Natasha ANGELOSKA-GALEVSKA
Oliver BAKRESKI

UDK: 42.738:378.4(497.7)
Original research paper

PERSONAL DATA PROTECTION IN THE ACADEMIC ENVIRONMENT: REGULATIONS, CHALLENGES, AND PRACTICES

Abstract:

Ensuring the protection of personal data within universities is essential for maintaining the privacy and security of students, staff, and faculty. Universities must implement technical and organizational measures such as encryption, access control, regular staff training, and incident response plans to safeguard data.

The aim of this paper is to analyze the measures and mechanisms implemented at the Faculty of Philosophy in Skopje to ensure the protection of personal data. To obtain valid and in-depth insights, a qualitative study was conducted through semi-structured interviews with key officials and content analysis of relevant documents. In addition, to enhance scientific reliability, a quantitative survey was carried out with other stakeholders (teaching staff, administrative and technical staff, and students). The paper predominantly presents results and conclusions drawn from primary data collected through interviews, as well as secondary data obtained from the review of literature and the analysis of documents.

The findings indicate that the Faculty of Philosophy has established appropriate policies and practices for the protection of personal data of all stakeholders, thereby contributing to greater transparency and trust in institutional operations.In recent years, numerous regulatory acts have been adopted to secure various types of information. Significant security measures are in place, particularly concerning the personal data of students and employees, exam results, and other critical faculty-related information. However, further enhancements are necessary due to ongoing threats to data security.

Keywords: *Personal data, Security measures, Data protection, University*

1. Introduction

Ensuring the protection of personal data within universities is crucial for maintaining the privacy and security of students, staff, and faculty. In the Republic of Macedonia, the Law on Personal Data Protection (2020), aligned with the EU's General Data Protection Regulation (GDPR), sets the framework for these protections. Key principles include transparency, legality, purpose limitation, data minimization, accuracy, and security. Universities are obliged to implement technical and organizational measures such as encryption, access control, regular staff training, and incident response plans to safeguard data. Moreover, individuals have rights including access, rectification, erasure, restriction of processing, and data portability. These measures ensure that personal data is handled responsibly, reducing the risk of unauthorized access and breaches.Regular audits and strict compliance with legal standards are essential to maintaining trust and integrity within the academic environment.

The following textpresents the results of a comprehensive analysis of the measures and mechanisms implemented at the Faculty of Philosophy in Skopje to protect personal data, offering deeper insight into institutional practices, procedures, and challenges.

2.Strategies for strengthening the protocols for data protection at University

In today's digital age, universities handle vast amounts of sensitive data, including student records and personal information of students, staff, and faculty, financial data, as well as confidential research data and intellectual property. Ensuring the security of this data is paramount to maintaining trust, complying with legal requirements, and safeguarding academic integrity. A breach in data security not only jeopardizes the privacy of students, staff, and faculty but also has far-reaching legal, financial, and reputational implications for the institution as a whole.

Educational institutions are increasingly relying on software solutions to streamline administrative tasks, enhance teaching methodologies, and improve communication among teachers and students. Recent cyberattacks on organizations, including one that disrupted access to our institution's website for several days, have underscored the critical importance of robust data security measures. From high-profile breaches that compromised student personal information to ransomware attacks that disrupted operations, the vulnerabilities in educational systems have attracted the attention of malicious actors seeking to exploit weaknesses in software infrastructures. To address this escalating concern, educational institutions must be proactive in selecting and implementing the right software solutions that prioritize data security without compromising functionality.

Protecting sensitive personal data requires the implementation of a range of strategic and procedural measures that universities have to implement.

2.1. Basic principles for personal data protection

The following section presents the key principles that form the foundation for effective personal data protection within the academic context. These key strategies are seen as crucial and are pointed out in the relevant documents. (Solove, D.J., 2006; Solove, D.J., 2008; De Hert, P. and Gutwirth, S., 2006)

2.1.1. Transparency and legality: Personal data should be processed transparently and legally. Universities must inform data subjects about how their data will be used and the purposes of the processing.

2.1.2. Purpose of processing: Data should be collected for specific, clear and legitimate purposes and may not be further processed in a way that is not compatible with those purposes.

2.1.3. Minimality of data: Only those data that are necessary to fulfil the purpose for which they are processed are collected.

2.1.4. Accuracy and Timeliness: Data must be accurate and, if necessary, updated. Universities should take steps to ensure that inaccurate data is deleted or corrected.

2.1.5. Security and confidentiality: Universities must apply technical and organizational measures to protect personal data from unauthorized access, processing or publication.

We further analyzed relevant sources that provide a mix of policy, practice, and empirical research relevant to technical and organizational security measures in university settings

2.2. Technical and organizational measures

In this section we point out to the technical and organizational security measures undertaken at universities that can mitigate the risk of unauthorized access to sensitive information and personal data (ENISA, 2016; Kerkhove, T.V. and Charlier, N., 2021; Ifenthaler, D. and Schumacher, C., 2016, Jisc, 2018).:

2.2.1. Data encryption and anonymization: Data encryption is a fundamental security measure that involves encoding data so that it can only be accessed by authorized individuals with the correct decryption key. Universities should ensure that both data at rest (stored data) and data in transit (data being transmitted over networks) are encrypted. This helps protect sensitive information from unauthorized access, even if physical devices or communication channels are compromised.

The use of encryption and anonymization of data can significantly reduce the risk of unauthorized access. The specific types of encryption to be employed will depend on the organization's needs, the nature of the data being handled, regulatory requirements, and the technological infrastructure in place. Implementing a combination of these encryption methods will help ensure a robust and multi-layered defence against potential data breaches and unauthorized access.

Three main encryption methods that are essential to implement are encryption at rest and in transit, and end-to-end encryption:

2.2.1.1. Data at Rest Encryption: Encrypting data stored on physical devices such as servers, databases, and storage systems. This prevents unauthorized access if hardware is lost, stolen, or compromised.

2.2.1.2. Data in Transit Encryption: Encrypting data as it travels across networks, ensuring that information remains confidential and secure during transmission, particularly when accessed remotely or through cloud services.

2.2.1.3. End-to-End Encryption: Ensuring data remains encrypted from the moment it's generated until it's accessed by authorized recipients, minimizing exposure to potential interceptors.

Approach to encryption encompasses a variety of other methods that are worth implementing in the organization's security policy.

2.2.2. Access control: Limiting access to personal data only to those persons who need it to perform their work tasks. Implementing strict access controls is crucial to ensure that only authorized personnel can access sensitive data. This can be achieved through role-based access control (RBAC), where access rights are assigned based on the user's role within the university. Multi-factor authentication (MFA) adds an additional layer of security by requiring users to provide multiple forms of verification before accessing data.

2.2.3. Regular Security Audits

Conducting regular security audits helps identify vulnerabilities and ensure compliance with security policies. These audits involve thorough examination of the university's IT infrastructure, policies, and procedures to detect potential weaknesses and areas for improvement. Regular audits also help in keeping up with the latest security standards and best practices.

2.2.4. Data Backup and Recovery

Maintaining regular backups of critical data is essential to mitigate the impact of data breaches, hardware failures, or other disasters. Universities should implement a robust data backup strategy that includes both onsite and offsite backups. Additionally, having a comprehensive disaster recovery plan ensures that data can be restored promptly, minimizing downtime and data loss. Educational organizations have increasingly become targets of ransomware attacks, where cybercriminals encrypt data and demand payment for its release, which causes unaffordable interruption of performance apart from the financial threat it directly imposes. Having up-to-date backups allows institutions to recover data without yielding to extortion demands, safeguarding their finances and preserving the integrity of their information.

2.2.5. Cybersecurity Training and Awareness

Human error is a significant factor in many data breaches. Therefore, educating students, faculty, and staff about cybersecurity best practices is vital. Regular training sessions and awareness programs can help individuals recognize phishing attempts, create strong passwords, and understand the importance of protecting sensitive information.

Organizing cybersecurity training for employees and students in an educational organization is essential to create a culture of awareness, responsibility, and vigilance against cyber threats. By educating individuals about cybersecurity best practices and potential risks, the organization can significantly enhance its overall data security posture, in addition to measures implemented on the IT administration level.

An optimal approach is to organize a customized curriculum tailored to organization's unique needs (e.g. password security, email safety, safe browsing, social media risks, secure file sharing) and to choose from a variety of formats to train the users: workshops, online modules, videos, webinars, and interactive simulations, engaging different learning styles.

It is also useful to organize one-time or recurring guest lectures, inviting speakers and experts to share insights, experiences, and best practices, enriching the training content.

Finally, faculty should provide resources such as tip sheets, infographics, and reference materials that individuals can access and refer to after training.

2.2.6. Secure Network Infrastructure

A secure network infrastructure is the backbone of data security. Universities should deploy firewalls, intrusion detection and prevention systems, and secure Wi-Fi networks to protect against unauthorized access and cyberattacks. Regular updates and patches to network hardware and software are also essential to protect against vulnerabilities.

2.2.7. Compliance with Legal and Regulatory Requirements

Universities must comply with various legal and regulatory requirements related to data protection, such as the General Data Protection Regulation (GDPR) in Europe or the Family Educational Rights and Privacy Act (FERPA) in the United States. Adherence to these regulations ensures that universities handle data responsibly and avoid legal penalties. Universities in Macedonia are required to comply with national and international data protection regulations, most notably the Law on Personal Data Protection, which is harmonized with the European Union's General Data Protection Regulation (GDPR). This legal framework mandates that higher education institutions implement both technical and organizational measures to ensure the lawful, transparent, and secure processing of personal data. (Agency for Personal Data Protection (АЗЛП), 2020) Compliance not only safeguards the rights of students, staff, and researchers, but also helps universities avoid legal sanctions and reputational damage

2.2.8. Incident Response Plan

Having a rapid incident response plan in place is crucial for promptly addressing data breaches or other security incidents. This plan should outline the steps to be taken in the event of a security breach, including identifying the breach, containing the damage, notifying affected parties, and preventing future incidents. A well-prepared incident response team can significantly reduce the impact of a data breach.

3. Subjects' rights regarding personal data

Central to the framework of personal data protection is the recognition of the rights of data subjects, individuals whose personal data is collected, stored, and used. These rights are also enshrined in legal instruments such as the EU General Data Protection Regulation (GDPR) and the national Law on Personal Data Protection in North Macedonia. Further we provide an overview of the key rights afforded to data subjects, including the right to access, rectify, erase, restrict processing, and portability. Understanding and upholding these rights is essential for fostering transparency, accountability, and trust in the handling of personal data within universities.

3.1. Right of access: Students and employees have the right to know what personal data is being processed about them and for what purposes.

3.2. Right to rectification: Right to correct incorrect or incomplete data.

3.3. Right to erasure: The right to request the erasure of personal data that is processed illegally or is no longer needed.

3.4. Right to restriction of processing: Under certain conditions, the right to request restriction of the processing of their data.

3.5. Right to portability: The right to receive a copy of their personal data in a structured, frequently used and machine-readable form and to transfer it to another controller.

The application of these measures and rights helps to ensure the trust of data subjects in the educational system and protects them from potential abuses and violations of privacy.

4. Measures and documents for ensuring data security at the Faculty of Philosophy

The aim of our research was to analyze the measures and mechanisms undertaken at the Faculty of Philosophy in Skopje to ensure the protection of personal data. In order to achieve the research aim and objectives, a qualitative study was conducted through semi-structured interviews with key officials, including the Adviser for teaching and science from the Faculty's Human Resources Department, the Personal data protection officer, the Head of the Student affairs office, and three senior associates for student affairs at the Faculty of Philosophy. Furthermore, a content analysis of relevant documents was carried out, whereby the results and conclusions are drawn from primary data obtained through the interviews and secondary data collected from the literature review and document analysis. To strengthen the scientific reliability of the study, a quantitative survey was also administered among the teaching staff, administrative staff, and students as stakeholders; however, the present paper primarily focuses on the findings of the qualitative research.

Faculty of Philosophy complies with national and international data protection regulations. From the national legislation, the primary documents that guide the activities in this sphere are the Law on Personal Data Protection (2020), which entered into force in February 2020 with amendments and supplements in 2021, and the Regulation on the Security of Personal Data Processing (2020), documents fully aligned with European regulations. This legislative is implemented and supervised by the Agency for Personal Data Protection and it applies to all public and private entities, including universities.

According to the Law, faculty has core requirements, such as: to appoint a Data Protection Officer (DPO), to maintain records of data processing activities, to obtain valid consent where required, to ensure data minimization, storage limitation, and security, to enable data subjects (students and staff) to exercise their rights (access, rectification, erasure), to train staff on data protection, etc. According to the requirements, the Faculty of Philosophy - Skopje set appropriate acts and practices for the protection of personal data of all stakeholders. Safety is especially taken care of on the information connected with the data on the students, the results from the exams, the discussion on the digital platforms and other data related to the basic activity performed by the faculty.

In recent years, numerous acts have been adopted to regulate the procedures for the protection of the security of information of a different nature, such as:

4.1. PROCEDURE for physical, technical and organizational measures at Ss. Cyril and Methodius University in Skopje

4.2. RULEBOOK for the way on performing on video supervision.

4.3. PROCEDURE for management and use of passwords at The Faculty of Philosophy Skopje

4.4. PROCEDURE for management the rights on access at The Faculty of Philosophy in Skopje

4.5. CONCEPT for log records at The Faculty of Philosophy in Skopje

4.6. POLICY for internet certainty on office devices and E- mail at The Faculty of Philosophy in Skopje

4.7. PLAN for reporting, reaction and remediation on incidents to The agency for protection on the personal data

4.8. POLICY for management and engagement of managers at The Faculty of Philosophy in Skopje

4.9. POLICY of privacy at The Faculty of Philosophy in Skopje - Ss. Cyril and Methodius University in Skopje

4.10. RULEBOOK for the way on processing on the personal data of subjects engaged on projects at The Faculty of Philosophy in Skopje.

4.11. PROCEDURE for the activities of The officer for protection on the personal data

4.12. PROCEDURE for realization the rights of the subject on personal data

4.13. RULES for way on destruction of documents, as well as the method of destruction, deletion and cleaning on the media

4.14. PROCEDURE for security copy (backup) of the personal data at The Faculty of Philosophy in Skopje.

All these documents are publicly accessible on the faculty's website http://fzf.ukim.edu.mk/dataprotectiondocs/

In relation to the data, everything is collected in paper format, according to The Law for Higher education and the Statute of Ss. Cyril and Methodius University. These documents determine what data should be processed in the students' files. In the process of enrolment at the Faculty, students sign agreement for processing their personal data. At the same time, personal data are processed only in scope which is necessary for the appropriate purpose and with appropriate technical and organizational methods to protect their safety.

5. Security of the electronic system

The Faculty of Philosophy as unit of Ss. Cyril and Methodius University in Skopje processes the data on the students in digital form through electronic system called "I know", maintained by the University. In this system each employee at the faculty and each registered student can approach to information for their own activities after performed security authorization.

The e-system at Ss. Cyril and Methodius University in Skopje (UKIM), encompassing platforms like iKnow, iLearn, and Repository, incorporates several security measures to protect user data and ensure system integrity.

5.1. Security Measures in Place

5.1.1. Single Sign-On (SSO) via SEN-UKIM: UKIM employs the SEN-UKIM system, allowing users to access all electronic services with a single login. This centralized authentication enhances security by reducing password fatigue and potential entry points for unauthorized access.

5.1.2. Centralized Help Desk Support: A Help Desk facilitates the reporting and resolution of technical issues, ensuring timely responses to potential security concerns.

5.2. Considerations and Potential Vulnerabilities

Despite the benefits of the e-system, such as transparency and streamlined processes, there remains a vulnerability to hacker interference. This underscores the importance of continuous security evaluations and updates.

One of the weakest points in the security framework of the e-system at the Faculty of Philosophy at Ss. Cyril and Methodius University is the digital infrastructure, which can be characterized as modest. This vulnerability is not new, it stems from a long-standing institutional gap: the absence of dedicated IT personnel responsible for managing and maintaining the faculty's digital systems. For more than a decade, this lack of oversight has exposed the infrastructure to a range of risks, including outdated software.

Limited financial and human resources have further constrained the faculty's ability to implement modern cybersecurity protocols. Without proper staffing and investment in infrastructure, essential measures such as regular system updates, vulnerability assessments, and proactive threat detection are often neglected. This not only compromises the local systems but can also create potential entry points into broader university-wide platforms.

In the current digital landscape, where universities are increasingly reliant on integrated platforms for academic administration, learning management, and research data, such weak points pose significant risks. To address this, a strategic commitment is needed at both the faculty and university levels to prioritize cybersecurity, allocate necessary resources, and establish technical roles dedicated to maintaining the digital ecosystem.

6. Conclusion

Protecting data at a university is a complex but critical task that requires a multi-faceted approach. By implementing robust security measures, conducting regular audits, educating the university community, and ensuring compliance with legal requirements, universities can create a secure environment that protects sensitive information and maintains the trust of all stakeholders.

The findings of the research indicate that the Faculty of Philosophy has established appropriate policies and practices to protect the personal data of all stakeholders. In recent years, numerous regulatory acts have been adopted to secure various types of information, and these are publicly accessible on the faculty's website.

Our findings indicate that robust security measures are in place, particularly concerning the personal data of students and employees, exam results, and other data related to the faculty's core activities. Further regular audits and compliance with legal standards are essential to maintain trust and integrity in the academic environment.

University e-system demonstrates a commitment to security through centralized authentication and dedicated support structures. However, acknowledged vulnerabilities and infrastructural limitations in the faculty suggest areas for improvement. For users, adhering to best practices, such as using strong, unique passwords and promptly reporting suspicious activities, can further enhance personal security within the system.

BIBLIOGRAPHY:

- Закон за заштита на лични податоци (2020). Службен весник на Република Северна Македонија бр. 42 /The Law on Protection of Personal Data (2020), Official Gazette of the Republic of Macedoniano. 42.https://azlp.mk/law on personal data protectioni.pdf
- Закон за изменување и дополнување на законот за заштита на лични податоци (2021). Службен весник на Република Северна Македонија бр. 294 / The Law on Amending and Supplementing the Law on Personal Data Protection (2021). Official Gazette of the Republic of Macedoniano. 294.https://azlp.mk/law on amending the law on personal data protection.pdf
- Правилник за безбедност на обработка на личните податоци (2020). Службен весник на Република Северна Македонија бр. 122 / Rulebook on the Security of Personal Data Processing (2020). Official Gazette of the Republic of North Macedonia No. 122.
- Agency for Personal Data Protection (АЗЛП). (2020). Law on Personal Data Protection [online]. Skopje: Агенција за заштита на личните податоци. Available at: https://dzlp.mk [Accessed 21 May 2025].
- De Hert, P. and Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In: E. Claes, A. Duff and S. Gutwirth, eds. Privacy and the criminal law. Antwerp: Intersentia, pp.61–104.
- De Hert, P. and Papakonstantinou, V. (2012). The proposed data protection regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review, 28(2), pp.130–142.
- ENISA (2016). *Privacy and data protection by design – from policy to engineering*. [online] European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design [Accessed 21 May 2025].
- European Union.(2016). General Data Protection Regulation (EU) 2016/679. Official Journal of the European Union, L119, pp.1–88.
- Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, (170), pp.10–13.
- Ifenthaler, D. and Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, 64(5), pp.923–938.

- International Organization for Standardization. (2013). *ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO.
- Jisc.(2018). Protecting research data: Managing information security in higher education. [online] Available at: https://www.jisc.ac.uk/guides/protecting-research-data [Accessed 21 May 2025].
- Kerkhove, T.V. and Charlier, N. (2021). Data protection in higher education: A review of data governance policies and practices. *Journal of Higher Education Policy and Management*, 43(5), pp.521–537.
- Smith, R. (2021). Data protection compliance in higher education: A comparative study of GDPR implementation. Journal of Higher Education Policy and Management, 43(3), pp.241–257.Information for Students/e – Services (accessed May 20, 2025). https://ukim.edu.mk/en/studii/informacii-za-studentite/e-servisi/?utm_source=chatgpt.com
- Solove, D.J.(2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), pp.477–560.
- Solove, D.J. (2008). Understanding privacy. Cambridge, MA: Harvard University Press.