ARTICOLO DI ELEARNINGNEWS

Year 2 - number 26 Wednesday 23 maggio 2018

eLearning and GDPR

What are the implications of GDPR on eLearning?

The "General Data Protection Regulation" of the European Union (**GDPR**) will be fully operational from 25 May 2018 in all European Union countries. The new regulation aims to increase transparency and accountability of companies that process personal data, to promote a "privacy culture" on the Internet and to protect users.

What are the main guidelines of the GDPR and what are its general and specific implications related to eLearning?

Who is it for?

Any company (based in the EU or outside the EU) offering services to EU citizens or tracking the behaviour of EU citizens (through online profiles, cookies and other similar means) is required to comply with the GDPR.

Why?

A non-compliant company may be subject to fines of up to 4% of its annual turnover.

GDPR terminology

- **Elaboration**: everything a company can do with personal data (collection, organization, conservation, adaptation, transmission, sharing ...).
- **Data controller**: companies that collect, store or manage data of people for a particular purpose (and determine the way in which the collection takes place).
- **Data manager**: a company that stores or processes user data on behalf of other companies (data processors). Data Controllers are companies that have the primary purpose of collecting data, and Data Processors are companies that offer data processing, storage, etc. The Data Processor can not use the data for purposes other than those for which the Data Controller has collected them.
- **Data subject**: a natural person - as a student or a teacher.
- **Personal data**: any information relating to a subject such as name, email ...
- **Consent**: a clear indication from an interested party that agrees with the collection and processing of their personal data.

What to do to comply with the GDPR?

If your company uses an LMS for training, GDPR compliance is a shared responsibility between your company (the "controller") and your LMS provider (the "processor").
As a controller, you must define the objectives of the processing, check the data of the learners, administrators and teachers that will be processed.

First of all, you should not collect more data than necessary for your purposes or use the data for purposes other than those for which they were collected.

Track data (sources, systems where they are stored, data streams and access rights) ensuring that privacy is always respected. Defining adequate protection and data retention policies and setting up controls can be very useful for this purpose. Also, be sure to keep updated databases and prepare means for correction.

Limit access to personal data collected by your company to employees who need to have them available to perform their business.

In the more specific case of eLearning, it is necessary to carefully examine the GDPR compliance program, the privacy policy and the conditions of use of the LMS used and sign a DPA (Data Processing Addendum) compliant with the GDPR with the LMS provider.
The DPA must clearly specify the instructions that the LMS service should follow and obliges both parties to comply with the legal obligations related to the GDPR.

What shall the LMS service provider do to comply with GDPR?

The LMS service provider must provide customers with the means to satisfy the privacy rights of the persons concerned through the LMS functionality.
The rights referred to are:

- the right to be informed (that you have their own data),
- the right of access,
- the right to rectify data,
- the right to be forgotten,
- the right to file a complaint,
- the right to limit or interrupt data processing,
- the right to obtain data in a structured format (eg download CSV),
- the right to refuse the use of data for marketing purposes.

With regard to this last point, it is important to identify the contact person responsible for data protection (or a data protection officer) who can easily be reached by the customers, e.g. through an email address published on the website.
In addition, the provider must provide sufficient information regarding its Privacy Policy, Terms of Service and DPA. This means documenting the scope, nature, types of data, the retention policy, the list of sub-processors used (e.g. for hosting Cloud or processing payments), the controller's instructions and transfers international organizations so that LMS users can make informed decisions about the use of the service.

Likewise, it is important to:

- offer users the opportunity to ask questions, submit complaints or exercise the rights established by the GDPR;
- examine all sub-processors and ensure their compliance with the GDPR;
- provide legal justifications for processing and data transfer operations. For example, a service that sends user data from the EU to the US should have at least some legally approved Binding Corporate Rules governing the transfer and management of such data;
- support access to personal data according to the roles;
- comply with the GDPR certifications and approved codes of conduct.

With regard to the code of conduct it is important:

- give clear directives on the conditions of confidentiality to the personnel who access the data;
- collaborate with data controllers and supervisors;
- in the case of data breaches, have a policy and a plan to be implemented to give notice to the supervisory authorities and interested parties within 72 hours;
- support the export of LMS data in other formats and the possibility of transferring data to another supplier;
- review, update and periodically test the effectiveness of policies, procedures and controls.
  It is the responsibility of the user, as data controller, to verify that the above is actually supported by the LMS service.

GDPR and data processing

In order for a company to **store and process personal data**, at least one of the following conditions should exist, as specified in the GDPR (Article 6):

- the data subject has given consent to the processing for specific purposes
- processing is necessary for the execution of a contract that the party has signed

- treatment is necessary for compliance with a legal obligation
- processing is necessary to protect the interests of the data subject
- processing is necessary for the performance of a task performed in the public interest
- processing is necessary for the legitimate interests pursued by the controller, except where such interests go beyond the interests or the fundamental rights and freedoms of the data subject

GDPR and eLearning

Here are two peculiarities of eLearning in reference to GDPR that you should know:

1. National limits to the processing of employee data

The GDPR allows national legislation to impose specific rules on the processing of personal data of employees in the workplace.
If your company has offices and employees throughout the EU, you should know the specific national legislation of the countries where your company is present.

2. Consensus problems

The power imbalance between employer and employee can make mere consent insufficient as a legitimate basis for processing employee personal data: adding a training path as a contractual term for your employees will serve as a stronger justification for data management for eLearning.

Read the complete article...