Issues in Information Systems
Volume 24, Issue 2, pp. 232-241, 2023

DOI: https://doi.org/10.48009/2_iis_2023_120

The GDPR and UK GDPR and its impact on US academic institutions

Leila Halawi, *Embry Riddle Aeronautical University, halawil@erau.edu*
Alpesh Makwana, *Embry Riddle Aeronautical University, makwana1@erau.edu*

Abstract

This research paper delves into the implications of the General Data Protection Regulation (GDPR) and the United Kingdom (UK) GDPR on academic institutions, shedding light on their significance for organizations and educational establishments handling data from individuals in the European Union (EU) and the UK. Non-compliance with these regulations can lead to substantial penalties. The study focuses specifically on US Higher Education and presents actionable measures that institutions can adopt to enhance compliance, fortify data protection, and safeguard the privacy of individuals.

Keywords: GDPR, UK GDPR, compliance, data protection, US academic institutions.

Introduction

The general data protection regulation (GDPR) and the United Kingdom (UK) GDPR are two distinct sets of data protection regulations that establish rules for the collection, processing, and usage of personal data within the European Union (EU) and the UK. One key difference between GDPR and UK GDPR is that UK GDPR applies only to data subjects in the UK, whereas GDPR applies to data subjects in all EU member states. The GDPR applies to foreign corporations if a cyberattack results in the identity theft of any individual within the EU territory. Consequently, organizations that conduct business in the EU and the UK must comply with GDPR and UK GDPR.

Beginning in 2018, when GDPR came into effect, companies and institutions have been revising their policies to adhere to the rigorous standards set by these regulations (Calder, 2018; Voss & Bouthinon-Dumas, 2021). Businesses in the US, including colleges and universities, are subject to GDPR if they handle data associated with people in Europe. Any higher education institution that gathers information in any capacity from individuals physically residing in the European Union (EU), such as alumni, vendors, and students, is obliged to adhere to GPDR regulations. These establishments are also subject to the Data Protection Act of 2018, which supplements the EU GDPR and the General Data Protection Law (LGPD) for Brazil (Erickson, 2019). Any failure to conform to the rules will lead to severe fines and could cost US institutions more than $23 million in penalties (Mckenzie, 2018). The governing body for GDPR, the European Data Protection Board (EDPB), has issued numerous fines to companies and organizations like Google LLC, Marriott International, and H&M for violating GDPR (European Data Protection Board, 2019, 2020).

The UK GDPR came into force on January 1, 2021, and replaced the EU GDPR in the UK (Bainbridge & Pearce, 1998). The UK GDPR largely mirrors the EU GDPR but includes some specific provisions that

reflect the UK's status as a non-EU country. Marriot International was fined £ 18.4 million by the UK Information Commissioner's Office (ICO) in October 2020 for failing to safeguard the personal information of approximately 339 million guests worldwide, of which 7 million were UK residents (Reuters, 2020). In July 2019, the UK's Information Commissioner's Office (ICO) announced its intention to fine Marriott International £99 million ($124 million) for a data breach that exposed the personal data of millions of customers. The fine was later reduced to £18.4 million ($23 million) in March 2020. Organizations such as Google, Microsoft, Facebook, Airbnb, and Apple have altered their policy and processes to minimize the risks.

According to Borio, a lawyer who counsels the European Association of Study Abroad, the GDPR would roughly affect all US higher education institutions (2018). The EU's GDPR and the UK GDPR will impact any organization worldwide that processes data relating to people in these regions, including US colleges and universities. "The Information Systems Audit and Control Association (ISACA) found that fewer than one-third of senior executives and boards of directors globally are satisfied with their organization's progress in preparing for GDPR. Also, 35% of respondents were unaware of whether their organization had made any progress (ISACA 2018)."

Like most, the academic institution in the US has many relationships with Europe or people based in Europe and the UK. Consequently, they need to be apprehensive about this regulation. This research focuses on raising awareness and improving data protection and privacy to a higher level. It is common knowledge that many universities, including ours, have become targets of hackers in recent times, making us vulnerable to various security breaches. These breaches allow competitors to gain an advantage, damage the university's reputation, and erode trust among multiple stakeholders.

As of May 2023, five United States (US) states have successfully enacted comprehensive consumer data privacy laws. Notably, California, Colorado, Connecticut, Utah, and Virginia have all implemented legislation that significantly impacts various institutions' operations and data privacy. The enactment of these laws empowers consumers with increased control over their data and its utilization by businesses.

Furthermore, these laws impose more significant transparency obligations on firms, compelling them to disclose their data collection and usage practices. Since these laws are relatively new, it is too early to tell their full impact. It is important to emphasize that this paper will not delve into the details of the Federal Trade Commission (FTC) or other federal data privacy laws within the United States.

This research aims to highlight the impact of the EU GDPR and the UK GDPR on US higher education and identify measures institutions can take to improve compliance with these regulations and enhance data protection and privacy. This research seeks to answer the following questions: 1) How do US academic institutions comply with the GDPR and UK GDPR provisions? 2) What steps can US academic institutions take to ensure compliance?

This article begins by providing an overview of the fines and the general impact of GDPR and UK GDPR on institutions. Subsequently, the study presents a literature review of the two regulations highlighting their requirements, similarities, and differences and examining their influence on academic institutions in the United States. A list of critical steps that can help ensure compliance follows. The conclusion is presented last.

General Data Protection Regulation (GDPR) Overview

The GDPR emphasizes the contrasts in protecting personal information and privacy between the US and the EU. It started on May 25, 2018, and supersedes the EU Data Protection Directive implementations (UK the "Data Protection Act"). All institutes that gather and process the personal data of EU data subjects are affected. The regulation is borderless and applies to data processors and controllers. The penalties are up to 20 M € or 4% of the organization's annual global turnover, whichever is higher. Data subjects can claim compensation for damages from breaches of their data.

The GDPR establishes uniform legal grounds for processing personal data, obtaining consent for data collection, and protecting the rights of individuals whose data has been collected. This encompasses data under Article 9 of the GDP, which includes sensitive information such as race, ethnicity, political opinions, religious or philosophical beliefs, trade union memberships, genetics, biometrics, health, and sexual orientation. In addition, Article 6(4) of the GDPR outlines the factors that data controllers must consider when deciding whether to grant new researchers access to a dataset for reuse. This required universities, research institutions, and data archives to modify their procedures and protocols regarding data collection, documentation, and distribution.

The goal of GPDR is to 'give citizens back the control of their data, while imposing strict rules on those hosting and 'processing' this data, anywhere in the world," and "one of the things GDPR states is that data 'should be erasable.' Since throwing away your encryption keys is not the same as 'erasure of data,' GDPR forbids us from keeping personal data on a blockchain level (Herian, 2018). Data protection authorities' enforcement of the rules in EU member states has not yet ramped up due to the lack of resources, difficulties in cross-border enforcement, and the lack of business cooperation.

According to Brown and Marsden (2013), the EU has successfully influenced other regional privacy laws by limiting the transfer of personal data from member states to countries that do not have adequate privacy protection. This determination of "adequacy" is overseen by the European Commission and requires other states to incorporate many of the essential protections outlined in EU data protection directives and regulations into their national laws.

Key Requirements For the GDPR

Listed below are the essential requirements for an institution to comply with GDPR:

- Breach Notification: establishing mechanisms to report Privacy breaches to the regulator within 72 hours and potentially to the data subjects.
- Privacy by design: reduce and minimize the collection of personal data and ensure that the proper security controls are in place throughout all development phases.
- Data Subject's rights: New rights include the right to erasure and data portability.
- Consent: Requirement to gain unambiguous consent.
- Data Protection Officer: DPO is required for organizations that conduct regular and systematic monitoring of data subjects on a large scale or process Special Categories of data on a large scale.

United Kingdom (UK) GDPR

The UK GDPR is a data protection regulation that applies to the United Kingdom (UK) due to its departure from the EU. The UK GDPR came into effect on January 1, 2021, and is primarily based on the GDPR, with some modifications to reflect the UK's legal and regulatory framework. Like the GDPR, the UK GDPR applies to any organization that processes the personal data of UK residents, regardless of where the organization is located.

Differences Between GDPR and UK GDPR

Organizations must understand the differences between the GDPR and UK GDPR to ensure they comply with the relevant regulations in their operations. This requires a comprehensive understanding of regulations' jurisdiction, applicability, and legal nuances of both regulations, as well as ongoing efforts to stay up-to-date with any changes or updates.

- Jurisdiction: The GDPR applies to all EU member states, while the UK GDPR applies only to the UK.
- Applicability: The GDPR applies to organizations that process the personal data of EU residents, while the UK GDPR applies to organizations that process the personal data of UK residents.

The UK GDPR makes some modifications to the GDPR to reflect the UK's legal and regulatory framework, such as changes to the terminology used in the regulation.

GDPR & US Academic Institutions

Academic Institutions in the US typically have a diverse community of international students, prospective students, distance learning students, alums, donors, vendors, and faculty who may work across different counties. Non-compliance with GDPR could lead to significant financial costs, especially for institutions with worldwide locations and distributed models.

Academic institutions must now provide all stakeholders, including faculty, staff, and students, with clear and concise information about how their personal data is collected, used, and shared and the right to rectify or erase it. Students must now be allowed to opt out of particular data collection and use practices. Academic institutions must now take steps to protect student data from unauthorized access, use, or disclosure.

To comply with GDPR and US data privacy laws, institutions must reduce the data they collect, restrict the processing of personnel data, develop privacy statements, enact policies, and implement systems to ensure the protection and anonymity of EU and UK data.

However, merely having a privacy statement or simple policies is insufficient. Institutions must engage in extensive data mapping to identify data under GDPR protection and prepare to handle such data. The ramifications of non-compliance can be severe, and some organizations have abandoned operations in the EU due to GDPR. Therefore, academic institutions must prioritize compliance with GDPR to avoid significant financial costs and reputational damage.

Identifiers for Personal Data

Academic institutions and businesses must be aware of the personal data they collect, process, and store. It is crucial to identify and categorize all personal data based on their sensitivity, including online and unique category identifiers.

Data are classified into three categories.

1. Personal data about the data subject include name, address, email, passport number, date of birth, personal photos, genetic data, ID, phone number, and financial and bank information.

2. Online identifiers refer to personal data about a user's devices, applications, and protocols. Online identifiers include IP address, MAC address, cookies, log files, browser fingerprints, GPS or other location data, International mobile equipment ID (IMEI), and International Mobile Subscriber Identity (IMSI).

3. Special or unique category identifiers are specific types of personal data that require additional protection. They include Biometric data, Religious beliefs, race, ethnic background, political opinion, health, sex life, sexual orientation, processing of genetic data, and trade union memberships.

It is important to note that additional categories of personal data may require protection. For instance, personal data related to a person's financial information, employment history, or criminal record may require additional safeguards.

Luckily, most US institutions understand the impact of the GDPR on their enrollment, research, and business dealings with students, faculty, and staff from the EU and UK or working there. While many organizations initially announced their intention to abandon operations in the EU, others have altered their policy and processes to minimize the risks. In 2020, Amazon announced that it would be opening a new data center in Switzerland. This move was reportedly due to concerns about the GDPR, as Switzerland is not a member of the EU (Burgess, 2021). For academia, putting a privacy statement on the website or enacting one or two more straightforward policies around GDPR are some changes to the journey toward compliance.

Learning Management Systems, Data Security, and GDPR

Academic institutions use Learning Management Systems, a software application that enables students to submit their homework and assignments and participate in discussions; for teaching faculty personnel to engage in class discussions, grade assignments, provide feedback, and post announcements; and for administrative staff to report and track student enrollments, and fulfill necessary technical tasks and documentation needs. Under the GDPR, in institutions that use an LMS, students, and staff have the right to access their data and request them to get corrected or deleted if it is inaccurate or no longer required. To make this happen, academic institutions must have necessary security provisions to prevent data breaches and unauthorized access and ensure that the use of personal data is only available to authorized personnel with a secured login. Academic Institutions with data breaches were steeply fined as they failed to take appropriate measures to protect personal data, violating GDPR. For example, the University of Greenwich was fined £120,000 (BBC, 2018); the University of East Anglia was fined £140,000 (Eastern Daily Press, 2020); Umeå University was fined $66,000.00 (The Chief I/O, 2021); and the University of Tampere in Finland was fined €50,000.

Example of How to provide GDPR Compliance in LMS:

The three well-known Learning Management Systems, Canvas, Blackboard, and Moodle, use Learning Tool Interoperability (LTI), which allows external applications (apps) and third-party systems to host content and tool within the LMS without requiring a user to log in separately on these external systems. Providing Single Sign-On (SSO) allows users to access multiple systems with a single set of credentials (Instructure, Blackboard, Moodle, May 2023). This seamless connection is a gateway to gamification, virtual experiments, interactive drag-and-drop activities, and more. This integration minimizes storing and retrieving users' data across multiple systems and ensures only authorized individuals can access an LMS. Academic Institutions and LMS providers must provide communication plans and tools so users can access their data to request correction or deletion.

Journey to Compliance Steps for Academic Institutions

Academic institutions and businesses anticipate passing federal privacy legislation worldwide and in the US, so they must proactively take steps to comply with state privacy regulations and international regulations. GDPR at an academic institution may appear to be a complex process; drawing on the seven principles of privacy by design (Cavoukian, 2012), we present some of the critical steps that can help ensure compliance:

1. **Understand and Analyze the compliance requirements** of GDPR, CCPA, and any new data privacy legislation or law.

2. **Appoint a data protection officer (DPO):** The DPO will advise the organization on data protection compliance and monitoring compliance with the GDPR and other emergent laws.

3. **Adopt industry-standard data privacy and cybersecurity compliance frameworks** to safeguard data and ensure data confidentiality.

4. **Develop and implement a plan** to gain a competitive edge in preparing for upcoming privacy laws.

5. **Develop Policies and Procedures:** review your data collection and use practices. State how and what type of personal data gets collected, how it is stored and retrieved, who within the organization can access it, and how it is protected against unauthorized access.

6. **Train Employees:** Ensure the staff has adequate knowledge, training, and responsibility for handling the data per GDPR.
   |
7. **Educate your students** about the law and how they can protect their privacy.

8. **Data Security and Encryption:** Implement encryption, access controls, and periodic backups to protect personal data from unauthorized access.

9. **Documentation of Procedures:** Stay updated with changes in EU and UK laws on GDPR to review and update processes on compliance and address any new risks or vulnerabilities. Validate for accuracy and redundancy. Instigate defensible risk mitigation processes. Obtain consent for

processing data.

10. **Obtain consent for processing data**: Consent must be freely given, specific, informed, and unambiguous.

11. **Monitor Compliance:** The institution should continuously monitor its compliance with data privacy laws. This can be done by conducting regular audits and reviewing student, faculty, and staff complaints.

Conclusion

The GDPR and UK GDPR are essential regulations for protecting personal data and privacy, and their impact on universities and other institutions is significant. Compliance with these regulations is critical to avoid fines, legal liabilities, and reputational damage. Therefore, it is crucial for all stakeholders, including leadership, faculty, staff, and students, to understand the regulations and their implications for the institution.

Overall, the GDPR has a potentially significant impact on governance structures, board composition, and many other aspects relating to board responsibility, accountability, and transparency, some of which are yet to emerge from this far-reaching regulation.

Within its jurisdiction, the European data protection policy is far-reaching and inclusive. The data protection regulation incorporates data protection and privacy regulation across sectors, generally about data uses in the whole jurisdiction. For example, banking, health, and education interests do not have separate privacy regulations, as can be the case in other economic jurisdictions, as is the case in the United States.

It is worth noting that the EDPB has not issued fines on the scale of those levied by US regulators, such as the Federal Trade Commission (FTC). However, GDPR fines are still substantial and can financially damage organizations and businesses. Although no US university has so far been penalized, institutions should be proactive and take steps to come into compliance with GDPR. There has lately been "a real hiring spree" of staff in the EU who will examine GDPR complaints, "Enforcement is coming in the next few years."(Herian, 2018).

The fact that no US higher education institution has been fined for non-compliance with any of the comprehensive consumer data privacy laws that have been enacted in California, Colorado, Connecticut, Utah, or Virginia, or the EU and UK GDPR, does not mean that these institutions are not at risk of being fined in the future. As more and more consumers become aware of their rights under these laws, there will likely be an increase in the number of complaints filed against businesses that violate these laws. As a result, US higher education institutions need to take steps to ensure compliance with these laws.

As the legal landscape becomes increasingly complex and fragmented, businesses and academic institutions must navigate the patchwork of laws independently. There is no straightforward solution. Educational institutions and companies must conduct their due diligence, determine which laws apply to them, and comply accordingly. Each existing and proposed law has different business provisions, and depending on the terminology used, these laws may apply to enterprises in various ways.

Data Protection is not a matter that will fade away anytime soon. It is an issue that will only gain significance over time. Individual rights will continue to drive compliance activities. The impact of cyber breaches on data protection cannot be ignored too. With the increasing frequency and sophistication of cyberattacks, protecting sensitive data has become a critical concern for organizations across various industries.

Breaches can lead to the exposure of private information, financial losses, damage to reputation, and legal consequences, all of which highlight the need for robust data protection measures. Therefore, businesses must implement strong security protocols and continuously monitor and update them to mitigate the risk of cyber breaches. Ensuring robust data protection measures is a top priority for businesses, organizations, and institutions, and so is compliance.

References

Bainbridge, D., & Pearce, G. (1998). The UK data protection act 1998 — data subjects' rights. *The Computer Law and Security Report, 14*(6), 401-406. https://doi.org/10.1016/S0267-3649(98)80057-5

Burgess, M. (2021). Why Amazon's £636m GDPR fine really matters. WIRED. https://www.wired.co.uk/article/amazon-gdpr-fine

Calder, A. (2018a). *EU GDPR: A pocket guide, school's edition* (1st ed.). IT Governance Publishing.

Calder, A. (2018b). *EU GDPR: A pocket guide, school's edition* (1st ed.). IT Governance Publishing.

Calder, A. (2019a). *EU GDPR & EU-U.S. privacy shield: A pocket guide*. IT Governance Publishing.

Calder, A. (2019b). *EU GDPR & EU-U.S. privacy shield: A pocket guide*. IT Governance Publishing.

Cavoukian, A. (2012). Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era. In G. Yee (Ed.), Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards (pp. 170-208). IGI Global. https://doi.org/10.4018/978-1-61350-501-4.ch007.

The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC | european data protection board. (2019, January 21).

Dixon, P. (2017). A failure to "Do no harm" -- India's aadhaar biometric ID program and its inability to protect privacy in relation to measures in europe and the U.S. *Health and Technology; Health Technol (Berl), 7*(4), 539-567. https://doi.org/10.1007/s12553-017-0202-6

Erickson, A. (2019a). Comparative analysis of the eu's gdpr and brazil's lgpd: Enforcement challenges with the lgpd. *Brooklyn Journal of International Law, 44*(2), 859.

Erickson, A. (2019b). Comparative analysis of the eu's gdpr and brazil's lgpd: Enforcement challenges with the lgpd. *Brooklyn Journal of International Law, 44*(2), 859.

Gazi, T. (2020). Data to the rescue: How humanitarian aid NGOs should collect information based on the GDPR. *Journal of International Humanitarian Action, 5*(1), 1-7. https://doi.org/10.1186/s41018-020-00078-0

GDPR and US higher education: What you need to know. https://moderncampus.com/blog/gdpr-and-higher-education.html

GDPR compliance checklist - cookie compliance - cookiebot™. (2020). Cookiebot. https://www.cookiebot.com/en/cookie-compliance/

GDPR violations lead to $66,000 fine for swedish university. (2021, January 11). *Thechief.Io*

Greenwich university fined £120,000 for data breach. (2018, May 21). *BBC News*

Hamburg commissioner fines H&M 35.3 million euro for data protection violations in service centre | european data protection board. (202, October 2). *European Data Protection Board*

Hamburg commissioner fines H&M 35.3 million euro for data protection violations in service centre | european data protection board. (2020, October 2). *European Data Protection Board*

Herian, R. (2018). Regulating disruption: Blockchain gdpr and questions of data sovereignty. *Journal of Internet Law, 22*(2), 1-16.

ICO statement: Intention to fine marriott international, inc more than £99 million under GDPR for data breach | european data protection board. (2019a, July 9). *European Data Protection Board*

ICO statement: Intention to fine marriott international, inc more than £99 million under GDPR for data breach | european data protection board. (2019b, July 9). *European Data Protection Board*

Ingley, C., & Wells, P. (2019). GDPR: Governance implications for regimes outside the EU. *Journal of Leadership, Accountability, and Ethics, 16*(1), 27-39.

Jay, R. (2000). UK data protection act 1998 - the human rights context. *International Review of Law, Computers & Technology, 14*(3), 385-395. https://doi.org/10.1080/713673366

Pearce, G., & BAINBRIDGE, D. (1998). Data protection: The UK data protection act 1998: Data subjects' rights. *The Computer Law and Security Report, 14*(6), 401-406.

Publish as LTI tool - MoodleDocs. https://docs.moodle.org/402/en/Publish_as_LTI_tool

Seventko, L. A. (2019). Gdpr: Navigating compliance as a united states bank. *North Carolina Banking Institute, 23*, 201.

Sharma, S., & Menon, P. (2020). *Data privacy and GDPR handbook* (1st ed.). John Wiley & Sons.

The swedish data protection authority imposes administrative fines on google | european data protection board. ().

The swedish data protection authority imposes administrative fine on google | european data protection board. (202, March 11). *European Data Protection Board*

Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., & Gallego-Nicasio Crespo, B. (2020). Privacy, security, legal and technology acceptance

elicited and consolidated requirements for a GDPR compliance platform. *Information and Computer Security*, *28*(4), 531-553. https://doi.org/10.1108/ICS-01-2020-0002

Voss, W. G., & Bouthinon-Dumas, H. (2021). Eu general data protection regulation sanctions in theory and in practice. *Santa Clara High-Technology Law Journal*, *37*(1), 1.

Wales Bethany. (2020, January 29). Students got £140,000 from UEA for private data leak. *Eastern Daily Press*