

TOTARA GUIDE



A GUIDE TO GDPR COMPLIANCE AND YOUR LMS

86% of organisations worldwide are concerned that a failure to adhere to GDPR could have a major negative impact on their business.¹

From the 25th May 2018, all companies operating in the EU will need to ensure that they are compliant with the new General Data Protection Regulation, or GDPR, a set of rules put in place to protect users' personal data. Wherever you are based in the world, it is still important to know about GDPR, as this affects companies who conduct any business in the EU, not just those based in the region.

The new regulation will affect the websites and platforms we use every day, social media, online shopping sites, forums and newsletters, as well as our learning platforms. With 79% of organisations using a learning management system (LMS)², it's vital that companies act sooner rather than later to ensure they are able to operate in compliance with GDPR.

The penalties imposed for failing to comply with GDPR can be up to €20 million or 4% of annual worldwide turnover, whichever is greater³. It is crucial, then, that your LMS allows you to manage this significant business risk.

GDPR can seem complicated at first, so we have broken it down into the type of scenario that real organisations might encounter to put the new data protection rights into context. This is a must-read for anyone working in HR or L&D for an organisation affected by GDPR, and will show why it's so important to select an LMS that supports GDPR compliance.



ALMOST A THIRD OF ORGANISATIONS GLOBALLY SAY THAT THE COMPLEXITY OF THE NEW LAWS IS THE BIGGEST BARRIER TO GDPR COMPLIANCE.⁴



WHAT ARE THE RISKS IF MY ORGANISATION FAILS TO COMPLY WITH GDPR?

The significant financial penalties should be a big enough motivator for most organisations operating in the EU. With massive fines for businesses found in breach of GDPR, this has the potential to put many companies out of business, making it absolutely essential that you comply with the new data protection rules.

Cyber attacks can cost businesses over \$2.35 million per incident,⁵ and with the number and severity of data breaches increasing all the time, this is only going to become a bigger risk for organisations worldwide. Equally significant is the reputational damage that businesses will suffer following a data breach, as users choose to withdraw their custom from organisations that put their personal data at risk. This can be catastrophic for a company, and it can take years to recover their reputation if they can manage this at all.

12% of businesses are very concerned about reputational damage after GDPR takes place.¹

¹ <https://www.veritas.com/en/uk/news-releases/2017-04-25-veritas-study-organizations-worldwide-fear-non-compliance-with-new-european-union-data-regulation-could-put-them-out-of-business>

² Towards Maturity Benchmark Report Jan 2018

³ <https://www.eugdpr.org/key-changes.html>

⁴ <https://www.helpnetsecurity.com/2017/11/09/top-gdpr-compliance-risks/>

⁵ <https://cybernewsgroup.co.uk/cases/the-risks-of-not-being-gdpr-compliant/>



HOW WILL GDPR AFFECT MY LMS?

Here are some common scenarios that you will encounter once GDPR is in force.

1. THE RIGHT OF ACCESS

Alex has been taking a health and safety course on your LMS at your organisation, Everglade Enterprises. They have been with the organisation for five years, and want to know what data you hold about them. Under GDPR, the right of access means you must give Alex all of the information you hold about them, including training records, performance evaluations, management feedback and appraisal comments.

2. THE RIGHT TO RECTIFICATION

If Alex requests their data and notices that something is inaccurate or incomplete, they have the right to have this rectified within the system. For instance, if they can prove that they completed a course that is not showing up on the system, this must be updated accurately. If you have shared this data with a third party, you must also inform them of the rectification where possible.

3. THE RIGHT TO ERASURE

Alex has the right to request that all of their data is deleted from your system. However, not every request for erasure must automatically be complied with. For instance, Alex may request that their data is deleted if the data is no longer necessary for its original purpose and this should generally be granted, but a request for the erasure of data which is legally required, such as a record of compliance training, does not have to be granted.

4. THE RIGHT TO RESTRICTION OF PROCESSING

Under the right to restrict processing, your organisation may store data, but not further process it. For instance, Alex may contest an assessment score stored in your LMS - in this case, you can keep this data stored in your system, but not process it further until the data has been either verified or amended.

5. THE RIGHT TO DATA PORTABILITY

This right means that if Alex wants to take the data they have given you and reuse it elsewhere, you must provide this data to them. This makes it easier for Alex to transfer their personal data between IT environments. For example, if Alex wants to access a third-party career planning website to analyse their current skills to date, they have the right to request the personal data you have stored about them at Everglade Enterprises for reuse in the other system. You must provide this data in a structured, commonly used and machine-readable format, such as a CSV file, which, ideally, could be exported automatically by your LMS.

6. THE RIGHT TO OBJECT

Perhaps signing up to your LMS automatically registers users for marketing emails, whether they opt in or not. Under GDPR, Alex can object to having their personal data used for direct marketing, profiling or processing for research and statistics. This right must be presented to Alex at the point of first communication and in your privacy notice, meaning you will need to add explicit mentions of any other reasons for collecting personal data on your LMS.

7. THE RIGHT NOT TO BE SUBJECT TO AUTOMATED INDIVIDUAL DECISION-MAKING RESULTING IN DECISIONS HAVING LEGAL OR SIGNIFICANT EFFECTS

Yes, it's wordy and unlikely in a learning context but here is an extreme example for Alex. Let's assume Alex has to keep their compliance training up-to-date as a condition of their employment. One year they fail to complete their compliance training on time and go overdue. An automated system in the organisation terminates Alex's employment with the organisation. In this case Alex could challenge that decision and request human intervention in the decision as it has a significant effect on them. It's highly likely the organisation would be forced to change this process.



WHAT DOES AN LMS THAT SUPPORTS GDPR COMPLIANCE LOOK LIKE?

32% of organisations are concerned that they are unable to manage data effectively with current technology provision.⁶

SITE POLICIES

Your LMS should enable you to track the version of a site policy and any opt-ins that a user has agreed to. Users should also be able to visit the site policy pages they have signed up to and amend their agreements.

DATA ACCESS

Your learning administrator should be able to export all of the data linked to a given user, which can be reviewed before handing the data over to the user. The user should be able to see what type of data processing is taking place with their data, and see how this aligns with the data policies they have signed up to. This includes processing of items such as appraisals, 360 feedback responses, course enrolments, progress and completion and site logins. This may or may not be in a human-readable format - it just needs to be consistent.



DATA PORTABILITY

Certain data items need to be available in a human-readable format to be ported between platforms. This may include completion data (such as courses, competencies and certifications), which a user may want to take with them to a new employer. This may be available via the learning platform's reporting functionality or the user's record of learning.

DATA DELETION

To comply with the right to erasure, your LMS should enable you to delete certain types of data from the system. You may need to keep certain data (such as certifications representing completion of compliance training), but want the ability to delete other data, such as forum posts. You could also anonymise a user's data so it can't be tracked back to them, or delete all data related to a user. Different types of data deletion may automatically be triggered a certain amount of time after a person leaves your organisation.

42% of businesses admitted that they don't have a way to determine which data should be saved or deleted based on its value.⁷

^{6,7} <https://www.veritas.com/en/uk/news-releases/2017-04-25-veritas-study-organizations-worldwide-fear-non-compliance-with-new-european-union-data-regulation-could-put-them-out-of-business>



HOW DOES TOTARA LEARN SUPPORT GDPR COMPLIANCE?

SITE POLICIES

Totara Learn allows organisations to create any number of site wide policies that users must agree to or decline. Agreement to a site policy can be made mandatory for further use of the site, multiple language translations are supported and different versions of a site policy are stored alongside corresponding consent records. Users are able to visit a dedicated site policy page and view or amend their consent as necessary.

DATA EXPORT

Administrators have the ability to export all data linked to a user, with the option to review the data prior to sending on to the individual.

This export file will allow the individual to review what type of personal data is processed within their Totara Learn site and reconcile this information with their corresponding version of the site policy. For example, from the exported file, a user will be able to see that the platform is processing items such as quiz answers, 360° feedback responses, course enrolments, progress and completions etc.

DATA PURGING

Totara Learn also provides administrators with the ability to create and manage multiple purge types. Purge types have an individual configuration, specifying the retention, deletion or anonymisation requirements of user data stored throughout the system. Users may have a purge type applied to their account so their data can be processed in accordance with a change in status or an organisation's data retention requirements.



WHAT CAN I DO TO PREPARE?

If you're worried about GDPR, don't panic! Help is at hand. Here are some things you can do right now to help protect yourself from the risks associated with non-compliance:

- ✓ Familiarise yourself with the new GDPR rights [here](#)
- ✓ Consult with your IT, digital and marketing teams to ensure everyone understands GDPR
- ✓ Consider hiring a Data Protection Officer to guide you through the process
- ✓ Download Totara and Deloitte Learning Solutions' HR guide to GDPR [here](#)
- ✓ Upgrade to an LMS that supports GDPR, such as Totara Learn 11



Totara supports GDPR compliance.

THE FUNCTIONALITY AVAILABLE INCLUDES:

- Management of data policies
- Clear consent statements and tracking of versions
- User status management
- Data anonymisation
- Data purging

For more details please visit
help.totaralearning.com/display/TPD/GDPR

*Legal disclaimer: the opinions and recommendations
in this guide should not be construed as legal advice.
Totara recommends that entities subject to
legislation seek legal counsel from qualified sources.*

NEW ZEALAND

Wellington
+64 (0)4 385 8399
enquiry@totaralearning.com

UNITED KINGDOM

Brighton
+44 (0)1273 964014

UNITED STATES

San Francisco, California
+1 707 559 9544