ELEARNING EXPERTS
8918 George Washington Memorial Hwy
Yorktown VA 23692 USA
888-928-3848
info@elearningexperts.net

GDPR - General Data Protection Regulation

May 10, 2018

Disclaimer: This is an informational document and the information contained within this document in no way constitute legal advice. Any person who intends to rely upon or use the information contained herein in any way is solely responsible for independently verifying the information and obtaining independent expert advice if required. **Independent legal counsel is strongly advised.**

What is GDPR?

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. **It applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.** It will apply to the processing of personal data by controllers and processors in the EU, **regardless of whether the processing takes place in the EU or not where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU.** This document is informed in part by EUGDPR.org . An overview of the GDPR may be found here.

Who does it affect?

GDPR carries provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU. The GDPR not only applies to organisations located within the EU, but also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What types of information does it protect?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. This includes such things as:

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

What constitutes consent?

Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Explicit consent is required only for processing sensitive personal data - in this context, nothing short of "opt in" will suffice. However, for non-sensitive data, "unambiguous" consent will suffice.

Children

Additionally, parental consent will be required to process the personal data of EU children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

When does it take effect?

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation has been scheduled to take effect after a two-year transition period and, unlike a Directive, it does not require any enabling legislation to be passed by government; meaning it will be in force **25 May 2018.**

The GDPR references controllers and processors. What is the difference?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Data Subject Rights

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices.

- May be a staff member or an external service provider.
- Contact details must be provided to the relevant DPA.
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge.
- Must report directly to the highest level of management.
- Must not carry out any other tasks that could results in a conflict of interest.

Moodle

GDPR for Organizations/Administrators

Moodle HQ has released documentation which provides important information and guidelines for maintaining GDPR compliance within your Moodle installation.

Additionally, with Moodle 3.4.2 onwards, there is a Policies plugin designed to support GDPR compliance. The Policies plugin provides a new user sign-on process, with ability to define multiple policies (site, privacy, third party), track user consents, and manage updates and versioning of the policies. The Data Privacy plugin provides the workflow for users to submit subject access requests and for the site administrator or Data Protection Officer (DPO) to process these requests.

The Policies plugin forms part of Moodle's privacy feature set and will assist sites to become GDPR compliant. It is available from the Moodle plugins directory. The plugin will be integrated in the Moodle 3.5 release in May 2018. Moodle 3.4.2 also includes the option of checking whether a new user is a minor.

The Data Privacy plugin forms part of Moodle's privacy feature set and will assist sites to become GDPR compliant. It requires Moodle 3.4.2 or later and will be integrated in the Moodle 3.5 release sometime in May 2018.

Specific Features

Moodle assists with GDPR compliance through features covering the following areas:

- Onboarding of new users, including; age and location check to identify minors, versioning of privacy policies and the tracking of user consents;
- Handling of subject access requests and erasure requests, and maintaining a data registry.

Important note: Installing the developed plugins alone will not be enough to meet the GDPR requirements. Correct configuration and implementation of the required processes and procedures is also required. One tool you may leverage is Site Policies. The Site Policy URL may be of particular interest. Note that these links are for version 3.3 - the latest documentation on Moodle.org as of this writing.

Moodle HQ highly recommends that you also engage your IT and legal departments on what is required for GDPR compliance.

Totara

At the time of this writing, Totara Learn recommends that you upgrade to Totara 11 to support GDPR compliance.

Specific Features

Totara Learn 11 features a range of data protection features and user data management tools to ensure your organisation's learning management system supports GDPR compliance. Totara Learn also offers a range of new functionality in this latest release for administrators, course managers and learners alike.

Totara policies and documents may be found here. Information about Site Policies for Totara may also be of interest.