GENERAL DATA PROTECTION REGULATION IMPLEMENTATION IN HIGHER EDUCATION INSTITUTIONS

A. Šidlauskas, T. Limba
Mykolas Romeris University (LITHUANIA)

Abstract

The General Data Protection Regulation, more commonly known as “GDPR”, is a regulation in the European Union law implemented since the 25th of May, 2018. It aims to increase data protection for EU citizens and individuals within the European Economic Area and simplify international regulations by unifying the European system.

The GDPR is a law that protects the personal information of all EU citizens, regardless of where their personal information is located and stored. The GDPR aims to give EU citizens greater protection and control of their personal information. Regulation coverage extends to all organizations – whether or not they have physical EU footprints – that control or process the personal information of EU citizens.

Many higher education institutions are gaining international students at a high rate throughout their various online education programs. If any portion of your online educational student base is made up of EU citizens, you will want to ensure that you have GDPR compliance plans in place.

The scientific problem, GDPR leaves much to interpretation and higher education institutions unaware of how to implement GDPR requirements.

The main purpose of this article is to provide an action plan to help higher education institutions implement GDPR requirements.

Tasks:
1. Identify the key aspects that GDPR should have on conceptual impact on data protection law.
2. Describe the challenges faced by higher education institutions in implementing the GDPR.
3. Provide a GDPR implementation model.

In this scientific article, methods of document analysis, scientific literature review, case study and generalization are used.

Keywords: General Data Protection Regulation (GDPR), personal data, higher education institutions, implementation of the GDPR.

1 INTRODUCTION

The implementation of the GDPR requirements demands substantial financial and human resources, many higher education institutions are not necessarily prepared for the changes and may lack awareness of the upcoming requirements. Early adoption of the required changes not only guarantees compliance with the GDPR but can also bring a competitive advantage [1].

The GDPR is designed to create business opportunities and stimulate innovation through a number of steps including [2]:

1. a single set of EU-wide rules – a single EU-wide law for data protection is estimated to make savings of €2.3 billion per year;
2. a data protection officer [3], responsible for data protection, will be designated by public authorities and by businesses which process data on a large scale;
3. one-stop-shop – businesses only have to deal with one single supervisory authority (in the EU country in which they are mainly based);
4. EU rules for non-EU companies – companies based outside the EU must apply the same rules when offering services or goods, or monitoring behaviour of individuals within the EU;
5. innovation-friendly rules – a guarantee that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default);
privacy-friendly techniques such as pseudonymisation (when identifying fields within a data record are replaced by one or more artificial identifiers) and encryption (when data is coded in such a way that only authorised parties can read it);

removal of notifications – the new data protection rules will scrap most notification obligations and the costs associated with these. One of the aims of the data protection regulation is to remove obstacles to free flow of personal data within the EU. This will make it easier for businesses to expand;

impact assessments – businesses will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals;

record-keeping – SMEs are not required to keep records of processing activities, unless the processing is regular or likely to result in a risk to the rights and freedoms of the person whose data is being processed.

The GDPR applies to the control or processing of data by institutions with “establishments” within the EU. The GDPR does not define what an “establishment” is, other than to say that the term “establishment” “implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.” In determining whether they have “establishments” in the EU, within the meaning of the GDPR, higher education institutions and boarding schools may want to consider factors such as: whether they operate a satellite campus in an EU state, whether they employ staff in an EU state, whether they rent office or other space in an EU state, whether they have relationships with other colleges, universities, or boarding schools in EU states, whether they have partnerships with corporations in the EU, and whether they send study abroad students to EU states.

Specifically, higher education institutions will need to follow a number of data privacy and data security requirements, such as:

1. Ensuring data security practices are in place.
2. Implementing privacy restrictions and personal data usage policies.
3. Developing a personal data consent collection process.
4. Identifying a data protection officer (DPO).
5. Implementing appropriate measures to protect personal data.
6. Adhering to the GDPR breach notification processes.

Implementation of the European General Data Protection Regulation (GDPR) can be complex and challenging.

2 METHODOLOGY

In this scientific article, methods of document analysis, scientific literature review, case study and generalization are used.

Document analysis is a systematic procedure for reviewing or evaluating documents—both printed and electronic (computer-based and Internet-transmitted) material. Like other analytical methods in qualitative research, document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge.

A literature review surveys books, scholarly articles, and any other sources relevant to a particular issue, area of research, or theory, and by so doing, provides a description, summary, and critical evaluation of these works in relation to the research problem being investigated. Literature reviews are designed to provide an overview of sources you have explored while researching a particular topic and to demonstrate to your readers how your research fits within a larger field of study.

A case study is an in depth study of a particular situation rather than a sweeping statistical survey. It is a method used to narrow down a very broad field of research into one easily researchable topic. This method of study is especially useful for trying to test theoretical models by using them in real world situations.
Generalization, which is an act of reasoning that involves drawing broad inferences from particular observations, is widely-acknowledged as a quality standard in quantitative research, but is more controversial in qualitative research. The goal of most qualitative studies is not to generalize but rather to provide a rich, contextualized understanding of some aspect of human experience through the intensive study of particular cases. The goal of most qualitative studies is not to generalize but rather to provide a rich, contextualized understanding of some aspect of human experience through the intensive study of particular cases [10].

3 RESULTS

3.1 Personal Data

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’) [11].

The GDPR defines some categories of personal data as very sensitive and imposes the prohibition to process them with very few exceptions. These categories of data are indistinguishably referred to as “Specially Protected Data”, “Special Categories of Personal Data” or “Sensitive Data” [12].

<table>
<thead>
<tr>
<th>Specially Protected Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Racial or ethnic origin;</td>
</tr>
<tr>
<td>Political opinions;</td>
</tr>
<tr>
<td>Religious or philosophical beliefs;</td>
</tr>
<tr>
<td>Trade union membership;</td>
</tr>
<tr>
<td>Genetic data;</td>
</tr>
<tr>
<td>Biometric data for the purpose of uniquely identifying a natural person;</td>
</tr>
<tr>
<td>Data concerning health or a natural person’s sex life and/or sexual orientation.</td>
</tr>
</tbody>
</table>

Institutions will be held far more accountable for the data they hold. As well as records of what personal data exist within the organisation, the GDPR requires a documented understanding of why information is held, how it is collected, when it will be deleted or anonymised, and who may gain access to it. Institutions are still required to apply appropriate organisational and technical measures to keep information secure and there are new duties to report security breaches to the Information Commissioner’s Office (ICO) and, in some cases, to the individuals affected [13].

GDPR Key Changes [14]:

1. More rigorous requirements for individuals’ consent, that should be obtained using a clear and understandable language. Silence and pre-validated options or omissions are not valid forms of consent;

2. No longer the use of long and illegible terms and conditions full of legal terminology. More transparency is required and data processing information should be easy to access and understand;

3. The extension of special data categories to: biometric data, race, ethnic origin, politics, religion, genetics, health, sex life and sexual orientation. The processing of such types of data is prohibited by default and can only be processed if the data subject gives explicit consent or in a small number of specified situations;

4. The right for individuals to be informed if their data are being processed, how, where, and for what purpose;
5 The portability of personal data between companies;
6 The right to be forgotten when data are no longer needed to the original purposes of processing;
7 Ensuring Privacy by Design (PbD) which means that data protection should be included since the beginning of the systems’ design;
8 The obligation to notify supervisory authorities and individuals affected within a maximum of 72 hours when a data breach may result in a risk for the rights and freedoms of people, subject to heavy penalties.

As a result of the GDPR, students will have more control over their personal data. Not only will they have access to their personal information with them, but students will also have the right to be forgotten. Essentially, the student will have the right to have their personal data erased from the institution’s system if any one of several conditions apply, such as data is no longer necessary or data has been unlawfully processed, for example.

3.2 Higher Education Institution’s Compliance with the GDPR

To comply to GDPR, organisations need to embed seven privacy principles within their operations:

1 Lawfulness, fairness and transparency.
2 Purpose Limitation.
3 Data Minimisation.
4 Accuracy.
5 Storage Limitation.
6 Integrity and Confidentiality.
7 Accountability.

Implementation of the European General Data Protection Regulation (GDPR) can be complex and challenging. Nine steps for implementing GDPR [15]:

1 Prepare for your GDPR project. 1) Create a project plan to implement GDPR; 2) Include the right stakeholders in your GDPR project; 3) Conduct a readiness assessment to find out what tasks you need to perform.
2 Define your Personal Data Policy and other top-level documents. 1) Create an internal Data Protection Policy for personal data; 2) Create other top-level policies as needed – e.g., the Data Retention Policy; 3) Create awareness among employees about key GDPR requirements; 4) Make a decision with regard to the assignment of a Data Protection Officer, and make sure the decision is documented; 5) If required, appoint a Data Protection Officer and communicate their name to the Supervisory Authority.
3 Create an inventory of processing activities. 1) List your processing activities and how these map to legitimate purposes defined in GDPR; 2) Be sure your company has published the necessary privacy notices for data subjects.
4 Define an approach to manage data subject rights. 1) Implement data subject rights through establishing a legal basis for processing; 2) Data subjects can provide consent and request access; 3) Your company must keep a record of data subject rights requests.
5 Implement a Data Protection Impact Assessment (DPIA). 1) Conduct a DPIA when initiating a new project, or when implementing a change to your information systems or a product.
6 Secure personal data transfers. 1) Analyse what personal data is being transferred outside of your company, and when; 2) Take necessary legal and security measures to adequately protect personal data when personal data is transferred outside of the company.
7 Amend third-party contracts. 1) Amend third-party contracts that include processing of personal data to become compliant with the GDPR.
8 **Ensure the security of personal and sensitive data.** 1) Implement the necessary organisational and technical measures to protect the personal data of data subjects; 2) Consider privacy and protection when designing new systems and processes.

9 **Define how to handle data breaches.** 1) Set up the processes to identify and handle personal data breaches. 2) Prepare for notifications to the Supervisory Authority and data subjects, if required, in the case of a personal data breach.

Steps to GDPR Compliance [16]:

1 **Update Your Institution’s Privacy Policy to Include Information Required by the GDPR.** Under the GDPR, when a data controller (i.e., a higher education institution) collects personal data from a data subject, the data controller must provide the data subject with specific pieces of information including, but not limited to: (1) the purpose for which the data is being processed; (2) the legal basis of the processing including, if applicable, the legitimate interests of the controller in processing the data; (3) the categories of personal data concerned; and (4) if applicable, the recipients of the data.

2 **Ensure that Your Institution Has Implemented Appropriate Security Measures To Protect Personal Data.** Data controllers must implement appropriate security measures and protect personal data against accidental or unlawful destruction, loss, alteration, or disclosure. Your institution’s data security measures should include mechanisms for detecting personal data breaches.

3 **Update Your Institution’s Agreements with its Data Processors.** When an institution engages another party to process personal data on its behalf, the parties must enter into a contractual relationship to ensure that the data processor complies with the requirements of the GDPR.

4 **In the Event of a Security Breach, Notify the Relevant Supervisory Authority.** In the event of a security breach, controllers must notify the relevant supervisory authority if the breach is likely to result in a risk to the rights and freedoms of natural persons. This notification must be given within 72 hours of the controller’s discovery of the breach. Additionally, under certain circumstances, the data controller will also be required to report the data breach to affected data subjects.

5 **Obtain Students’ Consents to Send Unsolicited, Direct Marketing Communications.** GDPR guidance provides that if an entity plans to send direct email marketing communications to particular individuals located in the EU with whom it does not have a prior relationship, the entity must obtain the consent of the individual before doing so.

Steps towards GDPR compliance [17]:

1 **Data audit** – to identify what data they currently collect from and about EU residents.

2 **Data justification**– to evaluate the purpose of each data point they collect and process, as to prepare to articulate its value in furthering institutional mission.

3 **Consent EU**– residents must also give consent for their information to be processed in specific ways. And while the text of GDPR doesn’t model this, they must also articulate the purpose of data collection and application in layman’s terms that the resident can understand.

4 **Data access, integrity, and deletion processes** – need to put in place processes that allow EU residents to access their data in a format they can understand, to revise it to ensure accuracy, to limit its application, and to request its deletion.

Since the new protections enacted by GDPR are data-focused, most campuses should start focusing on compliance around data discovery, management processes, and policies.
These are all incredibly important points that must be followed should you agree to the GDPR compliance requirements. On the one hand, universities and other research institutions are of course providing general information about the GDPR to their employees, and have a Data Protection Officer who can be contacted for specific matters. On the other hand, GDPR-compliant strategies need to be instantiated to the specific research problem, and many of these are difficult to interpret without domain-specific knowledge. Therefore, researchers should themselves be aware of the implications of the GDPR and have reflected about it [18].

4 CONCLUSIONS

The GDPR is a law that protects the personal information of all EU citizens, regardless of where their personal information is located and stored. The GDPR is designed to create business opportunities and stimulate innovation. To comply to GDPR, organisations need to embed seven privacy principles within their operations – Lawfulness, fairness and transparency; Purpose Limitation; Data Minimisation; Accuracy; Storage Limitation; Integrity and Confidentiality; Accountability.

Higher education institutions will need to follow a number of data privacy and data security requirements:

1. Ensuring data security practices are in place; Data audit.
2. Implementing privacy restrictions and personal data usage policies.
3. Developing a personal data consent collection process.
Identifying a data protection officer (DPO).
Implementing appropriate measures to protect personal data.
Adhering to the GDPR breach notification processes.

The GDPR implementing steps in higher education’s institutions:
1. Prepare for your GDPR project; Data audit.
2. Define your Personal Data Policy and other top-level documents; Update Your Institution’s Privacy Policy.
3. Create an inventory of processing activities; Data justification.
4. Define an approach to manage data subject rights; Consent; Consents to send unsolicited, direct marketing communications; Data access, integrity, and deletion processes.
5. Implement a Data Protection Impact Assessment (DPIA).
6. Secure personal data transfers.
7. Amend third-party contracts; Update your institution’s agreements with its data processors.
8. Ensure the security of personal and sensitive data; Security measures to protect personal data.
9. Define how to handle data breaches; Security breach, notify the relevant supervisory authority.

It is wise to follow these steps to plan your GDPR implementation strategy and to understand that we are entering a new era where the consumers are in control of their data privacy.

Institutions will be held far more accountable for the data they hold. As well as records of what personal data exist within the organisation, the GDPR requires a documented understanding of why information is held, how it is collected, when it will be deleted or anonymised, and who may gain access to it. Institutions are still required to apply appropriate organisational and technical measures to keep information secure and there are new duties to report security breaches to the Information Commissioner’s Office (ICO) and, in some cases, to the individuals affected.

REFERENCES


