



GDPR & IMS



Steven Threadgold

Head of Product Management

Why GDPR?

- 1. Lawfulness, fairness and transparency*
- 2. Purpose limitation & Data minimization*
- 3. Accuracy*
- 4. Storage limitation*
- 5. Integrity and confidentiality (security)*
- 6. Accountability*

GDPR Hints and Tips for Success

Some comments on our experiences 17 months on from 'GDPR day'.

1. Clear information for customers and users

The screenshot shows the top navigation bar of the itslearning website with links for COUNTRY SELECTOR, CONTACT US, LEADERSHIP, CAREERS, SUPPORT, FRONTER, COMMUNITY, REQUEST A DEMO, and LOGIN. Below this is the itslearning logo and secondary navigation for K-12, Higher Education, About, Services, and Blog. A dark blue navigation bar contains links for GDPR, Security Measures, Sub-processors, and Privacy. The main content area features a large heading "We are GDPR compliant!" followed by a sub-heading "Information to our customers about GDPR". The text explains the EU's General Data Protection Regulation (GDPR) and itslearning's commitment to data privacy. Below this, two columns provide further details: "itslearning GDPR Commitment." and "What does GDPR require from you as a customer?". The first column states that itslearning complies with GDPR requirements for its services. The second column lists requirements for customers, such as documenting data processing. A green chat icon is visible in the bottom right corner.

COUNTRY SELECTOR ↓ CONTACT US LEADERSHIP CAREERS SUPPORT FRONTER COMMUNITY REQUEST A DEMO LOGIN

itslearning K-12 Higher Education About Services Blog

GDPR Security Measures Sub-processors Privacy

We are GDPR compliant!

Information to our customers about GDPR

The EU's [General Data Protection Regulation \(GDPR\)](#), approved by the European Parliament in 2016, is the most important change within data protection regulation in 20 years. It replaces the Data Protection Directive 95/46/EC and local law and regulations across the EU/EEA. The new regulation is designed to strengthen the individual's rights to privacy and harmonize data privacy laws across Europe.

itslearning has been committed to data privacy for nearly 20 years and welcomes the new regulation. We will keep doing our part to ensure that all our customers are GDPR compliant. There is a big, untapped potential in using technology and cloud services to improve teaching practices and learning outcomes. One of the keys to unlocking this potential is to earn the trust of teachers, students, and parents. In this sense, the increased focus on data protection and privacy due to GDPR is beneficial for all parties.

itslearning GDPR Commitment.

We fully comply with the requirements for all of our services, including itslearning, Fronter and SkoleIntra to be GDPR ready. We have been working with GDPR for a long time to analyse the new regulation, and making the necessary changes to our services, procedures, and organization. During the previous months, we made available all documentation, contract addendums, and

What does GDPR require from you as a customer?

In general, GDPR requires you to:

- Document and assess all processing of personal data and the systems being used. The purpose and lawfulness of the processing should be defined and you should make sure you do not process personal data that is not needed for the defined purpose.

2. Allow customers to easily manage rights under GDPR

Self-service:

- The **right** to be informed
- The **right** of access
- The **right** to rectification
- The **right** to erasure/to be forgotten
- We also provide access to the DPO.

its Home Groups Library Admin Developer

Admin

Manage personal data (GDPR)

[Back to User and access rights](#)

Check the personal data and make sure you've selected the right person:

First name: Admin
Last name: Admin
Username: admin
Profile: Custom Administrator

I confirm that I have selected the correct user

Recent actions:

TYPE	STATUS	REQUESTED ON	EXPIRATION DATE	REASON
None				

Choose what to do:

Preview / Download
Save all the user's data to an xml file.

Edit
Change the user's basic data in [Edit user's data](#) page.

Restrict user's data
Restricted users can no longer use their itslearning accounts. All their personal data will be saved, but it will not appear to other users. To cancel a restriction, go to the Trash can and use the GDPR button to restore the user.

Delete the user's profile with all data
Deleted users are removed from itslearning with all their personal data. **This action cannot be undone.**

State the reason for your changes:

Reason: Admin, admin wants to be removed from itslearning because lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore, so help him God.

More information about GDPR: [Restrictions from EU](#)

3. Never forget the flow of data

Under GDPR you should not let your instructors control the flow of students personal data into 3rd party applications.

Fines and liability are increased under GDPR, expect more vigilance from both parents and supervising authorities.

Personal data is the new “currency” online, and we have a responsibility to protect our students from becoming a tradeable commodity.

Have oversight of over 3rd parties that receive personal data from the your solution.

Suitable control over how 3rd party tools are used in your LMS.

Pre-installed 3rd party tools must be under compliant legal agreements, either as a sub-processor or directly contracted with your institution.

4. Pro-active vendor compliance and competence

Be aware of how your vendors process data from your platform.

Actively review standard data processing agreements.

Good partners will be ready and willing to answer these questions.

Ask about what training staff the vendors staff has undergone.

Interview the data protection officer or security officer.

Check the data breach process.

Ask for historical security audits.

Ask for statistics on historical security incidents.

Interview staff.

5. Test your processes for a data breach

Do you have an realistic, actionable and appropriate communication plan if disaster strikes?

Test and retest your plan.

Can we alert our data subjects and the Data Protection Agency in time?

Are our and our vendors security/processes appropriate?

Is our processing well-documented and lawful?

Have we minimised the risk for the data subjects? Have we minimised the data being processed?

Are we making sure we don't process data from former students/employees?

6. Your data practices and processes must be embedded in daily work

Make data privacy a living process in your organisation.

Train your staff and have data security understanding part of onboarding with yearly refreshers.

Add data security by design to the development process.

Regular updates from the DPO.

Challenges we addressed in the last year:

- Ensuring consultants or part-time staff were aware of our data policies.
- Auditing how we handle non-LMS customer data. E.g. Ad hoc Emails from customers.
- Making sure local teams following the global policies.