DOI: https://doi.org/10.31410/ITEMA.2023.365

Students' Privacy vs. Improved Learning Experience

Marija Kuštelega[1]
Renata Mekovec[2]

Received: December 22, 2023
Accepted: February 9, 2024
Published: May 28, 2024

Keywords:
Privacy compliance;
Learning experience;
Students' privacy

Abstract: *Data-driven technologies have had a significant impact on every sector of the economy. The increased use of these technologies has boosted the volume and potential value of data for individuals, corporations, and society. Many universities also gather and analyze data about their students in order to improve the learning experience. In this study, the authors examine how well universities in Croatia uphold fundamental privacy principles. An attempt was made to link ISO/IEC 29100, the GDPR and the Data Act Proposal. Six major Croatian universities' privacy compliance was examined using the multiple case study methodology. The major finding demonstrates that not all universities adhere to privacy standards to the same level, with non-compliance with the data reduction principle being particularly alarming. Because more personal information is released than is required, there is a greater chance that it may be linked to other personal information, endangering the student's privacy.*

1. INTRODUCTION

E-learning platforms have revolutionized education, enabling students to access diverse materials, start discussions, and think critically about certain topics (Pardo & Siemens, 2014). The improved learning experience with the help of information and communication technologies (ICT) has simplified tasks for educators, enabling effective and preventive monitoring (Jones & Hinchliffe, 2023). Higher education institutions are deploying learning analytics (LA) with the aim that teachers would be able to extract meaningful insights about student learning and make decisions to improve their teaching (Kaliisa et al., 2023).

Based on a national survey, learning engagement analytics is favored by 80% of 496 undergraduate students polled across the United Kingdom (Open Access Government, 2023). Nearly three-quarters of students (71%) concur that institutions should use this data to figure out what kind of additional academic support students might need. Research on the application of learning analytics shows that since 2011, when the field's awareness was brought to light, the amount of available research on the subject has grown rapidly (Ferguson et al., 2016). Learning analytics is increasingly being used to understand and improve the learning process (Ouhaichi et al., 2023) because it has a wide range of possible applications. A study that used learning analytics to analyze students' pattern recognition skills identified learning gaps that traditional assessments could not (Henkel & Belfi, 2023).

Learning analytics may be utilized to uncover learning strategies in the flipped classroom (Jovanovic et al., 2017), improve learning design activities (Rienties & Toetenel, 2016) and make interventions based on students' online learning behavior (Akçapınar & Hasnine, 2022). In a quasi-experimental study including 348 students, Ameloot et al. (2024) explored the impact of using learning analytics to boost students' autonomy and competency. The findings show that

[1] University of Zagreb, Faculty of Organization and Informatics, Pavlinska 2, 42000 Varaždin, Croatia
[2] University of Zagreb, Faculty of Organization and Informatics, Pavlinska 2, 42000 Varaždin, Croatia

adjusting teaching methods based on learning analytics reports has a beneficial impact on student satisfaction in a blended learning environment. In today's society, Zamecnik et al. (2022) emphasizes the value of a learning analytics dashboard in fostering collaborative learning. It may be used to monitor team interactions, support self-regulation, and provide teachers better insight into collaborative learning processes. As a result, by utilizing technology, we can acquire valuable insights about the students' real ability to cope with the given tasks.

The objective of learning analytics is to evaluate data from students and learning environments in order to support learning at various levels. However, the increased availability and use of sensitive and personal student data raises new privacy concerns (Jones, 2019). Understanding students' privacy concerns is the first step toward adopting effective privacy-enhancing measures in learning analytics (Mutimukwe et al., 2022). This paper aims to explore how higher education institutions manage the personal data they obtain on students. The authors present the methods of the research design as well as the examination criteria.

2. METHODOLOGY

The research utilized a case study methodology to collect concrete evidence on how universities handle student data protection. The methodology, as defined by Yin (2009), involved six key phases in order to correctly plan, design and analyze the data obtained from the case study. Figure 1 provides an overview of the methodology used to conduct the case study, outlining the key components of each executed phase.

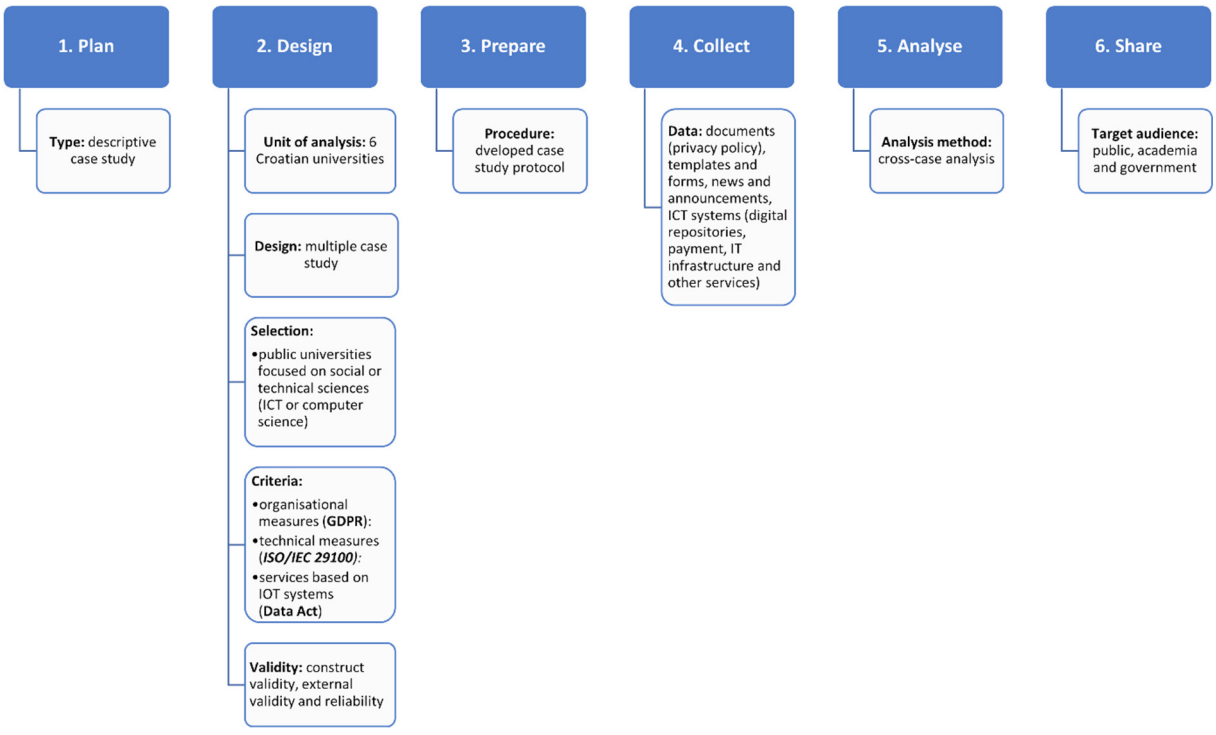

Figure 1. Methodology of the conducted case study process

Source: Own processing

Given the nature of the problem, we used a descriptive multiple case study with a sample of six major public universities in Croatia associated with ICT and related. For this purpose, a protocol was developed for implementation and data collection. The quality of the selected empirical

case study was checked depending on construct validity, external validity and reliability. Construct validity requires correct operationalization, defining attributes and criteria to measure the concept to be investigated (Saith, 2001). To satisfy the construct validity, the following activities were undertaken:

1. An operationalization was carried out in which the verification criteria were defined based on theoretically valid and generally known privacy principles.
2. Use of multiple sources of evidence (documents, templates, forms, news, announcements and ICT systems) to measure the criteria
3. The author's internal agreement on the conduct of the research (fulfilment of the requirement that the individual case meet the level of a certain criterion: no, partially, or yes).

To enhance external validity, multiple case studies were analyzed to assess predictability and similarity of results. The verification of the reliability of the study is made possible by detailed descriptions of the methodology, which enables the repetition of the data collection procedure following the criteria and theoretical construct defined by the author, which would have yielded the same results. As far as the case study studies are concerned, a theoretical framework of three criteria is being prepared consisting of criteria describing:

a. organizational measures
b. technical measures and
c. the application of modern technologies such as services based on IOT systems.

For data analysis, cross-case analysis was applied, to develop an explanation about similarities and differences in the observed unit of analysis.

3. CRITERIA

The study assesses Croatian higher education institutions' commitment to student privacy using principles from the General Data Protection Regulation (GDPR), Data Act, and ISO/IEC 29100:2011. The primary concepts and ideas that best capture the attitude toward privacy protection were extracted from each of these three important documents. Based on this, three criteria were created focusing on organizational, technical and IoT service-related measures.

The General Data Protection Regulation outlines regulations for natural persons' protection in personal data processing and free data flow, emphasizing trust building for the digital economy and ensuring easy access and control of personal data (Official Journal of the European Union, 2016). Personal data handling should be fair and legal, with clear notice of data collection, use, and clear justifications for processing. To ensure security and confidentiality, proper handling procedures for personal data must be followed, including the designation of individuals in charge of data processing and preventive measures against unauthorized access to personal data.

Criteria for organizational measures (from GDPR):

1. lawfulness, fairness and transparency,
2. purpose limitation,
3. data minimization,
4. accuracy,
5. storage limitation,
6. integrity and confidentiality.

For technical measures, ISO/IEC 29100:2011 was chosen as a privacy framework that identifies actors, roles, challenges, and references established privacy principles for information technology processing of personally identifiable data (International Organization for Standardization, 2011).

Criteria for technical measures (from ISO/IEC 29100):

1. **Consent and choice:** Participants should be informed about data processing, purpose, and rights before giving consent. Processing without consent is illegal, especially for sensitive data.
2. **Purpose legitimacy and specification:** Before data collection begins, the aim of data collection should be clearly defined, and participants should be informed of it.
3. **Collection limitation:** Data collection should be limited to only what is required for a specified purpose and is required by law.
4. **Data minimization:** Unlike the collection limitation principle, it refers to the limitation of personal data processing. This includes measures such as restricting data access, using pseudonymization or other solutions to limit the connectivity of personal data with the rightful owner, and regularly deleting data that is no longer required for a specific purpose.
5. **Use, retention and disclosure limitation**: Limiting data to only those that have a justified legitimate purpose. This principle emphasizes the importance of limiting data usage and implementing practices like storing data only for a certain period and later destroying or anonymizing them to ensure secure archiving and data protection.
6. **Accuracy and quality**: States that the data's accuracy, completeness, and up-to-date, as well as the source's dependability, should be ensured. It refers to facilitating procedures and control mechanisms for data collection, and storage, as well as checks of their quality and accuracy. This principle is especially important in cases where inaccurate and low-quality data could result in the denial of an individual's rights or benefits.
7. **Openness, transparency, and notice:** Refers to the provision of clear and easily accessible information related to the processing of personal data, including the purpose of the data collection, who processes it and how to contact them.
8. **Individual participation and access**: Refers to the right to access, review, correct, or delete data, including mechanisms that allow individuals to access only their data promptly and effectively.
9. **Accountability:** Provide privacy policies, organize training, and inform individuals about privacy attacks to mitigate potential harm and mitigate the damage caused to those who have experienced privacy violations.
10. **Information security:** Protecting personal data against security risks like unauthorized data access, use, and modification. It is necessary to perform careful selection of data processing employees and implement appropriate control systems.
11. **Privacy compliance:** Implement safeguards and systems to ensure privacy compliance, using privacy risk assessments to evaluate program and service compliance with privacy regulations.

The Data Act aims to strengthen the EU's data economy by releasing industrial data, promoting a competitive cloud market, and enabling users to access data generated by connected devices. It promotes innovation and aftermarket services while protecting trade secrets (European Parliament and Council, 2022). This criterion aimed to find out to what extent Croatian universities take advantage of the opportunities brought by the new flow of digital data.

Criteria for services based on IOT systems (from Data Act):

1. Utilization of associated goods or services,
2. Ability to gather data from related products or services.

One of the important steps for conducting a case study is the selection of documents and other materials that could be used to sufficiently address the stated research questions. Some examples of these measures include privacy policies, documents/forms for exercising rights, news published by universities, and information systems they use. Table 1 shows a more detailed description of the documents searched from the faculty's website.

Table 1. Documents, news and ICT systems for conducting case studies

Privacy policy
Information on the principles of personal data processing
Data processed (types of personal data collected)
Purpose of personal data processing and legal basis
Making personal data available (to third parties)
Information about personal data protection officers, manager and processor
Amendments to the privacy policy
Documents/forms
Templates for exercising the right to access information (request for access to information, supplement/correction of information, reuse of information)
Forms (consent, deletion of data, limitation of data collection)
News (principle of minimality)
Rector's awards
Ranking list of university scholarship winners
Information systems
Digital repository
Security of personal data (where personal data is processed, personal data retention period, etc.)
Other services and IT infrastructure (payments, instructions for using distance learning tools and digital services, etc.)

Source: Own processing

4. RESULTS

Preliminary research was conducted on the sample of three universities to determine whether the criteria and accompanying metrics were well defined. The preliminary research aimed to define the evidence available on the university's websites that can be related to established criteria in the case study. This study contributed to the development of a procedure for implementing the case study approach, ensuring that all researchers examined the same criteria in the same way.

Even on a small sample, it was assessed that there are significant differences between universities in terms of compliance with privacy principles. For example, not all universities had their privacy policies or they didn't have clearly described principles, purposes, and individuals responsible for handling data. Also, it was observed that the problem arises with the amount of data that is published, where some universities reveal more personal data about their students than they should.

5. CONCLUSION

The criteria and measures outlined in this document can be utilized for more comprehensive research on universities and faculties. The primary conclusion demonstrates that not all faculties follow the same set of privacy regulations, with alarming non-compliance with data reduction guidelines. Student privacy is compromised when more personal information is disclosed than is necessary since it is more likely to be connected to other personal information.

References

Akçapınar, G., & Hasnine, M. N. (2022). Discovering the effects of learning analytics dashboard on students' behavioral patterns using differential sequence mining. *Procedia Computer Science*, *207*, 3818-3825.

Ameloot, E., Rotsaert, T., Ameloot, T., Rienties, B., & Schellens, T. (2024). Supporting students' basic psychological needs and satisfaction in a blended learning environment through learning analytics. *Computers & Education, 209*, 104949.

European Parliament and Council. (2022). *Proposal for a Regulation of the European Parliament an of the Council on Harmonised Rules on Fair Access to an Use of Data (Data Act).* COM(2022) 68 final.

Ferguson, R., Brasher, A., Clow, D., Cooper, A., Hillaire, G., Mittelmeier, J., Rienties, B., Ullmann, T., & Vuorikari, R. (2016). *Research Evidence on the Use of Learning Analytics - Implications for Education Policy.* R. Vuorikari, J. Castaño Muñoz (Eds.). Joint Research Centre Science for Policy Report; EUR 28294 EN; https://doi.org/10.2791/955210

Henkel, M., & Belfi, L. (2023). Utilizing Learning Analytics in Radiology: A Pilot Study of an e-Learning Platform in Medical Student Education. *Academic Radiology.* https://doi.org/10.1016/j.acra.2023.05.021

International Organization for Standardization. (2011). *ISO/IEC 29100: 2011; Information technology – Security techniques– Privacy framework.* Technical report, ISO JTC 1/SC 27.

Jones, K. M. (2019). Learning analytics and higher education: a proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Educational Technology in Higher Education, 16*(1), 1-22. https://doi.org/10.1186/s41239-019-0155-0

Jones, K. M., & Hinchliffe, L. J. (2023). Ethical issues and learning analytics: Are academic library practitioners prepared?.*The Journal of Academic Librarianship, 49*(1), 102621. https://doi.org/10.1016/j.acalib.2022.102621

Jovanovic, J., Gasevic, D., Dawson, S., Pardo, A., & Mirriahi, N. (2017). Learning analytics to unveil learning strategies in a flipped classroom. *Internet and Higher Education*, *33*, 74-85. https://doi.org/10.1016/j.iheduc.2017.02.001

Kaliisa, R., Jivet, I., & Prinsloo, P. (2023). A checklist to guide the planning, designing, implementation, and evaluation of learning analytics dashboards. *International Journal of Educational Technology in Higher Education, 20*(1), 28. https://doi.org/10.1186/s41239-023-00394-6

Mutimukwe, C., Viberg, O., Oberg, L. M., & Cerratto-Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development. *British Journal of Educational Technology, 53*(4), 932-951. http://dx.doi.org/10.1111/bjet.13234

Official Journal of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC* (General Data Protection Regulation) OJ L 119/1.

Open Access Government. (2023). *National survey finds 80% of students support the use of learning engagement analytics*. Retrieved December 12, 2023, from https://www.openaccess-government.org/national-survey-finds-80-of-students-support-the-use-of-learning-engagement-analytics/170783/

Ouhaichi, H., Spikol, D., & Vogel, B. (2023). Research trends in multimodal learning analytics: A systematic mapping study. *Computers and Education: Artificial Intelligence*, 100136. https://doi.org/10.1016/j.caeai.2023.100136

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology*, 45(3), 438–450. https://doi.org/10.1111/bjet.12152

Rienties, B., & Toetenel, L. (2016). The impact of learning design on student behaviour, satisfaction and performance: A cross-institutional comparison across 151 modules. *Computers in Human Behavior*, *60*, 333-341. http://dx.doi.org/10.1016/j.chb.2016.02.074

Saith, R. (2001). Capabilities: the Concept and its Operationalisation. Oxford: Queen Elizabeth House. United States. General Accounting Office. Program Evaluation, & Methodology Division. (1992). *The evaluation synthesis* (Vol. 10). The Office.

Yin, R. K. (2009). *Case study research: Design and methods (Vol. 5)*. Sage.

Zamecnik, A., Kovanović, V., Grossmann, G., Joksimović, S., Jolliffe, G., Gibson, D., & Pardo, A. (2022). Team interactions with learning analytics dashboards. *Computers & Education*, *185*, 104514. http://dx.doi.org/10.1016/j.compedu.2022.104514