NATIONAL FORUM FOR THE ENHANCEMENT OF TEACHING AND LEARNING IN HIGHER EDUCATION

Forum Insight

teachingandlearning.ie

Learner Data and the General Data Protection Regulation (GDPR)

January 2018

This ***Forum Insight*** serves as a quick guide to some of the legal obligations arising from the EU's General Data Protection Regulation (GDPR), the data protection legislation that becomes enforceable across the EU from 25 May 2018. The GDPR will have an impact on how we all work with data, but it will have particular implications for the use of learner data to support student success. It is imperative that any use of such data, or any personal data, is compliant with this legislation and consistent with best practice. It is noteworthy that the GDPR enables the imposition of severe fines (potentially up to millions of euro) on organisations that are found to be in breach.

Please note that this is not an exhaustive guide to the GDPR, but an introduction to some of the major themes that will impact on how higher education institutions (HEIs) and staff use data. Compliance with these principles alone does not guarantee full compliance with the GDPR.

Definitions

Personal data refers to any information relating to a living person where that person can be identified through the data in any way. Use of any such information is governed by the GDPR.

Bear in mind that a student's name or student ID are not the only ways of identifying them. They could also be identified, for example, through being unique in some way, such as being the only mature student in a module. For such a student, their date of birth could be an identifier.

Processing means working with data in any way. It includes collecting, recording and storing data as well as any subsequent reporting or use of that data

Principles

The GDPR details a set of six principles that must be adhered to when processing personal data.

Personal data must be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and only used for these purposes.
- adequate, relevant and limited to what is necessary. In other words, only data that is required for the explicit purpose detailed above should be gathered and stored.
- accurate and up-to-date.
- stored for no longer than is necessary.
- processed in a secure manner that protects against unauthorised processing, loss and accidental destruction or damage.

Data Protection – Quick Wins

Here are a few quick steps that you can take to improve your personal compliance:

- Keep your computer's operating system and all software up to date and run your antivirus software regularly.
- Ensure that all of your electronic devices (desktop, laptop, mobile phone) are password-protected.[1]
- Always lock your computer when leaving it unaccompanied (PC: Press the Windows Key and L to lock, Mac: Press Control + Shift + Eject/Power)
- Don't print documents or emails with personal information unless it is necessary. If you do print them, be sure to store them securely and destroy them when no longer needed.
- Be conscious of how you use data. Ensure that you never include information that isn't necessary (for example, does a given report you're working on need to have students' dates of birth? Would it work just as well without them?). A useful question to ask yourself is 'Would a student be surprised that I'm using their data in this way?'

Lawful Processing

You can see from the principles above that data must be processed lawfully. This means that anyone using personal data must be able to justify doing so through meeting at least one of the six criteria below. Of these, Consent and Legitimate Interests are the most likely grounds on which HEIs would process learner data

- Consent – Where students have given full, free and explicit consent (see the following section for further details)
- Contract – Where processing is necessary to satisfy a contract with the student
- Legal Obligation – Where processing is required to comply with an EU or member state legal obligation to which the HEI is subject
- Vital Interests – Where processing is needed to protect the life of the data subject
- Public Interest – Where processing is necessary for the public interest or in the exercise of an official authority vested in the data controller
- Legitimate Interests – Where processing is necessary for the legitimate interests of the HEI, in other words where data processing is required to enable the HEI to carry out its core functions. This basis is only lawful if it does not override the fundamental rights and freedoms of the student. Any HEI that uses this as their basis for legal processing must be in a position to prove that they have considered the rights and reasonable expectations of the student and to document the steps they have taken to ensure that all students' rights are protected.

Consent

As listed above, consent is one of the legitimate bases for processing personal data. The GDPR lists a number of conditions that are required for consent to be considered authentic.

These include the following:

- Consent must be freely given. It is not enough, for example, to include reference to learning analytics in the general terms and conditions that students must accept at the start of each year in order to register. This does not constitute freely-given consent for analytics as students do not have the choice to refuse such terms and conditions.
- The terms to which students are consenting must be concise and easily understandable, and must use 'clear and plain language'.
- Consent must be informed: 'The [student] should be aware at least of the identity of the [HEI] and the purposes of the processing.'
- The HEI must be able to demonstrate evidence that the student has given consent.
- Consent must be given through an 'affirmative act'. In other words, expressions of consent must be based on an action that students have taken (such as clicking an 'Accept' button). To this end, 'silence, pre-ticked boxes or inactivity' are not recognised as consent.
- Consent must be given for each individual data processing operation.
- Students must have the right to withdraw consent at any time and it must be as easy to withdraw consent as it was to give it.
- The minimum legal age at which a person can give consent for their data to be used is 16 years.

Transparency

Being upfront and open with students about how we use their data is critical. To remain transparent, HEIs must provide students with key information regarding the use of their data. This information must include the following:

- The contact details of the institution's Data Protection Officer
- The purposes of the processing
- The legal basis for the processing (see previous section on Lawful Processing)
- Where Legitimate Interests are used as the legal basis for the processing (see previous section on Lawful Processing), HEIs must detail what these interests are.
- The categories of data that are used
- The recipients or categories of recipient of the data (e.g. student advisors)
- If there is an intention to transfer their data to another country or to an international organisation
- The period for which the data will be stored (or, if that is not possible, the criteria that will be used to determine how long it will be stored)
- An explanation of students' rights around access to and rectification or erasure of their data
- An explanation of students' rights in relation to objecting to the processing of their data
- The right to withdraw consent at any time (where consent is the legal basis of the processing – see previous section on Lawful Processing)
- The right to lodge a complaint with the Data Protection Commissioner's Office

GDPR – Key Steps for Preparation

The Data Protection Commissioner's Office has published a guide to preparing for the GDPR[2] that outlines key steps organisations should undertake. These steps include:

- identifying the personal data held.
- implementing effective safeguards to ensure data is stored securely.
- knowing the legal basis you rely on (see previous section on Lawful Processing).
- ensuring you are collecting the minimum data necessary, that the data is accurate and that it is held for no longer than required.
- being transparent with students about the reasons for collecting their data, how it will be used and how long it will be stored.
- establishing whether you are holding special categories of data (defined in Article 9 as data revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership'. These categories also include genetic data, biometric data and data relating to a person's health, sex life or sexual orientation). Due to the sensitivity and restrictions on the use of such data, HEIs are advised against its inclusion in student success initiatives.
- considering how you will process student requests for access to and rectification or erasure of their data (as applicable) or the recording and withdrawal of consent.
- compiling policy/procedure documents that detail how compliance with data protection legislation is ensured.

Further Reading

The Data Protection Commissioner's Office has compiled a considerable suite of resources, available at http://gdprandyou.ie/resources/

These include checklists and introductory guides, as well as the full text of the General Data Protection Regulation.

1. Further information available at https://support.google.com/accounts/answer/32040?hl=en
2. Available at http://gdprandyou.ie/wp-content/uploads/2017/12/A-Guide-to-help-SMEs-Prepare-for-the-GDPR.pdf'

DOI: 10.6084/m9.figshare.6097133