gdpr/).

The right to data portability

In some cases, the Data Subject can have a right to get data exported from Fronter.

To export the specific information stored in Fronter related to a Data Subject, the system administrator can contact itslearning support staff. The file format will be machine readable, and the file will be sent from itslearning to the system administrator in a secure manner.

Details about what data that will be exported can be provided upon request from system administrator to itslearning support staff.

More details about this right can be found in Article 20 of GDPR (https://gdpr-info.eu/art-20-gdpr/).

The right to rectification

Should there be inaccurate, incomplete or erroneous personal data concerning a Data Subject, the Data Subject has the right to have the Data Controller rectify it.

More details about this right can be found in Article 16 of GDPR (https://gdpr-info.eu/art-16-gdpr/).

In many cases the user can correct information himself in the Fronter interface. In other cases, and most commonly, information about a person like name, email address and so on should be edited in the external student information system (MIS) and synchronised with Fronter. Other types of data can be corrected by teachers, tutors or administrators in the Fronter system.

The right to restriction of processing

Restriction will be performed as a “soft delete” when the administrator deletes a user/Data Subject from the system options in Fronter. The Data Subject will be moved to a trash can in Fronter. All information about a user will be removed, but not irreversibly erased. According to GDPR there are exceptions when the data is considered necessary…

- … to exercise right of freedom of expression and information of other data subjects
- … to comply with legal obligations or the performance of a task carried out in public interest

- … for archiving, historical or statistical purposes

More details about this right can be found in Article 18 of GDPR (https://gdpr-info.eu/art-18-gdpr/).

This might in some cases mean that the user name is anonymised/obfuscated, while content is kept available (pseudonymisation). The table below outlines how this is handled in the different categories of personal data:

Category	Effect of RESTRICT
Personal information (contact information)	Removed
Communication	Anonymised
Course material (produced by user in context of teaching)	Anonymised, unless the material exists so that it is only available to the data subject in question
Assessments (given by teacher to student)	NOT removed – as this infringes on the rights of the student
Calendar entries	Removed if personal, anonymised if shared
Student responses	Removed
Internal logic	Not visible in UI

Restriction is reversible and can be performed by restoring the data subject (user) from the trash can. When restriction of processing is lifted, the Data Controller is obligated to inform the data subject.

The right to erasure ("right to be forgotten")

In almost all cases, deleting a Data Subject and related data, will be done because the purpose for processing his data is no longer valid. Most commonly because a student left school, or a teacher changed jobs, or because the customer has terminated the contract with itslearning. The Data Controller needs to have their own procedures for how long they store data about the Data Subject after the need of processing data is no longer valid. (they leave the school etc.). And they need to contact itslearning support staff when they want data on a specific Data subject to be deleted from Fronter. As mentioned, when the contractual agreement between the Data Controller and the Data Processor (itslearning), is no longer valid – all data will be permanently deleted, according to the GDPR regulations.

More details about this right can be found in Article 17 of GDPR (https://gdpr-info.eu/art-17-gdpr/).

Deleting information related to a specific Data Subject request based on his right to erasure as defined in GDPR, can be done by contacting the itslearning support staff. Itslearning will run the delete script and this will completely erase any information related to the data subject from the Fronter platform, with the same exceptions as mentioned in the section about right to restriction of processing.

As an example, this will include assessments given by a teacher to a student. If the teacher is deleted, these data will still remain in the system to retain the rights of the student.

Please note that this action is not reversible.

Category	Effect of DELETE
Personal information (contact information)	Permanently deleted
Communication	Permanently deleted when all affected users are deleted. For example, a group conversation in the message system is deleted when all participants of that conversation are deleted. Bulletins and discussions are deleted when the course they belong to is deleted.
Course material (produced by user in context of teaching)	Anonymised, unless the material exists so that it is only available to the data subject in question (in which case it is permanently deleted)
Assessments (given by teacher to student)	NOT removed if the teacher is deleted, as the assessments are still of value affecting the rights of the student.
Calendar entries	Permanently deleted if personal, anonymised if shared
Student responses	Permanently deleted
Internal logic	Permanently deleted

Data Protection – in every step of our product development process

itslearning's product development process embraces a number of industry-leading frameworks, including a close adherence to developing software that includes data protection by design and by default. This includes the adoption of a set of standardized principles, and the use of a checklist to ensure at each stage of our development process data protection is considered and included as necessary.

Basic requirements for any software handling personal data

- Lawful, fairly and transparent: All personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject
- Ensure purpose limitation: The software must only collect personal data for specified, explicit and legitimate purposes.
- Ensure data minimisation: The software must only process personal data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Ensure accuracy: The software must ensure that all personal data is accurate and up-to-date. Incorrect data must be deleted or rectified.
- Ensure storage limitation: The software must ensure that it is not possible to identify the data subject for longer than is strictly necessary for the purposes for which the personal data are processed.
- Ensure integrity and confidentiality: The software must ensure appropriate security of the personal data.

Key concerns for establishing Data Protection and Information Security

As itslearning works on developing software, there are a number of steps and questions related to data protection and information security that we consider. These reflections include considering:

- Define the processing to be done, and establish an overview of the personal data: Will personal data be processed by the software?
- If the software is working as intended without identifiable data, no identifying data must be collected.
- Data protection can be designed in using pseudonymisation techniques in the software.
- The software must only use personal data as planned.
- Personal data must be available to those authorised to use it when necessary.
- The software must be developed with default settings that protect the rights of data subjects and safeguards privacy.
- When personal data is collected from persons other than the data subject, information must be provided concerning which categories, e.g. information about assessments, of personal data are being processed
- To ensure security of processing of personal data, it is necessary to:
    - ensure confidentiality. Personal data must be secured against unauthorised disclosure or access.
    - ensure integrity. Personal data must be secured against accidental and unlawful destruction, loss, or alteration.

- ensure accessibility. Personal data must be available to authorised personnel who require it for their work.
- ensure resilience. Resilience means that software that is processing personal data must be able to resist e.g. vulnerabilities, attacks, and accidents.

Use of Sub Processors

When using (sub) processors, we ensure that we have a Data Protection Agreement with the processor. We also require that:

- The controller must only use processors who provide adequate guarantees that they will implement measures ensuring compliance with the data protection regulation and ensure the protection of the rights of the data subject.
- The controller must ensure that any suppliers and subcontractors fulfil all requirements by entering into processing contracts.

Principles for Data Protection and Privacy by Design and Default

The 7 principles below are created by the Information & Privacy Commissioner of Ontario. We have embedded them in our software development process, from the way we work through the ideation phase, through to how software developers work with the requirements, up to the release of new software to the itslearning platform.

1. Proactive, not Reactive

2. Privacy as the default setting

3. Privacy embedded into design

4. Full functionality

5. End-to-end Security

6. Visibility and Transparency

7. Respect for User Privacy

Data protection by Design and by Default for new products/features in itslearning

We have a checklist to help teams understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. The checklist is inspired by a similar checklist developed by The Norwegian Data Protection Authority.

The core elements of the checklist describe what considerations are taken by the people involved in each step of our product development process:

Innovate

The product owners are responsible for designing, writing requirements and specifications for a new or changed feature so that:

- The purpose and lawfulness for processing personal data is defined
- Security and privacy is ensured through Design and by Default
- Our data-protection principles are followed
- New / existing sub-processors are identified, and there is a valid DPA.

Build

The software architects, developers and test engineers are responsible for designing, coding and testing new and changed features so that:

- All processing of personal data is aligned with the defined purpose and lawfulness
- The feature meets data-protection principles
- Fulfils the data-protection principles
- They write secure code by implementing the requirements for data protection and security according to official itslearning coding standards

Deliver

The integration consultants are responsible for ensuring that:

- Any processing through integrations meets the purpose and lawfulness of the feature
- The integration design fulfils the data-protection principles
- Fulfils the data-protection principles
- Write secure code by implementing the requirements for data protection and security

Support/maintenance

The operation engineers are responsible for considering the following for new services:

- The processing in the new service is aligned with the defined purpose and lawfulness
- The design of the new service fulfils the data-protection principles
- Fulfills the data-protection principles
- Follow the company policy regarding Incident Management

Passing data to 3rd party providers

The Fronter LMS is flexible, and can be extended with tools, content and additional services. This can be done by our customers, our end users and third parties acting on behalf of both itslearning and our customers. The purpose of such extensions is always to offer more tools, capabilities and options for our users. Examples of such extensions can be:

- Assessment tools, for example assignment tools or digital test tools tailored for specific curriculum or teaching methods
- Teaching and learning activities, such as interactive study materials
- Open Educational Resources (OER) and licensed content provided by publishers
- Third party applications for mobile devices

In some cases, these extensions will require some personal data to be transferred from itslearning in order to provide value to our users, for example:

- Show the name of the user as part the application
- Give a teacher a list of students and their group affiliation when assessing an activity
- Suggesting additional tools or materials based on achievements

For itslearning, it is of the highest importance that our customers and end users feel secure that their data is protected, and only used according to the specified requests and needs of our customers. As such, itslearning takes strong measurements in order to protect all personal data, and only expose this data to the extent that our customers need.