CHALLENGES FOR THE IMPLEMENTATION OF THE GDPR IN HIGHER EDUCATION INSTITUTIONS IN PORTUGAL

N. Bessa Vilela
IJP- Portucalenniside Portucalense Infante D. Henrique (PORTUGAL)

Abstract

The General Data Protection Regulation that came into force on the 25th May 2018 has been the centre of discussion within the administrations of the Higher Education Institutions, Data Protection Officers and the CNPD (National Committee for Data Protection).

Accountability for the breach of the Regulation and the leakage of private data is one of the biggest issues, as it is, at the moment, virtually impossible to determine what data is to be considered private, either by identifying or making the person identifiable.

Portuguese Higher Education institutions were, and are not prepared for fully meeting the rules set forth by the regulation. This lack of preparation is not due to the lack of legal provisions, as the Regulation directly applies in all Member States of the European Union but rather because the specificities of such an institution are not completely in sync with the letter of the law. The Right to be forgotten, for instance, shall not apply as there is the obligation of keeping records of all students and alumni. The same applies to thesis and dissertations that are to be made public as they are considered a contribution to knowledge and should be accessible for all those who want to deepen their knowledge in the subject in question.

If in the one hand assuring data processing is handled in a proper manner is a simple task to perform, given the mapping and verification of employees profile accesses, the same can’t be said about other aspects of the GDPR, as the understanding of its application to certain Institutional particularities, was not yet reached.

There are basic and fundamental principles that may be breached in case Higher Education Institutions decide to follow the GDPR in its full scope, which will be, in the end, the only way to do it, as the need to comply with EU can’t be put aside by any national legal or practical constraint.

So, let’s see… The principle of transparency, for instance, deeply collides with the GDPR. How will grading be transparent and accessible to the general Public if Personal Data can’t be disclosed?

This is where the concept of private data becomes more confusing within the Higher Education Institutions.

We will undertake a deep legal analysis of the regulations, the concepts therein foreseen and try to find a solution for the development of a manual of best practices applicable to all Higher Education Institutions in the Country. Advisory measures issued by CNPD will also be analyzed within the scope and reach of the GDPR.

Issues such as determining which information can and shall be disclosed to the general public, or if the principle of transparency is to be cast aside by the CDPR. Questions such as if students grades and ID numbers are a personal data, as well as the right way to inform the students of their grades will also be clarified, as well as the access to the scientific repository.

Keywords: GDPR, Higher Education, EU Law, Transparency, Best practices.

1 INTRODUCTION

Life in a globalized world where the mobility of people the movement of one’s data is a constant, there are fewer and fewer barrier or mechanisms that can be made use of in order to safeguard a person’s privacy and their fundamental right to private life.

The General Data Protection Regulation (herein after GDPR) [1] is intended to strengthen and unify the processing and data protection of all individuals within the EU, regardless of their citizenship. The Regulation, became effective on May 24th 2016, and entered into force, in all EU Members on the 25th May 2018. From that day on, any breach of the provisions set forth in the Regulation, will result with heavy fines to all institution that fail to comply with the law.
The path to full compliance with the GDPR hasn’t been easy for any organization. Higher Education Institutions are not the exception. Alongside with health providers, such Institutions are, and will be, the most affected by the provisions set forth in the GDPR.

Individual control, in particular with regard to one’s person, has been described as a reflection of fundamental values such as autonomy, privacy, and human dignity [2], values that are pivotal in the European Union.

It arises from the lettering of the GDPR that Higher Education Institutions, as controllers, become accountable for all the personal information of all their students. The concept of personal data is broader than it may, at first sight, seem.


The specify of the processing of Data in Higher Education institutions requires a full perception of the amount of data that is in their data bases and for which they become responsible. Data is with no shade of doubt, the currency of the digital economy today, and its monetary value is large and still growing [5].

2 METHODOLOGY

A thorough analysis of the GDPR was undertaken. The concept of data protection, as set forth by the Regulation itself, as well as the exhaustive case law of the ECJ, was studied and scrutinized in order to ascertain which data, of that processed by the Higher Education Institutions can be qualified as Personal Data. The specific concept of sensitive data had also to be studied, as several of the personal information processed by those Institutions is of sensitive nature.

The collision between data protection, as well as the disclosure of student’s data, and the principle of transparency was also analysed.

A deep legal analysis of the regulations, the concepts therein foreseen and try to find a solution for the development of a manual of best practices applicable to all Higher Education Institutions in the Country. Advisory measures issued by CNPD will also be analyzed within the scope and reach of the GDPR.

3 RESULTS

The specify of the processing of Data in Higher Education institutions requires a full perception of the amount of data that is in their data bases and for which they become responsible. The acknowledgement of all data flow, and the develop of mechanisms to regulate and ensure its protection deems necessary. For that the reason the GDPR, itself, foresees the need for a DPO, or committee of DPOs.

DPOs that hold solid understanding of the GDPR, as well as some IT training have come to be an institution’s most valuable asset when it comes to data processing and protection. They will ‘project manage’ the transition from the existing to the necessary standards of protection and be responsible for ensuring that the Institution complies with the Regulation, whilst acting as an educator, explaining the changes in a way that is both straight-forward and relevant to the institution they are working at.

The existing privacy policies often serve more as liability disclaimers for businesses than as assurances of privacy for consumers [6]. This new Regulation came to cast aside such possibility, creating a new paradigm that is reveling itself to be of indescribable difficulty, the full protection of the data of the person and the need for explicit permission for its processing [7] [8].
3.1 Data Flow

We were able to identify 3 stages of the typical, ideal, consent-based data processing timeline. In the first stage, information is received, and permission for processing is explicitly granted; being that consent in one of the 6 legal basis for data processing in accordance with Article 6 of the GDPR; in the second stage, the collected data is used to meet the goals of the data controller, limited by the law, and according to the legal expectation of his data processing, and thirdly, there is the reutilization of data.

The impact of GDPR in higher education will be profound. Under new GDPR rules, Higher Education Institutions became more accountable for the data they possess. As such, they need to have organized records of all personal data that exists, as well as all necessary documentation justifying the need to hold such data, the way it had been collated, who has access to it and when it will be removed or anonymized, if ever [9].

3.2 The principle of transparency

Transparency of personal data processing is a basic privacy principle and a right that is well acknowledged by data protection legislation (GDPR).

The concept of transparency comprises both ‘ex ante transparency’ and ‘ex post transparency’ [10]. Ex ante transparency exists to inform about the intended data collection, processing and disclosure, enabling the anticipation of eventual consequences that might arise from the disclosure of data even before data has actually been disclosed. Ex post transparency provides insight about what data were collected, processed or disclosed by whom and to whom, and whether the data processing totally complied with the negotiated or stated policies and should particularly inform about consequences if data already has been revealed [11].

Other side of the principle transparency is, at times, related to the possibility of the population to surveil the work of the public administration [12]. In this sense we mean that the public disclosure of grades of students, that are considered, under our perspective, as personal data, might work in the public interest, even if in breach of the protection of the data of the student that might, for several reasons, prefer to have the grade made confidential, and available to him alone.

3.3 The national paradigm

The CNPD has failed to find a solution for the difficulties in implementing the GDPR in the Portuguese Higher Education Institutions.

Several advice has been issued, such as the respect for the minimum necessary exposure of data. No definition for what it actually means is lacking.

Institutions were forbidden of publishing, on open website any information regarding the grades of students. Such information should only be made available in their own personal user profile.

The publication of paper grids with the grades of students, containing their names, number of classes attended and missed, as well as any other unnecessary information was forbidden. Questions still remain in what concerns to the grades that shall follow along with the student’s name.

Two solutions have been put forth:

• No grids are to be published on the hallways and corridors of the Institutions;
• The name of the student is replaced by the student's ID number, which is revealed to the student alone.

None of the above seems to please the academic community that is used to being able to "surveillance" the performance of the students, and colleagues, regardless of the lack of relevance such information is supposed to have, following none of the exceptions put forth on the GDPR, in Article 6.

3.4 The repository

Student's works are supposed to be made available to the institution that has the obligation to keep it in its records for the period of time set forth by the National Legislation.

Access to such work is subject to the permission of the author/student, that may wish to have its work publicly available, or to have it unpublished and deposited for the single purposes legally foreseen.

As a contribution for knowledge all scientific works should be made public, in the perspective of the author.

4 CONCLUSIONS

Having concluded the research and gone through the available international bibliography referring to this same matter in other countries, we have come to the conclusion that the difficulty in properly applying the GDPR is transversal to all Higher Education Institutions in all the Member States, as the GDPR did not foresee the specificity of such field of action. An amendment to the existing GDPR might seem an appropriate solution for the global problem all Educational Institutions are facing, not only those of Higher Education.

Portuguese Higher Education institutions were, and are not prepared for fully meeting the rules set forth by the regulation. This lack of preparation is not due to the lack of legal provisions, as the Regulation directly applies in all Member States of the European Union but rather because the specificities of such an institution are not completely in sync with the letter of the law. The Right to be forgotten, for instance, shall not apply as there is the obligation of keeping records of all students and alumni. The same applies to thesis and dissertations that are to be made public as they are considered a contribution to knowledge and should be accessible for all those who want to deepen their knowledge in the subject in question.

The specific of the processing of Data in Higher Education institutions requires a full perception of the amount of data that is in their data bases and for which they become responsible. The acknowledgement of all data flow, and the develop of mechanisms to regulate and ensure its protection deems necessary. For that the reason the GDPR, itself, foresees the need for a DPO, or committee of DPOs.

Transparency of personal data processing is a basic privacy principle and a right that is well acknowledged by data protection legislation (GDPR).

The CNPD has failed to find a solution for the difficulties in implementing the GDPR in the Portuguese Higher Education Institutions.

Several advice has been issued, such as the respect for the minimum necessary exposure of data. No definition for what it actually means is lacking.

REFERENCES


