VARSTVOSLOVJE
Journal of Criminal Justice and Security
year 2026
volume 28
pp. 1–37

Implementation of the General Data Protection Regulation in Slovenian Higher Education

Mojca Tancer Verboten, Kristina Pavli, Miha Dvojmoč

Purpose:

The article examines differences and similarities in how teaching and non-teaching staff at three Slovenian public universities perceive the level of implementation of the "General Data Protection Regulation (GDPR)" („Regulation (EU) 2016/679 of the European Parliament and of the Council ... and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)" 2016) in Slovenian higher education. The analysis takes account of the adoption of the national data protection act ("Zakon o varstvu podatkov, (ZVOP-2)", 2022) being delayed until late 2022, the disruptions brought by the coronavirus disease 2019 [COVID-19] pandemic, along with insights from the universities' data protection officers [DPOs].

Design/Methods/Approach:

In May 2022, a quantitative study using a questionnaire was administered to teaching and non-teaching staff at the University of Ljubljana, the University of Maribor, and the University of Primorska. The questionnaire covered key GDPR areas, with additional structured interviews being conducted with each university's DPO.

Findings:

It was revealed that the pandemic and the legislative delay negatively impacted implementation of the GDPR. Significant differences were observed between groups of staff, notably on understanding of the legal bases, data breach procedures, and the allocation of responsibility while processing personal data.

Research Limitations/Implications:

The study refers to the higher education sector; still, the findings may also apply to other areas in the public and private sectors. The methodology could be extended to lower levels of the Slovenian education system (higher vocational, secondary, primary; also educational institutions), while similar studies performed abroad could use it to provide an international comparison. The results could also underpin more research concerning implementation of the GDPR in other public-sector organisations, and an evaluation on the level of the supervisory authority, which would permit a more comprehensive system-level assessment of compliance.

Practical implications:

The study is the first to empirically investigate implementation of the GDPR in Slovenian higher education. The importance of raising awareness among key stakeholders to ensure lawful, effective and coherent implementation of the data protection rules in practice is shown. Concrete guidance is provided for improving/upgrading existing institutional practices and helping to develop a more consistent data protection culture within the sector.

Originality/Value:

The study stresses the urgent need to improve sector-specific guidance, clarify the legal bases, and raise awareness among stakeholders in higher education. The results may be seen as valuable input for shaping national policy and institutional practices and support the development of good GDPR-implementation practices in the broader European higher education context.

Keywords: data protection, GDPR, COVID-19, Slovenia, higher education

UDC: 342.738:378

Implementacija splošne uredbe o varstvu podatkov v slovenskem visokem šolstvu

Namen prispevka:

Prispevek proučuje razlike in podobnosti v percepcijah pedagoškega in nepedagoškega osebja na treh slovenskih javnih univerzah glede stanja izvajanja Splošne uredbe o varstvu podatkov (»GDPR«, 2016) v slovenskem visokem šolstvu. Analiza upošteva zamudo pri sprejetju nacionalnega zakona o varstvu podatkov (»ZVOP-2«, 2022) do konca leta 2022, motnje, ki jih je povzročila pandemija koronavirusne bolezni 2019 (v nadaljevanju COVID-19), in ugotovitve pooblaščenih oseb za varstvo podatkov (v nadaljevanju DPO) na univerzah.

Metode:

Maja 2022 je bila izvedena kvantitativna študija z uporabo vprašalnika, ki je bil razdeljen pedagoškemu in nepedagoškemu osebju na Univerzi v Ljubljani, Univerzi v Mariboru in Univerzi na Primorskem. Raziskava je zajela ključna področja GDPR, dodatni strukturirani intervjuji pa so bili opravljeni z DPO vsake univerze.

Ugotovitve:

Ugotovitve kažejo, da sta pandemija in zakonska zamuda negativno vplivali na izvajanje GDPR. Opazne so bile znatne razlike med skupinami osebja, zlasti glede razumevanja pravnih podlag, postopkov ob kršitvi varstva podatkov in razporeditve odgovornosti pri obdelavi osebnih podatkov.

Omejitve/uporabnost raziskave:

Raziskava se osredotoča na področje visokega šolstva, vendar je njene ugotovitve mogoče prenesti tudi na druge dejavnosti javnega in zasebnega

sektorja. Možna je razširitev na nižje ravni izobraževanja v Republiki Sloveniji (višješolske, srednješolske in osnovnošolske ustanove ter vzgojne zavode) ter primerjava s tujino ob izvedbi vsebinsko sorodnih raziskav. Rezultati predstavljajo tudi izhodišče za nadaljnje raziskave implementacije z vidika drugih javnih subjektov ter evalvacijo na ravni nadzornega organa, kar omogoča celovitejšo presojo skladnosti na sistemski ravni.

Praktična uporabnost:

Gre za prvo študijo o implementaciji GDPR na področju visokega šolstva v Republiki Sloveniji. Osveščanje interesnih skupin na področju ene izmed najpomembnejših evropskih zakonodaj zadnjih let je izjemnega pomena za nadaljnjo kakovostno implementacijo (in njeno nadgradnjo) z GDPR ter za učinkovito in zakonsko skladno delo na področju visokega šolstva. Interesne skupine dobijo konkretne informacije za morebitne popravke ali nadgradnjo svojih obstoječih praks na področju varstva osebnih podatkov za dosego skladnosti z GDPR.

Izvirnost/pomembnost prispevka:

Študija poudarja nujno potrebo po izboljšanju sektorskih smernic, pojasnitvi pravnih podlag in ozaveščanju zainteresiranih strani v visokem šolstvu. Rezultati ponujajo dragocene informacije za oblikovanje nacionalne politike in institucionalnih praks ter podpirajo razvoj dobrih praks za izvajanje GDPR v širšem evropskem kontekstu visokega šolstva.

Ključne besede: varstvo podatkov, GDPR, COVID-19, Slovenija, visoko šolstvo

UDK: 342.738:378

1 INTRODUCTION

Ever since the remote education process was introduced, the Slovenian supervisory authority, namely, the Information Commissioner of the Republic of Slovenia (IC RS) (Informacijski pooblaščenec, 2021c), has detected a rise in questions about teaching and other school activities, together with the organisation of work performed by teachers using Information Technology (IT), especially during the COVID-19 crisis.

Six years after the most extensive reform of personal data protection, the authors consider the state of the GDPR's implementation in higher education in the Republic of Slovenia, with the aim to determine the situation in practice. Building on a review of the situation, the goal was to establish starting points for controllers, processors, persons authorised to process personal data, data protection officers, and (potentially) the supervisory authority, which could compel it to recognise that it is necessary to upgrade the implementation.

The authors reviewed scientific and professional works. Using the descriptive method and method of analysing the content of written sources, they analysed existing Slovenian and European legislation on the protection of personal data, as well as normative legal sources relevant to the analysis of higher education in

Slovenia. The survey method was also applied. Using two research questionnaires, they studied differences/similarities in opinions held by teaching and non-teaching staff at three public universities in the country (University of Ljubljana, University of Maribor, University of Primorska), which account for almost 90% of the country's higher education students, concerning the GDPR's implementation in higher education, also encompassing the impact of the COVID-19 pandemic.

Although the GDPR did not bring significant changes for higher education institutions with regard to their activities within the legislative framework, in some areas the criteria it provided were stricter. The failure to adopt "ZVOP-2" (2022) until late 2022 coupled with the COVID-19 pandemic produced a noticeable negative impact on implementation. In this article, we define the key areas of personal data protection, show the need for public higher education to be upgraded, especially in terms of defining the legal bases, review the adequacy of records of personal data filing systems, examine attitudes to breaches, and point to various stakeholders' responsibilities for processing personal data. Differences in opinions among teaching and non-teaching staff on the level of regulation in the field of personal data protection is another prominent issue.

While the presented research focuses on higher education, it could also be applied to other activities in both the private and public sectors. Its scope could be further extended to lower education levels in Slovenia (post-secondary, secondary, primary; also perhaps educational institutions) and for comparisons with other countries if similar studies are conducted abroad. The findings can be used to research the state of implementation from other angles, such as the perspective of a data protection officer or supervisory authority and the legislature while preparing legislative amendments.

This article presents the first study on GDPR implementation in higher education in Slovenia. Raising the awareness of interest groups about what is one of the most significant European legislative acts in recent years is essential for further high-quality implementation (and upgrading) of the GDPR together with effective and legally compliant work in higher education. Interest groups are given specific guidance as to potential corrections or refinements of their established personal data protection practices to assure that they comply with the GDPR.

The key areas of the GDPR described above were considered while we prepared questionnaires for the two-phase empirical part about certain aspects of it. Aiming to handle personal data in line with the applicable regulation in this field, universities have made efforts to adjust their procedures accordingly and assure adequate security in the processing and storage of data while also adhering to the principles of the GDPR and pursuing simplicity, practicality and flexibility for efficient and manageable work. The research paper thus aims to determine awareness of the GDPR's requirements, opinions on the success and complexity of implementing it, and challenges seen with the implementing and processing of personal data (especially in the COVID-19 pandemic) in higher education. The objectives of the main research questions were to:

- **evaluate the state of GDPR implementation in higher education in Slovenia** in defined key areas using a survey conducted among teaching

and non-teaching staff in higher education at all three Slovenian public universities;
- **inform data protection officers** at the three universities of the results and conduct structured interviews with them to ascertain their views on GDPR implementation;
- **determine the biggest challenges and risks with the current implementation of the GDPR in higher education in Slovenia**; and
- **identify aspects that require further consideration and upgrades in the implementation by the stakeholders involved.**

Following the mentioned steps, the central goal was to establish **guidelines for future GDPR implementation which may assist the stakeholders involved** (management of the respective controller, data protection officer, persons authorised for processing, processors, supervisory authority, and potentially the legislature) to raise the level of implementation. The latter has become extremely important since "ZVOP-2" (2022) entered into force in January 2023 and calls for a strong implementation base to ensure full compliance.

2 PAST STUDIES

To demonstrate the originality, value, applicability and wider implications of the presented research, we first looked at previous studies on the topic of the GDPR in higher education in Slovenia and abroad.

A review of works published in Slovenia on the subject of the GDPR, with emphasis given to scientific articles, showed that while the GDPR has been extensively researched, not much research has focused on its implementation in education.

2.1 The GDPR, implementation and education

In their article Implementacija splošne uredbe o varstvu osebnih podatkov (GDPR) z dobrimi praksami (eng. I*mplementation of the General Data Protection Regulation (GDPR) with Good Practices*"), Majerle and Markelj (2018) present implementation of the GDPR, including good practices of companies and organisations being currently applied or which could be used to achieve compliance (e.g., ISO/IEC 27001, personal data protection by default, enhanced awareness of employees, and processes for regularly testing, assessing and evaluating). Studies have also considered the GDPR's impact in particular areas in the Republic of Slovenia, for example, the impact of the GDPR on detective activity, with Primc et al. (2018) providing guidelines for revising or upgrading existing business practices to assure GDPR compliance. The even quicker pace of the development of science and resulting accessibility of technology has led to increasing digitalisation, which is found in almost all areas (public and private). The reform of personal data protection legislation concerns practically everyone, individuals and entities, both public and private alike, as Dvojmoč (2022) states in his article "Reform of European personal data protection legislative framework – Main changes". Research on the GDPR was thus also conducted in Slovenia relative to

digitalisation, for example by Hribar et al. (2018), who studied the GDPR's impact on mobile phone users or, more broadly, in connection with cyber (in)security, whereas Tancer Verboten and Dvojmoč (2022) addressed the security of personal data and information in this era of digitalisation.

For instance, implementation of the GDPR was discussed by Petra Iskra (2019) with respect to related challenges with documentation at RTV Slovenia. Since RTV is the Slovenian national public broadcaster and a public institution, Iskra's work is especially relevant to the topic. The contribution presents the core aspects of archival legislation concerning the GDPR and linked issues.

In the field of education, Petelin (2019) studied personal data protection in educational institutions under the GDPR, largely focusing on the processing of such data of children involved in educational institutions, their parents, employees of the institution, and business partners. He researched general areas (collection of personal data, contractual processing of personal data, protection of personal data, transmission of personal data to other recipients, other GDPR novelties, namely the obligation to self-report and data protection officers, and specific cases from previous years and opinions of the supervisory authority), before concluding the field has been neglected and is in need of legislative regulation.

Implementation of the GDPR in higher education has also been researched by authors in Lithuania, Portugal and Croatia. These studies are referenced for their thematic relevance as at the time of writing they are some of the few available empirical contributions dealing with GDPR implementation in higher education rather than forming part of a systematic comparative country analysis. Šidlauskas and Limba (2019) approached the GDPR from the perspective of international exchanges, chiefly in various online education programmes. If the online education student database encompasses European Union (EU) citizens, GDPR compliance plans must be put in place. In the authors' opinion, higher education institutions are not familiar with how to implement the GDPR's requirements. This led the authors to create an action plan that stresses the key aspects of the GDPR, the challenges higher education institutions face while implementing it, and the GDPR implementation model. Similar conclusions were drawn by Bessa Vilela (2019) about the Portuguese higher education system, which apparently is unprepared to fully comply with the rules contained in the regulation. In Portugal, this is not attributed to a lack of legal provisions but to non-compliance with the legislation. There are institutional peculiarities, according to Bessa Vilela (2019), that rely on the principle of transparency in higher education institutions and the concept of private data, which is not clearly defined. The article aimed to develop good practices on the national level. Sousa and Bessa Vilela (2019) argue such practices are needed because of globalisation and the mobility of the flow of (one's own) data, with ever fewer barriers and mechanisms established to maintain privacy. Higher education institutions and the community must also adapt to the natural (and ever increasing) correlation between the fields of law and technology. The lack of response and inadaptability of the GDPR to all the issues it covers causes multiple problems that have to be addressed. Sousa and Bessa Vilela (2019) state that new approaches and responses to upcoming issues are required and that a gap exists in education which must above all be filled by legislation, even though

the protection of personal data calls for a multidisciplinary approach. The ability to master different areas of knowledge is needed to understand how the various information systems function. Fernandes et al. (2022) went further by determining critical success factors with GDPR implementation in Portuguese public higher education institutions through, among others, semi-structured interviews with university employees. They listed several factors, among which they highlighted the empowerment of employees in the field of GDPR, the commitment of top management to the GDPR, GDPR being implemented with the involvement of management and employees, the development of a data protection culture, and establishment of a decentralised team for data protection.

Closer to Slovenia, in Croatia (Mekovec et al., 2020) researchers have also recognised the importance of the issue of privacy since higher education institutions and the teaching process itself largely depend on accessing, collecting and sharing the personal information of students. The processing and analysis of students' study performance is vital for improving the quality of study programmes and the study process. To ensure the realisation of all student rights and the obligation to protect privacy throughout the teaching process, among other things it is essential to perform an inventory of data and create a record of data processing activities and records of privacy breaches. With examples of good practices, it should be possible to align the privacy requirements with pedagogical standards, the learning outcomes of given study programmes, and the transparency of the evaluation process.

2.2 The GDPR, education, and COVID-19

In Slovenia, the COVID-19 pandemic's impact on the GDPR was discussed in connection with the right to personal data and its role in developing modern information technologies (Pirc Musar, 2021). Otherwise, the GDPR was mainly considered in the pandemic context from the aspect of the introduction of contact-tracing applications. Nardoni and Mali (2021) researched the rights held by data subjects associated with the "Ostani zdrav!" (eng. *Stay Healthy*) application. In general, the link between the GDPR and COVID-19 was studied in connection with the processing of sensitive personal data, and prejudice to the rights of data subjects (Rodríguez Ayuso, 2020; Becker et al., 2020; Micozzi, 2020), or with regard to the processing of employee personal data during the pandemic (Suder, 2021); only to a smaller extent was it studied explicitly in the education context. Nevertheless, all three concepts (COVID-19 pandemic, education, GDPR) were successfully connected by authors researching distance education, such as Nottingham et al. (2022) who in addition prioritised the rights held by individuals who are obliged to provide education even during a global health crisis.

COVID-19 caused an expansion in online learning by preventing participants in the education system from attending physically. While the effectiveness of digital platforms made it possible for schools to fulfil their duties to provide education, the urgency of the situation and absence of regulation led to a situation defined by insufficient consideration of the risks posed by various online learning tools to personal data and, in turn, inadequate data protection. Although the GDPR

gives a framework of regulations and rights to protect the users of such systems, tensions remained with balancing the rights of mainly younger participants (pupils) and the public need to make sure that all children are provided with an education. Nottingham et al. (2022) emphasise the need for changes in digital education practices.

In Slovenia, several options are available to address these areas on the level of higher education. The IC RS dedicated a website to the protection of personal data in the COVID-19 pandemic on which current opinions and views on the subjects of employment relationships and remote work, education, healthcare, measures, system and applications, legislative proposals, public notifications, news, the European Data Protection Board, and other EU documents were published (Informacijski pooblaščenec, n.d.-d).

In the education context, for example, the IC RS (Informacijski pooblaščenec, n.d.-d) considered the application of a particular solution for remote online examination (opinion no. 07120-1/2020/683) together with a written assessment with recording (07120-1/2020/404), the recording of lessons carried out remotely (opinion no. 07120-1/2020/649) and recording of lessons carried out via a videoconference (opinion no. 07120-1/2020/630), an opinion on the provision of personalised school e-mail addresses (opinion no. 07121-1/2020/2058) and concerning consent for access to digital classrooms (opinion no. 7121-1/2020/369), more general opinions concerning distance education in connection with particular aspects (e.g., concerning videoconferences, opinion no. 07121-1/2020/600) and the protection of personal data in general (opinion no. 07120-1/2020/274), as well as more specific opinions, such as those on the use of applications for electronic voting given that voting in person was infeasible during the pandemic (opinion no. 07120-1/2020/591).

Due to the education process being altered by the exceptional circumstances arising from measures introduced to prevent the spread of the COVID-19 virus, the supervisory authority called on the Ministry of Education, Science and Sport to define the statutory legal basis by way of uniform instructions to educational institutions. According to the supervisory authority, point 6(1)(c) of the GDPR is the only suitable legal basis for processing the personal data of participants in education conducted in online environments in exceptional circumstances. For the processing of the personal data of teaching staff, the collection, publication and storage of video recordings of lessons performed in an online learning environment should only be admissible under Article 48 of the Employment Relationships Act ("Zakon o delovnih razmerjih (ZDR-1)", 2013), provided that the processing is necessary for the exercise of rights and obligations stemming from the employment relationship or in connection with it, which the employer must be able to demonstrate (Informacijski pooblaščenec, 2020). The IC RS (Informacijski pooblaščenec, 2020) stressed that a unified approach is urgently needed when IT solutions are used in education: ideally on the level of the whole country, but at least on the level of an individual institution.

In particular, the supervisory authority drew attention to the need for security while processing personal data relative to a transfer to third countries (Informacijski pooblaščenec, 2020):

> Ensuring the security of personal data can be especially problematic when using online tools used by teachers at their discretion, potentially without prior consideration of how to assure the security of personal data. Therefore, we believe that the use of particular tools should be given proper consideration and – if possible – that the choice of tools should be approached uniformly.

This aspect is crucial for compliance with the GDPR.

Guidance materials and opinions issued by the Information Commissioner served as a suitable starting point for the preparation of internal documents by data protection officers (DPOs) at individual universities (Infocenter, n. d.; Univerza v Mariboru n.d.-a). DPOs addressed the legal bases for the lawfulness of the processing and other principles relevant to the processing of personal data that must be considered regardless of the epidemiological situation, as well as the IC RS' opinions on the recording of lectures, good practices for obtaining contact data for distance lecturing, the recording of lectures by participants, invitations to active participation by turning on audio and video devices, sending messages via the application, screen sharing, and similar activities.

At the same time, with respect to compliance with the RVT (recovered, vaccinated, tested) (slov. *PCT = preboleli, cepljeni, testirani*) conditions, the supervisory authority issued guidelines on verifying those conditions for schools.

> Schools as employers, school employees, pupils, students, parents, guardians and other users who must ensure compliance with RVT conditions by their employees and service users in accordance with the government measures imposed to curb the spread of the SARS-CoV-2 virus.

This must be done in harmony with the GDPR (Informacijski pooblaščenec, 2021b). The materials are intended for the education system in general (including higher education). This broader context of legal uncertainty was also reflected in a decision by the Constitutional Court of the Republic of Slovenia (Ustavno sodišče Republike Slovenije, 2022), which underlined the need for a clear statutory legal basis for the personal data processing measures adopted during the COVID-19 pandemic.

In light of the exceptional circumstances faced by educational institutions following the start of the pandemic, our questionnaire includes the challenges and impact of the pandemic on practical implementation of the GDPR's provisions.

3 NORMATIVE LEGAL POSITION OF PERSONAL DATA PROTECTION IN THE REPUBLIC OF SLOVENIA

Dvojmoč and Pavli (2018) analysed the impact of the reformed regulations in the field of personal data protection on national legislation in Slovenia as soon as they came into force, noting that Personal Data Protection Act ("Zakon o varstvu podatkov (ZVOP-1)", 2007) was outdated and, in some places, clashed with the new regulation, which meant subjects should follow the GDPR instead of the relevant national legislative act. Even then, the situation was described as

unacceptable. These legal deficiencies were only rectified in December 2022 with Personal Data Protection Act ("Zakon o varstvu podatkov (ZVOP-2)", (2022), entering into force on 26 January 2023.

As the applicable act until December 2022, "ZVOP-1" (2007) regulated certain substantive areas concerning personal data protection. Still, because it was adopted before the GDPR it did not fully comply with the new EU policy. Instead, it was consistent with Directive 94/46/EC, which the GDPR replaced. To achieve compliance with the GDPR on the national level, Slovenia had been on track to adopt "ZVOP-2" (2022) for the previous 4 years, as the IC RS chronologically presented in its annual report for 2020 "Waiting for ZVOP-2" (Informacijski pooblaščenec, 2021a). Of special significance is the fact, as also noted by the Ministry of Justice (Ministrstvo za pravosodje, 2022), that in general, "all EU Member States have adopted new laws for the implementation of the GDPR since this is the only way to achieve the actual (complete) implementation of the GDPR in practice".

The first draft of "ZVOP-2" (2022) was published on 23 January 2018, but since it was not adopted before the appointment of a new government, the period of legal uncertainty continued until the end of 2022.

> The new law is necessary because the GDPR has fundamentally changed the approach to the protection of personal data and because of the direct applicability of a large part of its provisions, which replaced a significant part of provisions under the currently valid "ZVOP-1" (2007), thus ensuring legal certainty in the field of personal data protection.

The above wording was included by the Ministry of Justice (Ministrstvo za pravosodje, 2022) in the Proposal for the Personal Data Protection Act submitted as part of the regular procedure for reading the proposed draft, number: 007-87/2019 of 4 July 2022, EVA 2018-2030-0045. It was hence implied that legal certainty in the area of personal data protection was inadequate and had been so for the previous 4 years. For example, the GDPR directly regulated and thereby replaced provisions on the procedure for exercising the rights of data subjects before controllers and processors and the Supervisory Authority, as well as penalty provisions. The above was supplemented accordingly in "ZVOP-2" (2022) "in parts where the GDPR provisions are insufficient from the perspective of their effect and application in our legal order. To regulate these issues in the existing act of 2004 would be utterly confusing", the Ministry of Justice concluded (Ministrstvo za pravosodje, 2022). The GDPR thus lays down the legal bases for the lawfulness of the processing of personal data (except in the part where it leaves regulation to the national legislature), which is why a significant part of the provisions contained in the currently applicable law, which are no longer adequate, must be replaced by the new ones (Ministrstvo za pravosodje, 2022).

"ZVOP-2" (2022) maintains the existing high level of protection of personal data in Slovenia and the realisation of the personal human right to the protection of personal data and, above all, takes account of information-communication and technological development in the field of personal data processing.

Certain aspects of "ZVOP-2" (2022) also add to the GDPR's provisions; for example, "ZVOP-2" (2022) regulates a few aspects of the data protection officer when they are acting on behalf of a state authority. Such officers must be employed in the public sector, and there is a possibility of jointly determining a data protection officer for several controllers, and so on.

Informacijski pooblaščenec (n.d.-c) highlights:

> "ZVOP-2" (2022) may regulate certain substantive areas, such as the use of data concerning health, biometric data or genetic data, certain procedural aspects (e.g., the procedure for imposing sanctions and legal remedies) and the relation to other areas and rights (e.g., access to public information, use of personal data for scientific and statistical purposes). However, "ZVOP-2" (2022) may not change the provisions of the GDPR, as the regulation must be directly applicable.

As such, in many of its provisions "ZVOP-2" (2022) also refers to the GDPR itself.

4 REGULATION OF HIGHER EDUCATION IN SLOVENIA RELATIVE TO PERSONAL DATA PROTECTION

At the time of the empirical study (May 2022), the applicable Higher Education Act ("Zakon o visokem šolstvu (ZViS)", 1993) defined the higher education system in the Republic of Slovenia as consisting of universities, faculties, art academies, and professional colleges. These aim to ensure the development of science, expertise and art, and to transfer knowledge from scientific, professional, research and artistic fields through the education process. Faculties, art academies, and professional colleges may be organised as part of universities or established as independent higher education institutions outside universities, states the Ministry of Higher Education, Science and Sport (Ministrstvo za visoko šolstvo, znanost in inovacije, 2023). The importance of higher education was upheld by the ministry (Ministrstvo za visoko šolstvo, znanost in inovacije, 2023) and established in adopted resolutions such as the Resolution on the National Programme of Higher Education until 2030 ("Resolucija o nacionalnem programu visokega šolstva do 2030 (ReNPVŠ30)", 2022) and the Resolution on the Slovenian Scientific Research and Innovation Strategy 2030 ("Resolucija o znanstvenoraziskovalni in inovacijski strategiji Slovenije 2030 (ReZrIS30)", 2022). Although Higher Education Act ("Zakon o visokem šolstvu (ZViS-1)", 2025) was adopted subsequently, it did not affect the institutional framework relevant to the scope and findings of our study.

The former includes data security among the measures for achieving strategic goals in digitalisation via the creation of a strategy for the digitalisation of higher education under Measure M 5.1 (»ReNPVŠ30«, 2022):

> A strategy for the digitalisation of higher education for the development of digital learning environments and study content and the development of teaching approaches and modern models of learning and teaching using Information and Communications

> Technology and digital tools and information resources for inclusive education will be developed. These are based on open principles, wide or universal accessibility, data security, inclusion, and transparency.

The latter resolution lists Measure 1.16 among those pursuing the goal of effective governance of the scientific research and innovation system (»ReZrIS30«, 2022):

> Further development of legislation and good practices in the field of protection of personal data (special categories) and their processing for the purposes of scientific research in order to effectively protect the rights of individuals, prevent abuse and ensure the availability of data necessary for research and thus a competitive research environment.

Managing personal data protection through implementation of the GDPR has thus been necessary for pursuing the objectives of the higher education system.

Universities considered various normative legal regulations to be relevant, with the Higher Education Act being crucially important ("ZViS", 1993). Explicitly referring to education, the IC RS (Informacijski pooblaščenec, 2020) notes:

> A school, as a public service provider (which, in part, also exercises public authority), shall process personal data to exercise its legal powers (for the needs of (mandatory) education) in the manner applicable to personal data processing in the public sector. In particular, Articles 6(1)(c) and 6(1)(e) of the GDPR shall apply. It is worth adding that in accordance with Articles 6(2) and 6(3) of the GDPR national legislation is applicable in the public sector – which includes higher education institutions. Therefore, it is also necessary to consider Article 9 of the Personal Data Protection Act ("Zakon o varstvu podatkov (ZVOP-1)", 2007), which provides general regulation of legal bases for the processing of personal data in the public sector. Article 9 of the "ZVOP-1" (2007) stipulates that personal data may only be processed if personal data and the processing of personal data are determined by law" (paragraph 1 of Article 9 of "ZVOP-1").

Under Article 38 of the Constitution of the Republic of Slovenia (1991 with amendments) ("Ustava Republike Slovenije", 1991), the processing of personal data was required to be provided by law. According to paragraph 4 of Article 9 of the "ZVOP-1" (2007), which still applied before "ZVOP-2" (2022) was adopted, such processing was also admissible in the case of exceptions such as where it was necessary for the exercise of the statutory competence of an educational institution and did not interfere with the legitimate interest of a natural person.

Personal data were processed in line with Chapter X of Higher Education Act ("ZViS", 1993), applicable at the time of the study, with respect to records and the protection of personal data. Under Article 81 (personal data records of students and persons enrolled in supplementary study programmes processed by higher education institutions), the personal data of students from records referred to in Article 81 shall be processed by higher education institutions for requirements

pertaining to their education and related scientific research activities, artistic and professional activities, and library activities. Pursuant to Article 81.a (personal data records of higher education providers processed by higher education institutions), the personal data of higher education providers from the records referred to in the article shall be processed by higher education institutions to establish compliance with the requirements for the performance of educational, scientific research and artistic activities and for monitoring the work and teaching obligations of higher education providers ("ZViS", 1993). Other bases for such processing are provided by the Employment Relationships Act ("Zakon o delovnih razmerjih (ZDR-1)", 2013) and the Public Employees Act ("Zakon o javnih uslužbencih (ZJU)", 2002), the Labour and Social Security Registers Act ("Zakon o evidencah na področju dela in socialne varnosti (ZEPDSV)", 2006) and other relevant legislation related to labour protection and records in the field of labour relationships (Univerza na Primorskem, n.d.-b). Under Article 81.b (personal data records kept for subsidised student accommodation requirements), higher education institutions and student halls of residence shall process the personal data from the records referred to in the article for the purpose of making decisions on students' entitlement to subsidised accommodation or on the extension of subsidised accommodation and for the needs of the ministry responsible for higher education regarding the payment of subsidies according to Article 73.b of this act. Article 81.e (eVŠ[1] records of students and graduates) states the Ministry of Education, Science and Sport shall process the personal data of students or graduates for the purpose of establishing students' rights pursuant to this act and pursuant to the act governing the exercise of rights from public funds.

Other important provisions on the processing of personal data in this chapter include Articles 81.c (records and analytical information system of higher education in Slovenia), 81.č (eVŠ records of higher education institutions), 81.d (eVŠ records of study programmes), 81.f (eVŠ records of applicants for enrolment), 81.g (eVŠ records of applicants for subsidised student accommodation), 81.h (eVŠ records of higher education providers), and 81.i (eVŠ records of private higher education teachers). Article 82 stipulates the rules for providing data for eVŠ. The personal data referred to in Articles 51.v (public records) and 51.z (register of experts) are collected, processed, kept, and transmitted for quality assurance in higher education. In accordance with »ZViS« (1993), the provisions concerning the keeping, use and storage of personal data contained in the records pursuant to "ZViS" (1993) also apply to documents serving as a basis for the collection of personal data.

In terms of the processing of personal data, other legal sources in the field of higher education, public officials, and similar are also relevant. University statutes and internal policies are essential for the activities of individual universities, while rules on the protection of personal data and potential policies in the field of information security are especially critical for the effective operation and management of personal data protection. Alongside the GDPR, other relevant regulations should also be taken into account; for example, the decree on public

1 ***eVŠ ("Evidenčni in analitski informacijski sistem visokega šolstva"*** *Republike Slovenije) is "Record and Analytical Information System of Higher Education" of the Republic of Slovenia. It is a central state information system used by the Ministry of Higher Education, universities, higher education institutions and other bodies.*

funding for higher education institutions and other institutions, the decree on the provision and re-use of public information, the decree on scientific research funding from the budget of the Republic of Slovenia, the decree on the protection of documentary and archive materials, among others, as well as sectoral rules and collective agreements. Also relevant is sectoral legislation governing specific activities and work in higher education (e.g., Institutes Act, Scientific Research and Innovation Activities Act, Professional and Academic Titles Act, Librarianship Act, Protection of Documents and Archives and Archival Institutions Act etc.) (Univerza na Primorskem, n.d.-b).

5 KEY ASPECTS OF THE GDPR

On its website, the IC RS (Informacijski pooblaščenec, n.d.-b) describes the following areas of the GDPR as essential: data protection officer, data protection impact assessment, consent, contractual processing, records of processing activities, reporting security breaches, and informing individuals of the processing of personal data.

The IC RS (Informacijski pooblaščenec, n.d.-a) defines the GDPR briefly in one of its infographics for users. It addresses breaches and the reporting thereof, rights under the GDPR and their exercising, information, the keeping of filing systems of personal data or processing activities, their security, legal bases for the collection of personal data, processing by a contractual processor with a contract and essential components of that contract, as well as processing from the perspective of joint management and, finally, transfers to third countries and international organisations.

However, unlike the guidelines on the RVT conditions, the guidelines for providing IT solutions in education (adopted quite late, in 2021) address key areas and issues related to compliance (generally and in connection with IT). Even though they do not expressly mention higher education, the principles and policies may also be applied to that level. In terms of ensuring compliance in personal data protection while using IT solutions in education, they include, on top of the basic concepts, lawfulness (purpose, legal bases, data minimisation), security and responsibility of processing, contractual processing and joint controllers, transfers to third countries and international organisations, notifications to data subjects and their rights, records of personal data processing activities, data protection impact assessment, personal data breaches, and the role of the data protection officer (Informacijski pooblaščenec, n.d.-b).

As a result, we defined the core areas of the GDPR and based the questionnaire for the empirical part on the following defined aspects: lawfulness of processing (Article 6), rights of the data subject and information to be provided to the data subject (Articles 12–22), processing (Article 28), records of processing activities (Article 30), notification of a personal data breach to the supervisory authority and to the data subject (Articles 33 and 34), data protection impact assessment (Article 35), data protection officer (Articles 37–39), and transfers of personal data to third countries or international organisations (Articles 44–50).

6 RESULTS

In May 2022, we conducted quantitative research at the three largest public universities in Slovenia (University of Ljubljana, University of Maribor, University of Primorska) using a questionnaire covering the main areas of the GDPR. The questionnaires, together with conceptual instructions for completing the survey, were sent to the management at each university to be forwarded to the human resources departments of university institutional members (i.e., university faculties, libraries, student dormitories), their management, and the teaching staff. They were then distributed among the faculties, which forwarded them to the abovementioned employees.

Our initial hypothesis was that all three universities are aware of their obligations, as shown by the adopted privacy policies and appointed data protection officers according to the universities' websites (Univerza v Ljubljani, n. d.; Univerza v Mariboru, n. d.-b; Univerza na Primorskem, n. d.-a).

The returned sample consisted of 111 completed (and valid) questionnaires, divided into the categories of teaching (43 valid questionnaires) and non-teaching staff (68 valid questionnaires). The latter included rectors, vice-rectors, secretaries-general, and assistants to secretaries-general at universities, deans, vice-deans and secretaries-general at university institutional members, administration or general services, accounting offices, student affairs offices, and libraries. The category of teaching staff focused on higher education lecturers and professors. Regarding the approach to respondents and the sampling, the results are generalised to the population of teaching and non-teaching staff employed in public higher education in Slovenia.

The respondents mostly answered the questions using a five-level Likert scale of agreement or frequency of use ("1" representing not at all clear/not at all familiar/once a year or never; "5" representing completely clear/completely familiar/daily). Some questions required a choice between the options of "yes', "no", "I do not know/I am not sure", or a choice between multiple answers. Open-ended questions were mainly provided to management.

The results are presented with the frequency of valid answers and the average scores.

Taking the two categories into account, the structure of the questionnaires is shown in Table 6.1.

Table 6.1: Structure of the questionnaires

Section	Teaching staff	Non-teaching staff
General information	YES	YES
Legal bases (Article 6)	YES	YES
Rights of data subjects and providing information and access to personal data (for data subjects) (Articles 13 and 14 + articles concerning the rights)	YES	YES
Contracts concerning the contractual processing of personal data and records of contractual processors (Article 28)	NO	YES
Record of processing activities (Article 30)	YES	YES

Personal data breaches (Article 33)	YES	YES
Data protection impact assessment (Article 35)	NO	YES
Data protection officer (Articles 37–39)	YES	YES
Transfers of personal data to third countries or international organisations (Articles 44–50)	NO	YES

In terms of content, the depth of individual sections in certain areas was adjusted to the handling of personal data. In the case of non-teaching staff, we added a special section that addressed individuals who are operationally engaged in assuring compliance with the GDPR at the rectorates and deans" offices at university institutional members (e.g., faculties etc.).

We upgraded this first phase of the empirical study by providing the data protection officers at all three public universities with the quantitative research results and by conducting structured interviews. We combined the results for staff with the data protection officers' points of view to obtain the full picture and opinion on the state of implementation. Their assessment of their dedication (in terms of time and attention) to individual sections is, on average, shown in Table 6.2.

Table 6.2: Average score of teaching and non-teaching staff combined on assessment of dedication to an individual section

Section	Teaching staff Non-teaching staff
General information	21%
Legal bases (Article 6)	13.33%
Rights of data subjects and providing information and access to personal data (for data subjects) (Articles 13 and 14 + articles concerning the rights)	13.33%
Contracts concerning the contractual processing of personal data and record of contractual processors (Article 28)	12.67%
Record of processing activities (Article 30)	13.33%
Personal data breaches (Article 33)	5%
Data protection impact assessment (Article 35)	6.67%
Data protection officer (Articles 37–39)	10.67%
Transfers of personal data to third countries or international organisations (Articles 44–50)	4%

6.1 Awareness and implementation of the legal bases

The average score given for the clarity of the legal bases under Article 6 of the GDPR is 3.5/5 for non-teaching staff, while teaching staff considered the legal bases to be less clear on average, with an average score of 3.1/5. Most teaching staff (up to 37% of them) stated that the legal bases are neither unclear nor clear, while over half the non-teaching staff indicated the legal bases are clear (48%) or completely clear (8%). The latter category contains more non-teaching staff representatives (8% compared to 5% for teaching staff).

We believe that the reason for this lies in the fact that non-teaching staff handle more personal data, handle personal data for several categories of data subjects and, in general, for a broader scope of processing purposes, while the teaching staff use personal data in a more limited manner, largely as part of their teaching activities. However, the discrepancy in the clarity of the legal bases demonstrates the need for additional training and education of teaching staff to raise their awareness. Such a step would reduce the potential risk that could flow from the lack of awareness or less awareness of the legal bases.

For both categories of staff, the most frequently used legal basis on average is point 6(1)(a) (i.e., consent), with 71% of teaching staff considering it to be the most frequently used and 56% of non-teaching staff indicating the same. On average, the least frequent legal basis used by the teaching staff is the assessment of legitimate interests, with 69% stating this, while non-teaching staff process personal data the least frequently on the legal basis of the protection of vital interests (with 39% rating it second to last and 34% rating it last) and legitimate interests (41%). The most frequently used legal bases on average for both categories of staff are presented in Table 6.1.1 below.

Legal basis	Teaching staff	Non-teaching staff
6(1)(a)	1	1
6(1)(b)	2	3
6(1)(c)	3	2
6(1)(d)	4	6
6(1)(e)	5	4
6(1)(f)	6	5

Table 6.1.1: The most frequently used legal bases ("1" indicating the most frequently used and "6" indicating the least frequently used)

As expected, the legal obligation ranks high among the non-teaching staff, with 40% of respondents ranking it second, and 18% stating that they use this legal basis the most often. We would expect legal obligation to rank first, which raises the question of whether consent is indeed used the most frequently or if the respondents only feel that this is the case given that consent requires greater effort with the forms for the collection of personal data, more interaction with the data protection officer (concerning the coordination of forms) and the like.

As regards the use of point 6(1)(f) (i.e., legitimate interest) as a legal basis, both categories largely declared they had not used it (with just 5% of teaching staff and 23% of non-teaching staff having used it). According to the teaching staff, the assessment of legitimate interests (LIA) was not conducted in a single case, whereas 46% of non-teaching staff stated that it had been carried out.

In general, data protection officers assessed the knowledge of legal bases as worse among the teaching staff. The latter use personal consent as the most common legal basis, thinking that is correct because everything in their research work is based on consent, and they transfer this opinion to project work. The non-teaching staff occasionally still think about the legal basis or the exercise of statutory authority and the contractual legal basis. Nonetheless, along with all the normative legislation presented in Chapter IV, data protection officers need

to work more on conveying information about the legal bases, preferably to both teaching and non-teaching staff.

6.2 Awareness and implementation of the rights held by data subjects and requests to provide information to data subjects

The non-teaching staff were asked about the documents they used to provide information on the processing to data subjects, while the teaching staff were asked about their awareness of documents used to inform data subjects about their rights. The results are shown in Table 6.2.1 below.

Table 6.2.1: The use (non-teaching staff) or awareness (teaching staff) of documents that provide information

Document	Teaching staff (awareness on average)	Non-teaching staff (percentage of use)
University privacy policy as published on the website	2.9/5	43%
Privacy policy in areas of personal data processing	3.0/5	48%
Privacy statement on individual applications and forms	3.0/5	81%
We do not provide information to data subjects	N/A	6%

It is alarming to note that most teaching staff rated the level of their awareness of documents as neither familiar nor unfamiliar, and especially that 6% of non-teaching staff do not provide information to data subjects. Moreover, the opinions of data protection officers are not aligned on the topic of the documents used to inform. The data protection officer at the University of Ljubljana preferred the privacy policy in areas of personal data processing and privacy statements on individual applications and forms, while the data protection officers at the other universities preferred the latter (in line with Articles 13 and 14 of the GDPR) and an approach that includes the public disclosure of records of processing activities (Article 30).

Participants were also asked to identify different rights by their legal basis. Here, the vast majority (90%) of teaching staff responded that they did not recognise them, did not know, or were unsure whether they recognised them or not (only 11% do). Awareness was higher among non-teaching staff, with the majority (53%) of staff recognising different rights according to their legal basis, with 6% not recognising them and 41% not knowing or being unsure whether they recognise them or not.

We also evaluated the teaching staff's awareness of rights, with the average awareness of individual rights being shown in Table 6.2.2. The table includes data on the frequency of exercising individual rights by data subjects, as assessed by the non-teaching staff. For all rights, the respondents mostly answered that they are exercised once a year or never, which is why we merely depict the extent to which this applies.

Right	Teaching staff (awareness, on average)	Non-teaching staff (average frequency of exercising on the scale: 1 - once a year or never, 2 - once every 6 months, 3 - once a month, 4 - once a week, 5 - daily)
Right of access held by the data subject (Article 15)	3.5/5	1.3/5 89% selected 1
Right to rectify (Article 16)	3.6/5	1.5/5 70% selected 1
Right to erase (right to be forgotten) (Article 17)	3.4/5	1.2/5 92% selected 1
Right to restrict processing (Article 18)	3.1/5	1.3/5 89% selected 1
Notification obligation regarding the rectification or erasure of personal data or restriction of processing (Article 19)	3.1/5	1.4/5 86% selected 1
Right to data portability (Article 20)	2.8/5	1.7/5 67% selected 1
Right to object	3.0/5	1.2/5 94% selected 1
Automated individual decision-making, including profiling (Article 22)	2.6/5	1.2/5 94% selected 1

Table 6.2.2: Awareness (teaching staff) and frequency of exercising (non-teaching staff) of an individual right

Generally speaking, these rights are exercised very infrequently, with individual rights mainly exercised only once a year or never. The majority of respondents estimated that the rights to data portability (6% exercise it once every 6 months, and 20% exercise it once a month) and rectification (17% exercise it once every 6 months) are exercised more often. The responses given by data protection officers confirm the results as they all agree that they only have a few cases per year (no more than four), and that their established way of exercising the rights is similar. Not one university uses an online form to cover this aspect; one typically receives requests by e-mail, while the rest obtain them from university institutional members directly by e-mail and telephone calls. They assess aspects of the availability of information (everyone uses the email format of dpo@domain for easier access) as sufficiently managed, without any need for improvements.

In general, no universal form has been established in the higher education sector for informing data subjects, as required by Articles 13 and 14. Only 2% of teaching staff and 15% of non-teaching staff believe such a form has been established. The figure indicates low awareness since, at least at the University of Maribor, a standardised form has been approved, adopted and established. The data protection officers held different opinions here since one of them did not believe in the possibility of effectively including all information given that the situations, means, and methods of processing vary, and these dictate the information provided. Two believed that it can be done provided that this form covers records with a public character and the rights guaranteed there in Articles 13 and 14. The University of Maribor uses a standardised form, as its data protection officer explained: "It is a solution that is predominantly used in

practice, but of course, there are always exceptions, so we cannot talk about the complete implementation of a standardised form. But it would work since the elements for informing are uniformly prescribed by the GDPR."

The staff are generally also poorly acquainted with deadlines set for the erasure of various types of data for a given processing activity, since on a scale from 1 "I am not at all familiar" to 5 "I am completely familiar", the teaching staff rated familiarity at 2.2/5 and non-teaching staff did so at 2.9/5. Only 38% of the former and 9% of the latter declared themselves completely familiar with the deadlines. The data protection officers explained that the universities have a classification plan accessible to employees that can be used to help determine the retention period. One problem arises in practice when employees do not take care to delete and/or destroy documentation when the retention period has expired. It was also pointed out in two cases: "Knowledge of the classification plan is poor, and a challenge is also posed by some non-life acts of universities, which determine retention periods, that cannot be implemented in practice. There is also a problem with projects where retention periods are different and cannot be unified. This is where problems arise when managing individual projects and what to do with personal data. The solution is staff training."

6.3 Awareness and implementation of the contractual processing of personal data

Only non-teaching staff were questioned about processing contracts. The majority (56%) stated that they maintain the record of contractual workers, while 11% knew that they do not maintain the record, and 33% did not know or were unsure. The opinion on the updating of records is similar, with the majority (51%) claiming that they are updated regularly, 11% that they are updated regularly, and 38% that they did not know or were not sure. Likewise, 48% of respondents were aware that an administrator had been appointed for the record of contractual processors, 13% answered that they do not have one, and 39% did not know or were unsure.

Regarding the signing of agreements on contractual processing using contractual processors required by Article 28, the prevailing opinion (62%) was that they are being concluded. It is worrying that the remaining 38% either believed they are not being concluded (5%), did not know, or were not sure about it (33%). The content of contracts was seen as appropriate by 59% of respondents, 5% believed the content does not comply with the minimum requirements, while 36% did not know or were unsure.

6.4 Awareness and implementation of provisions on the record of processing activities (Article 30)

Findings on the record of processing activities reveal such records are routinely maintained (with 63% of non-teaching staff stating that they maintain the record and only 14% replying that they do not). However, the consistency with which records are updated seems to be problematic since 44% of respondents indicated they did not know whether a record is being updated, and 18% responded that records are not updated. This means that just 38% of the non-teaching staff who

completed the questionnaire thought these records are updated. In contrast, 55% were aware that an administrator had been appointed, 15% that an administrator had not been appointed, while the remaining respondents did not know if one had been appointed.

We the teaching staff were asked whether they knew which personal data were systems are created in the scope of their teaching activities, and only one-third (33%) responded in the affirmative. The majority (60%) did not know or were not sure, and 7% did not know. Teaching staff were familiar with the following personal data filing systems which are created within the scope of teaching activities: lists of enrolled students, lists of exam applications, lists of completed exams and other study obligations, lists of violations of examination rules, lists of attendance, lists of information provided on safety in laboratory work, lists of students in individual subjects, grades obtained in tests, colloquiums, seminars, homework, exams, adjustments for certain students (corresponding decisions), number of attempts at a particular exam, records of candidates before enrolment in a doctoral study programme; some teachers were also aware of records of candidates sitting international exams, records of certificates issued concerning foreign language competencies etc., as well as records of employees, retired members, visiting professors and experts, student exchanges, internship mentors, alumni club members, and similar.

The data protection officers agreed that records (of processing and contractual processing that might even be included in the former) should be reviewed annually. This should be included in the written instructions, argued the data protection officer at the University of Ljubljana, while the data protection officer at the University of Maribor noted the need for a preliminary data protection officer check of individual institutional members of the university and the requirement that individual records be entered at the rectorate level in coordination with the data protection officer: "There is such a procedure at the University of Maribor. I would suggest the same to other universities." The steps should include: 1) a proposal to inform the data protection officer when a new record has been created; 2) an inventory of all records; and then 3) notification of a contact person when new ones are created.

6.5 Awareness and implementation of provisions on personal data breaches

The teaching staff largely (52%) stated that they had not encountered personal data breaches in their work, while 17% declared they had (the rest were unsure or did not know).

For those who had already encountered a breach, we also enquired about the nature of that breach. Results for both staff categories are presented in Table 6.5.1.

Table 6.5.1: Personal data breaches that had been encountered, in percent

Nature of the breach	Teaching staff (in percent)	Non-teaching staff (in percent)
Confidentiality (e.g., unauthorised disclosure of data, unauthorised access to data etc.)	64%	53%
Integrity (data alteration etc.)	9%	6%
Availability (e.g., data loss, data destruction etc.)	27%	41%

According to the teaching staff, the nature of the incident at issue was most often the unintentional publishing of data (21%), personal data still contained on an outdated device (13%) or displaying the wrong person's data (13%). The non-teaching staff indicated most breaches were cases of false representation ('phishing', 16%), unintentional publication (14%) or data contained on an outdated device (13%), as well as lost or open mail (11%) or unauthorised verbal disclosure of personal data (10%).

Typically, such a breach interfered with the personal data of students (with 36% of teaching staff and 44% of non-teaching staff holding such an opinion) or employees (with 18% of teaching staff and 35% of non-teaching staff holding such an opinion). The breaches concerned the following personal data: enrolment number, a student's name and surname, a student's grade, identification number, personal data in the habilitation procedure, or documentation concerning public procurement. Inspection procedures were primarily conducted in relation to the protection of the personal data of students (38%).

Non-teaching staff were mainly (49%) aware that a record of detected personal data breaches is maintained (35% did not know or were unsure, while 16% stated that no such record is maintained). However, according to 95% of respondents breaches are detected only once a year or never; 3% estimated that they happen once every 6 months, while 2% believed they happen once a month. Correspondingly, the supervisory authority (according to 98% of non-teaching staff and 100% of teaching staff) is informed of a breach once a year or never (the remaining 2% of non-teaching staff indicated they are informed once every 6 months).

Both categories asserted that most breaches occur for internal rather than malicious reasons (67% of teaching staff and 44% of non-teaching staff held this opinion). According to the respondents, the next most common causes are malicious external and unknown causes.

The non-teaching staff stated that data subjects are predominantly (84%) notified of a breach only once a year or never. The remaining 16% believed that notifications are communicated once a month.

The data protection officers all stated the universities have implemented some kind of protocol in the case of a data breach. Two of the three had included it in the internal information security policies, which unfortunately do not cover all potential breaches. "A protocol would make sense if it was properly designed from a usability point of view – it should cover all possible scenarios", stated the University of Ljubljana's data protection officer. Another issue is the possible detection of a violation, after which an individual can consult the data protection officer, determine whether it is actually a violation, and distinguish an event from

an incident. One of the three universities uses the protocols and information of the European supervisory authority and the IC RS. The University of Primorska has in place a data breach protocol according to which the first point is to inform the data protection officer and provide as much information as possible for analysis and coordination when notifying the supervisory authority. It also contains a protocol for the open inspection control of the supervisory authority. The processor must inform the data protection officer, supply as much information as possible, provide all relevant documentation obtained from the supervisory authority, and give a preliminary response and explanations so that the data protection officer can check, comment and expand on them while coordinating the response and further developments.

6.6 Awareness and implementation of provisions on data protection impact assessment

With regard to maintaining the record of data protection impact assessments (DPIAs), the prevailing opinion among the non-teaching staff was that it is not maintained; specifically, 60% believed that one is not maintained, and 40% did not know. No one responded in the affirmative to the question of whether DPIAs are maintained at their university.

Regarding the areas of impact assessment, 75% did not want to disclose the answer, 13% did not know, and the remaining 13% stated that they did not carry out any impact assessments. Fifty-eight respondents unanimously declared that they conduct the assessment no more than once a year (or never).

The role of data protection officers is mainly collaborative, giving opinions and advice. "The data protection officer's role is to review, direct the creation, and check the identified security risks. We receive quite a few evaluations for verification; we also issue written opinions on processing", explained the data protection officer at the University of Maribor. Two of the three data protection officers indicated that too few impact assessments are carried out. Sometimes even information about further procedures does not reach the data protection officers. This may be seen as a challenge during periods of distance learning when the risks of non-compliant processing of personal data increase significantly through the use of IT solutions. Measures must be taken to ensure the verification of any new processing of personal data: 1) an appropriate definition in the records of processing activities; 2), if necessary, an impact assessment; and 3) the adoption of appropriate measures and instructions for carrying out specific processing of personal data (Informacijski pooblaščenec, 2021c).

6.7 Awareness and implementation of the data protection officer's role

The teaching staff rarely reached out to the DPO, with 87% approaching them only once a year or never; 11% asking a question once every 6 months, and the remaining 3% once a month. The level of cooperation with the DPO was estimated at 2.9/5 on average. Up to 20% of them stated the level of cooperation was insufficient, 7% considered it to be sufficient, 43% chose the middle option, 20% responded that the level was high, and 10% responded that it was very high.

Given the results, the cooperation of non-teaching staff with the data protection officer is not more frequent, with 55% mainly contacting them only once a year or never, 27% once every 6 months, and the remaining 18% once every month. On average, they rated cooperation better than the teaching staff did, with a score of 4/5, and almost half (48%) of respondents considered the cooperation to be on an extremely high level.

On a scale from 1 "I completely disagree" to 5 "I completely agree", the teaching staff rated the effectiveness of the DPOs' activities and tasks with an accumulated average score of 3.3/5. Among others, they evaluated the following categories of activities and tasks of the DPO: the effectiveness of informing the controller and the employees who perform the processing and advising them of their obligations under the regulation; the effectiveness of monitoring compliance with the regulation, assigning responsibilities, raising awareness and training staff; the effectiveness of advising on impact assessment and monitoring its performance; the effectiveness of cooperation with the supervisory authority, and the effectiveness of acting as a contact point for the supervisory authority.

Non-teaching staff rated the reasons with 4/5 on average (or 3.9/5 as regards the effectiveness of advising on impact assessment and monitoring its implementation, and 4.1/5 on the effectiveness of acting as a contact person for the supervisory authority). Half the respondents gave individual reasons a score of 5/5.

The IC RS (Informacijski pooblaščenec, 2020) points out that data protection officers are precisely those persons who can "make a key contribution to ensuring compliance of the organisation in the field of personal data protection".

6.8 Awareness and implementation of provisions on the transfers of personal data to third countries or international organisations

The regulation's central relevance to the area of transfers of personal data to third countries or international organisations was similarly unfamiliar to the participants and often regarded as an area of impact assessment. Up to 90% of respondents had encountered this issue only once a year or never, 8% once every 6 months, and the remaining 2% once a week.

As concerns the implementation of the basis for transfers, exemptions for specific situations (42%) and appropriate safeguards (39%) were considered to be the most common. In 15% of cases, the basic legal basis under Articles 6 or 9 in connection with Article 28 applies to the transfer, while in the remaining 3% of cases the adequate level of protection of personal data in the country established by the European Commission and the Information Commissioner applies.

Data protection officers chiefly have an advisory and educational role while transferring data to third countries or international organisations. This includes education about needs, reviewing policies and contracts, and making recommendations for appropriate safeguards and processing practices. Only one in three believed that inspections are carried out on time and to an adequate extent. This is problematic because the aspect of transfer to third countries is also extremely important from the point of view of IT when it comes to assuring compliance in

the area of IT solutions, where the nature of the operation of information and communication technology, the use of services offered by providers such as Google, Microsoft, Zoom, among others (the servers of these providers are located in third countries) often means that personal data is transferred to third countries (Informacijski pooblaščenec, 2021c).

6.9 A special segment

In a special segment intended for individuals operationally engaged in ensuring compliance with the GDPR at the rectorates and dean's offices at the universities' institutional members, we established that higher education controllers include 11–140 personal data filing systems in the record of processing activities, with 11 being a very low number because personnel records alone require the separate management of each particular processing field. On average, they kept 32.5 records.

Regarding the content of the records of processing activities, we examined the sections shown in Table 6.9.1 below, as detailed by the indicated percentages.

Table 6.9.1: The percentage of processing activities by category

Category	Yes	No	I do not know
Title of the personal data filing system	89%	5%	5%
Type of personal data (indicating all personal data included in the filing system)	100%	0%	0%
Special categories of personal data	22%	67%	11%
Category of data subjects	82%	12%	6%
Number of data subjects	44%	44%	13%
Rights of the data subject	31%	50%	19%
Source of data	50%	38%	13%
Method of processing	69%	19%	13%
Type of processing	75%	13%	13%
Purpose of the processing of personal data	81%	6%	13%
The basis for the processing of personal data	88%	0%	13%
Period of storage of personal data	81%	6%	13%
The basis for the period of storing personal data	75%	13%	13%
Form/method of the storage of personal data	87%	0%	13%
Location of the filing system	81%	13%	6%
Organisational unit in which the filing system is formed	75%	19%	6%
A person responsible for the filing system	63%	25%	13%
Persons authorised to access	81%	13%	6%
Categories of recipients to whom the personal data have been or will be disclosed	75%	13%	13%
Access restrictions (internal)	87%	7%	7%
Recipients/categories of recipients – external transfer	69%	25%	6%

Recipients – contractual processing (subcontractor or external contractor)	44%	50%	6%
Categories of recipients in third countries or international organisations	31%	56%	13%
General description of technical and organisational security measures referred to in Article 32(1) of the GDPR	50%	25%	25%
Degree of risk of the personal data breach	44%	44%	13%
Comments	23%	62%	15%

Moreover, we were interested in the general organisation at the universities with respect to managing personal data protection (e.g., who is responsible for certain areas, how responsibilities concerning the processing of personal data are divided, whether a working group has been appointed, whether consultations are available, whether sufficient time, personnel and other resources are dedicated to the field of data protection etc.). As many as 7 out of 10 responses mainly referred to the data protection officer, who provides professional assistance on matters of data protection. He or she is also available for consultations, assistance, and advice. Prior to their appointment, one university had a working group in place to manage personal data protection. The most frequently asked questions and information are available on the intranet. In the remaining three cases, an explanation was provided that on the university level the area of personal data protection is very well regulated, as all documentation is available in SharePoint. On the level of university institutional members, the responsibility for each office (Student Affairs Office, General Affairs Office, Finance and Accounting) lies with the head of the office or persons in charge of personal data protection. Opinions concerning the GDPR are exchanged at meetings of support staff, but there is not enough time or personnel available to university members to assure high-quality management of the field. Relating to the responsibility in the case of members, one respondent maintained that it lies with the dean and the secretary or any employee who encounters personal data in their work and is obliged to comply with regulations concerning the protection of personal data.

The respondents mentioned the following main challenges with adjusting their activities to the objectives of complying with the General Data Protection Regulation and implementing it:

- **the (non-)adoption of national legal bases** (conformity with EU legislation) as the most prominent challenge given the failure to adopt the integral "ZVOP-2" (2022), which was to be signed by the government at the end of 2022;
- **the shortage of staff and time**, which especially came to the fore during the COVID-19 pandemic when a quick adaptation to the new approach and the new organisation of work was needed; because of priorities demanded by the situation, even less time could be devoted to the field of personal data protection;
- **excessive bureaucracy**, which is related to the previous point;

- doubts over **whether certain cases even concern the protection of personal data**;
- **the management and awareness of storage periods** for certain documentation;
- **the need to establish records** of processing activities and personal data filing systems; and
- **the need for additional training and education of employees**, **defining the responsibilities of the controller and processor**, and **verifying the risks** in compliance with the regulation.

Among the leading risks identified with the processing of personal data, they referred to the following:

- **the field's immensity combined with the excessive amount of manually performed tasks and the shortage of staff**, which causes a higher risk of processing errors and deficiencies, along with the related **inability to keep the obtained consents up to date**;
- being unsure **whether they have obtained the necessary consent from data subjects for all purposes of the processing**;
- being unsure **whether they have established records of processing activities for all necessary areas**, to which they added the opinion that the university should inform their members of areas in individual departments that necessarily require records of processing activities or that records should be maintained uniformly, with fewer tasks performed manually and with a higher level of transparency, the aspect of tracing that is not kept up to date given the shortage of time is also problematic, while certain units maintain a large number of filing systems due to the nature of their work, which wastes considerable time;
- being unsure **whether the notifications for informing data subjects were appropriately drafted;** and
- **printouts concerning consultations of personal data**.

Only one respondent replied to this question, stating that the protection of personal data at the University (of Maribor) is managed well.

In some cases, problems are also caused by the definition of the legal bases (in connection with storage periods). Further, we asked respondents about processing activities not sufficiently regulated in terms of legal bases, even though they would need personal data for their work, and found that they encounter the most issues in the area of processing data concerning the vaccination status of students (to carry out clinical tutorials in teaching institutions), in the area of processing activities related to vaccination generally and in the processing of data for the purposes of managing alumni clubs. The transmission of data (e.g., of students to learning databases and institutes acting as contractual processors) was frequently mentioned as an area in need of more regulation. The area of personnel records was the only one they considered to be sufficiently regulated.

The findings show that the COVID-19 pandemic made the processing of personal data considerably more difficult (45% fully agreed). In the times of the pandemic and the government ordinances on the method of verifying compliance

with the conditions of recovery, vaccination and testing in relation to the infectious disease COVID-19, the purposes of processing personal data were predominantly (according to 46% of respondents) not clear (at all), and the identification of the legal bases was difficult for some respondents (37%), while some found them clear (41%), and 23% stated that it did not have a significant impact. The majority (64%) agreed (fully) that they had been exposed to a higher risk of a breach in this time; however, half the respondents did not have the impression that in this time they dealt with more requests from the supervisory authority and more inspections. At least two of the universities surveyed had responded to a request from the supervisory authority concerning the processing in relation to the RVT.

Among the 13 respondents, 3 argued that the COVID-19 pandemic did not cause additional issues or have a particular impact on the field of personal data protection, while the remaining respondents noted that:

- there was considerable **ambiguity about the processing of personal data of students and employees in terms of permitted or unauthorised processing** (e.g., maintaining records and notifications, collection and storage of documents certifying recovery, vaccination, a negative COVID-19 test, test results, disclosing information about the employee's infection);
- switching to **the transfer of personal data by e-mail** (instead of physical transfers) **increased the risk of the processing**; and
- the pandemic generated an **additional workload for employees** and caused extra confusion in the area of personal data protection, while as a consequence of the new tasks and changed work practices, "monitoring of the GDPR was put on the back burner, and less time was unfortunately devoted to this area than before the pandemic", which primarily led to out-of-date records.

The data protection officers agreed that the biggest challenge is the ongoing monitoring of government decrees, which were changing weekly, and the uniform implementation of all the adjustments. This period rendered the area of personal data protection more difficult, and two of the three universities dealt with a supervisory authority control. One was related to the application for checking QR codes for RVT compliance, which was problematised by the IC RS, but later a similar application was introduced by the state. All teaching obligations and all elections for the leadership of the institutional members and the university also took place as normal. In the most recent case, the University of Maribor changed its rules for elections and implemented the option of online elections, in turn enabling everyone to participate, which the IC RS problematised with its control. Yet, the processing turned out to be compliant, and a DPIA was also prepared on this topic.

In conclusion, the data protection officers mostly assessed the GDPR's implementation in higher education in Slovenia as good. One even declared that it was performed above average. However, they were wary of the challenges of the new privacy act ("ZVOP-2", 2022) introduced in December 2022: "We have a lot of questions and doubts about how certain provisions will come to life in practice",

which further proves the need for a good basis while implementing the GDPR. "The challenges include the definition of a public space, the video surveillance of public areas, automatic recognition of licence plates and similar processing. The other challenges remain the same as before the GDPR". "ZVOP-2 (2022)" should accordingly not represent a major change.

7 DISCUSSION AND CONCLUSIONS

The state of implementation of the GDPR in higher education in Slovenia is good to above-average. The biggest challenges and risks (presented in the previous chapter) should be addressed for superior implementation of and improved compliance with the GDPR and "ZVOP-2" (2022). In conclusion, we wish to point out and synthesise those aspects that require further consideration and upgrades according to the study results. This may be seen as guidelines for future implementation of the GDPR and a prod in the right direction for the stakeholders involved, but especially the controllers and data protection officers in higher education, not just in Slovenia, but in the whole EU since the GDPR applies to it. Implementation of the GDPR in higher education has been researched by authors in Lithuania, Portugal and Croatia. Those studies constitute the available empirical research explicitly addressing GDPR implementation in higher education, and now also Slovenia, and different authors have found the problems to be aligned, which further shows the need for common solutions for the entire EU, noting that in Lithuania Šidlauskas and Limba (2019) found that the GDPR leaves much to interpretation and higher education institutions are unaware of how to implement its requirements. The solution, in their opinion, is to identify key aspects among the challenges faced by higher education institutions while implementing the GDPR. In Portugal, Bessa Vilela (2019) established that Portuguese higher education institutions were still not prepared to fully meet the rules imposed by the regulation.

The reviewed empirical studies indicated that the institutions were not completely in sync with the letter of the law and that understanding of the GDPR's application to certain institutional particularities had yet to be attained. The authors of these studies resolved to develop a manual of best practices applicable to all higher education institutions in combination with advisory measures issued by the Portuguese data protection authority.

Also with regard to Portugal, Fernandes et al. (2022) identified a list of 16 critical success factors in implementing the GDPR in higher education institutions, such as: empowering workers regarding the GDPR, committing top management to the GDPR, creating a culture of data protection, and establishing a decentralised team of pivots for data protection. They found universities to be following very different approaches to privacy and data protection, suggesting the need for a more universal approach.

In the rest of this chapter, we propose to implement and establish a good practice through higher education in the EU. The results of the structured interviews with the data protection officers at the three public Slovenian universities confirm that a more precise definition of legal bases is needed, preferably in the form

of improved sectoral legislation or, better still, a GDPR-compliant national law. The divergent opinions of both categories of staff on the clarity of the legal bases reveals the need for additional training and education of teaching staff to raise their awareness. This would reduce the potential risk that could arise from the lack of awareness or lower awareness of the legal bases. The role of a DPO in these cases is essential since staff education falls within their domain.

We would expect the legal obligation to rank first among the legal bases applied to the processing, which raises the question of whether consent is indeed used the most frequently or if the respondents only feel that this is the case, given that consent requires greater effort with the forms for the collection of personal data, more interaction with the DPO (concerning the coordination of forms) and the like. We believe the reason for the discrepancy in the data obtained from teaching and non-teaching staff lies is that non-teaching staff handle more personal data, personal data of several categories of data subjects and, in general, for a larger scope of processing purposes, whereas teaching staff use personal data in a more limited manner, chiefly for the performance of their pedagogical activities. In conclusion, while the educational contents of data protection officers must be adapted to each group individually, some common points are important for all.

More attention should generally be paid to the most exposed or most often detected areas of breaches, and the controller's security should be adjusted accordingly. Stronger emphasis is also needed in areas dealing with the drawing up of forms and keeping the existing documentation up to date, such as records, in connection with providing information to data subjects under Articles 13 and 14. Up to 6% of non-teaching staff in Slovenia stated that they do not inform data subjects about the processing in any way. It is generally necessary to raise awareness concerning documents for notifications to a higher level as the teaching staff were only somewhat familiar with these documents.

In Croatia, Mekovec et al. (2020) referred to implementing the performance of inventory data, the establishing of records of data processing activities and records of privacy breaches, and the outlining of the procedure to be used as an example of good practice. As concerns the content of a record, reviews of its substantive suitability are needed. While we examined more categories than those provided by the GDPR or listed by the IC RS in the sample of a record, the results of our analysis nevertheless show low awareness of the content as well as inadequately provided content. From the perspective of erasure periods, special training or work of stakeholders is called for since internal documents and classification plans have not been updated in recent years, despite the GDPR having introduced several innovations and additional requirements concerning processing.

With regard to the impact assessment, we propose that the record be kept as part of the joint record of personal data filing systems, with an additional column that specifies whether an assessment of the processing was conducted and what it concluded. Interest in this question was low in general, as was awareness of the field or record-keeping in practice, which may be attributed to the fact this field is highly technical, specialised and only mastered (and managed) by a handful of people, even though it should be familiar to all participants engaged in the

processing, which shows the aspect of awareness raising by the data protection officer is essential.

The attitude to responsibility for the processing of personal data must also be checked, and the answers should not be overly focused on the role of the data protection officer. Responsibility should be placed upon each controller (e.g., university members), their responsible persons and all individuals who encounter a minimum level of personal data in their work. Greater awareness is needed of the controller's responsibility and the contribution of each link in the processing chain, whether that refers to a non-teaching employee of a higher education controller or a teaching staff member.

Simultaneously, in order to better manage personal data protection in higher education it is necessary to focus on the revealed shortcomings of the system, which make reaching a higher standard unachievable. In that sense, we observe that in Slovenia not enough staff are available to university institutional members and not enough time is dedicated to managing the field in a satisfactory manner. It was up to the legislature of the Republic of Slovenia to regulate the legal vacuum and/or the grey area caused by the long delay in adopting "ZVOP-2" (2022), which has had a negative impact during the entire time of implementing the GDPR given that certain provisions of "ZVOP-1" (2007) were insufficient, deficient, or contrary to the GDPR. The adoption of clear legal bases (notably the regulation of sectoral legislation where the latter needs amending, e.g., concerning the transmission of students' personal data to institutions, processing of data on vaccination status etc.) would also facilitate and reduce the bureaucratic effort needed since, according to the respondents, the GDPR has produced unreasonable levels of bureaucracy. Bessa Vilela (2019) described this state as not being in sync with the letter of the law and the institutional particularities needed to reach an understanding of the GDPR's application.

The data protection officer has a substantial amount of work in the areas of advising and raising awareness of the definitions of personal data protection, managing storage periods, reviewing and providing guidance concerning the suitability of the content of records, reviewing the suitability of forms used for obtaining valid consent, and training and education of staff in general, especially in the areas the research identified to be less well known, less well managed, and where both teaching and non-teaching staff do not feel competent or educated enough to manage personal data protection. Even though not everyone is a professional lawyer capable of understanding the legal requirements of the field, everyone is ultimately required to act in harmony with the GDPR. The controllers should strive for a standardised and transparent manner of managing the field, attempt to reduce the number of manual entries and thus limit the possibility of errors, and promote the regular updating of consents, records and audit trails obtained in such a way.

Regarding the COVID-19 pandemic, which introduced additional uncertainties and, in the opinion of almost half the respondents, made the processing of personal data more difficult, greater clarity and better instructions as to certain aspects of processing would be expected in the future and in similar cases where the operation is dictated by government decrees. Therefore, controllers faced

uncertainties about the suitability of maintaining records and storage periods and informing employees of statuses (in terms of RVT and infections); the risk was also made greater by the increased volume of personal data (including special categories) being resent by e-mail, while at the same time less attention was paid to GDPR compliance as even more time and personnel were dedicated to the activities directly related to the higher education institutions' operations during the COVID-19 pandemic. These circumstances and the simultaneous failure to adopt "ZVOP-2" (2022) significantly affected the capacities and competence for tackling challenges in the area of GDPR compliance.

Through the presented research, we assessed the participants' awareness of the GDPR requirements, their opinions on the success and complexity of the implementation, and challenges seen in the implementation and processing of personal data (particularly in the time of COVID-19) in higher education. The defined key areas and the results of research conducted among teaching and non-teaching staff, coupled with data protection officers in higher education, helped clarify those aspects that require greater attention in the EU higher education sector and where the central stakeholders (management of the controller, data protection officer, persons authorised for processing, processors, supervisory authority and, potentially, the legislator) should be involved in the implementation. We propose more frequent monitoring of the level of implementation with the aim of directing the work of various stakeholders (e.g., data protection officers) and continuous improvement.

Given its broad scope (in terms of the defined areas of the GDPR) and the consideration of contemporary challenges during COVID-19, the research is also relevant for implementation in other activities in the private and public sectors, or at least for replication on lower levels of the EU education sector (in higher vocational education, upper secondary, primary, and educational institutions). This could identify additional needs for upgrading the system for managing personal data protection in education.

Comparative research involving other EU countries would help to acquire experience and ideas of good practice from abroad, whereas focusing on other aspects, for example, data protection officers or supervisory authorities, would contribute to a more comprehensive insight into management of the implementation and compliance with the GDPR in a selected EU member.

We proposed several recommendations that refer to possibilities for implementing upgrades in the field of higher education depending on the interest of key stakeholders on the part of controllers and processors, given that as the first study on implementing the GDPR in higher education in Slovenia it will raise the awareness of interest groups with respect to one of the most critical European legislative acts in recent years. Namely, the article is important for further high-quality implementation (and upgrading) of the GDPR, as well as for effective and legally compliant work in higher education across the EU.

REFERENCES

Rodríguez Ayuso, J. F. (2020). Protecció de dades personals en el context de la COVID-19: legitimació en el tractament de dades de salut per part de les administracions públiques. *Revista Catalana de Dret Public*, 137–152. https://doi.org/10.2436/rcdp.i0.2020.3449

Becker, R., Thorogood, A., Ordish, J., & Beauvais, M. J. S. (2020). COVID-19 Research: Navigating the European General Data Protection Regulation. *Journal of Medical Internet Research*, *22*(8), Article e19799. https://doi.org/10.2196/19799

Dvojmoč, M. (2022). Reform of European personal data protection legislative framework - main changes. *International Journal of Public Sector Performance Management*, *9*(4), 432–450. https://doi.org/10.1504/IJPSPM.2022.123705

Dvojmoč, M., & Pavli, K. (2018). General data protection regulation (GDPR), the data protection police directive, and the changes to national legislation in the Republic of Slovenia. In G. Meško, B. Lobnikar, K. Prislan, and R. Hacin (Eds.), *Criminal justice and security in Central and Eastern Europe: from common sense to evidence-based policy-making* (pp. 571–585). Univerza v Mariboru, Fakulteta za varnostne vede. https://press.um.si/index.php/ump/sl/catalog/view/352/321/566

Fernandes, J., Machado, C., & Amaral, L. (2022). Identifying critical success factors for the General Data Protection Regulation implementation in higher education institutions. *Digital Policy Regulation and Governance, 24*(4), 355–379. https://doi.org/10.1108/DPRG-03-2021-0041

Hribar, D., Dvojmoč, M., & Markelj, B. (2018). The Impact of the EU General Data Protection Regulation (GDPR) on Mobile Devices. *Varstvoslovje, 20*(4), 414–433. https://www.fvv.um.si/rv/arhiv/2018-4/02_Hribar_Dvojmoc_Marklej_rV_2018-4.pdf

Infocenter. (n.d.). *Izobraževanje na daljavo - Kaj je dovoljeno in kaj ne z vidika varstva osebnih podatkov pri predavanju na daljavo* [Distance Learning – What Is Allowed and What Is Not from the Perspective of Personal Data Protection in Remote Lecturing]. https://www.upr.si/files/pages/357

Informacijski pooblaščenec. (6. 4. 2020). *Mnenje št. 07120-1/2020/274: Izobraževanje na daljavo in varstvo osebnih podatkov* [Opinion No. 07120-1/2020/274: Distance Learning and Personal Data Protection]. https://www.ip-rs.si/mnenja-gdpr/6048a487a0e79

Informacijski pooblaščenec. (2021a). *Letno poročilo Informacijskega pooblaščenca za leto 2020* [Information Commissioner's Annual Report 2020]. https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/LetnoPorocilo2020_koncano.pdf

Informacijski pooblaščenec. (2021b). *Smernice o preverjanju PCT pogoja za šole* [Guidelines for Verifying Compliance with the Recovered–Vaccinated–Tested (RVT) Requirement in Schools]. https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice%20PCT%20za%20%C5%A1ole.pdf

Informacijski pooblaščenec. (2021c). *Smernice za skladno uporabo informacijskih rešitev v šolstvu* [Guidelines for the Compliant Use of Information Solutions in Education]. https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice%20za%20skladno%20uporabo%20IT%20re%C5%A1itev%20v%20%C5%A1olstvu.pdf

Informacijski pooblaščenec. (n.d.-a). *Infografike* [Infographics]. https://www.ip-rs.si/publikacije/infografike

Informacijski pooblaščenec. (n.d.-b). *Ključna področja Uredbe* [Key Areas of the Regulation]. https://www.ip-rs.si/varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/

Informacijski pooblaščenec. (n.d.-c). *Najpogostejša vprašanja in odgovori* [Frequently Asked Questions and Answers]. https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/najpogostejsa-vprasanja-in-odgovori

Informacijski pooblaščenec. (n.d.-d). *Varstvo osebnih podatkov v času epidemije koronavirusa (COVID-19)* [Personal Data Protection During the COVID-19 Pandemic]. https://www.ip-rs.si/varstvo-osebnih-podatkov/varstvo-osebnih-podatkov-v-%C4%8Dasu-epidemije-koronavirusa-covid-19

Iskra, P. (2019). Izzivi implementacije GDPR v TV-dokumentaciji RTV Slovenija [Challenges of GDPR Implementation in the TV Documentation of RTV Slovenia]. *Moderna arhivistika: časopis arhivske teorije in prakse*, *2*(1), 45–56. https://doi.org/10.54356/MA/2019/MUDW9259

Majerle, I., & Markelj, B. (2018). Implementacija splošne uredbe o varstvu osebnih podatkov (GDPR) z dobrimi praksami [Implementation of the General Data Protection Regulation (GDPR) with Good Practices]. In M. Modic, K. Prislan, I. Areh, & B. Flander (Eds.), *Zbornik povzetkov: 19. Dnevi varstvoslovja*. Univerza v Mariboru, Fakulteta za varnostne vede. https://press.um.si/index.php/ump/sl/catalog/view/339/299/536

Mekovec, R., Peras, D., & Zrinski, T. (2020). Improving Quality of Teaching Process Thought the GDPR Implementation. In L. G. Chova, A. L. Martinez, & I. C. Torres (Eds.), *INTED2019: 13th International Technology, Education and Development Conference* (pp. 5565–5574). PIATED. https://doi.org/10.21125/inted.2019.1371

Micozzi, F. P. (2020). Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito [Technologies, Data Protections and Covid-19 Emergency: Relationship Between the Possible and the Legally Permitted]. *Biolaw Journal-Rivista di Biodiritto*, *1*, 623–633. https://doi.org/10.15168/2284-4503-621

Ministrstvo za visoko šolstvo, znanost in inovacije. (12. 5. 2023). *Visokošolsko izobraževanje* [Higher Education]. https://www.gov.si/podrocja/izobrazevanje-znanost-in-sport/visokosolsko-izobrazevanje/

Ministrstvo za pravosodje. (2022). *Predlog Zakona o varstvu osebnih podatkov – redni postopek – predlog za obravnavo, številka: 007-87/2019, Ljubljana, dne 4. 7. 2022, EVA 2018-2030-0045* [Draft Personal Data Protection Act – Ordinary Legislative Procedure – Proposal for Consideration, No. 007-87/2019, Ljubljana, 4 July 2022, EVA 2018-2030-0045]. https://gradiva.vlada.si/mandat22/VLADNAGRADIVA.NSF/18a6b9887c33a0bdc12570e50034eb54/4eee7bca3cb79413c12588760023979c/$FILE/ZVOP-2_040722.docx

Nardoni, M., & Mali, F. (2021). Platformisation and Human Rights: Does use of the Slovenian #Ostanizdrav App Bypass Privacy Rights? *Teorija in praksa*, *58*, 536–554. http://dx.doi.org/10.51936/tip.58.specialissue.536-554

Nottingham, E., Stockman, C., & Burke, M. (2022). Education in a datafied world: Balancing children's rights and school's responsibilities in the age of Covid 19. *Computer Law & Security Review*, *45*, Article 105664. https://doi.org/10.1016/j.clsr.2022.105664

Petelin, D. (2019). Varstvo osebnih podatkov v vzgojno-izobraževalnih zavodih po GDPR [Personal Data Protection in Educational Institutions under the GDPR]. *Didakta*, *29*(201), 70–74.

Pirc Musar, N. (2021). Splošna uredba o varstvu podatkov - GDPR: pravica do varstva osebnih podatkov in njena vpetost v razvoj modernih informacijskih tehnologij in epidemijo covida-19 [General Data Protection Regulation – GDPR: The Right to Personal Data Protection and Its Connection to the Development of Modern Information Technologies and the COVID-19 Pandemic]. In J. Stare, & M. Pečarič (Eds.), *Znanost v javni upravi*. Univerza v Ljubljani, Fakulteta za upravo.

Primc, Ž., Šober Ažman, M., Hrastnik, P., & Dvojmoč, M. (2018). Vpliv GDPR na detektivsko dejavnost v Republiki Sloveniji [The Impact of the GDPR on Private Investigation Activities in the Republic of Slovenia]. In M. Modic, K. Prislan, I. Areh, & B. Flander (Eds.), *Zbornik povzetkov: 19. Dnevi varstvoslovja*. Univerza v Mariboru, Fakulteta za varnostne vede. https://press.um.si/index.php/ump/sl/catalog/view/339/299/536

Resolucija o nacionalnem programu visokega šolstva do 2030 (ReNPVŠ30) [*Resolution on National programme of higher education* until 2030]. (2022). *Uradni list RS*, (49/22).

Resolucija o znanstvenoraziskovalni in inovacijski strategiji Slovenije 2030 (ReZrIS30) [Resolution on the Scientific Research and Innovation Strategy of Slovenia 2030]. (2022). *Uradni list RS*, (49/22).

Šidlauskas, A., & Limba, T. (2019). General Data Protection Regulation Implementation In Higher Education Institutions. In L. G. Chova, A. L. Martinez, & I. C. Torres (Eds.), *Edulearn19: 11th International Conference on Education and New Learning Technologies* (pp. 2040–2047). IATED. https://doi.org/10.21125/edulearn.2019.0555

Sousa, M., & Bessa Vilela, N. (2019). The Impact of GDPR in the Higher Education - The Case of the 1st Cycle of Studies in Law. in L. G. Chova, A. L. Martinez, & I. C. Torres (Eds.), *Edulearn19: 11th International Conference on Education and New Learning Technologies* (pp. 8011–8014). IATED. https://doi.org/10.21125/edulearn.2019.1959

Suder, S. (2021). Processing employees' personal data during the Covid-19 pandemic. *European Labour Law Journal*, *12*(3), 322–337. https://doi.org/10.1177/2031952520978994

Tancer Verboten, M., & Dvojmoč, M. (2022, March 25–26). *Kibernetska (ne)varnost – varnost osebnih podatkov in informacij v času digitalizacije: predavanje* [Predstavitev prispevka]. [Cyber (In)Security – The Protection of Personal Data and Information in the Era of Digitalisation: Lecture [Paper presentation]]. *31. posvetovanje Medicina, pravo in družba*, Maribor, Slovenija.

Univerza na Primorskem. (n.d.-a). *Varstvo osebnih podatkov* [Personal Data Protection]. https://www.upr.si/si/o-univerzi-/predpisi-in-dokumenti-/varstvo-osebnih-podatkov/varstvo-osebnih-podatkov

Univerza na Primorskem. (n.d.-b). *Zakonodaja* [Legislation]. https://www.upr.si/si/univerza/zakonodaja

Univerza v Ljubljani. (n.d.). *Varstvo osebnih podatkov* [Personal Data Protection]. https://www.uni-lj.si/o_univerzi_v_ljubljani/varstvo_osebnih_podatkov/

Univerza v Mariboru. (n.d.-a). *Izobraževanje na daljavo - Kaj je dovoljeno in kaj ne z vidika varstva osebnih podatkov pri predavanju na daljavo* [Distance Learning – What Is Allowed and What Is Not from the Perspective of Personal Data Protection in Remote Lecturing]

Univerza v Mariboru. (n.d.-b). *Varstvo osebnih podatkov* [Personal Data Protection]. https://www.um.si/o-univerzi/dokumentno-sredisce/varstvo-osebnih-podatkov/

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov - GDPR). [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 - GDPR)]. (2016). *Uradni list Evropske Unije*, (119/1).

Ustavno sodišče Republike Slovenije. (2022). Odločba št. U-I-180/21 z dne 14. 4. 2022. https://www.us-rs.si/assets/Novice/sl_SI/46283/UI18021.pdf

Ustava Republike Slovenije (URS) [The Constitution of the Republic of Slovenia]. (1991, 1997, 2000, 2003, 2004, 2006, 2013, 2016, 2021, 2025). *Uradni list RS*, (33/91, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13, 75/16, 92/21, 98/25, 98/25).

Bessa Vilela, N. (2019). Challenges for the Implementation of the GDPR in Higher Education Institutions in Portugal. In L. G. Chova, A. L. Martinez, & I. C. Torres (Eds.), *EDULEARNn19: 11th International Conference on Education and New Learning Technologies* (pp. 1230–1234). IATED. https://doi.org/10.21125/edulearn.2019.0379

Zakon o varstvu podatkov (ZVOP-1) [Personal Data Protection Act]. (2007, 2020). *Uradni list RS*, (94/07, 177/20).

Zakon o varstvu podatkov (ZVOP-2) [Personal Data Protection Act]. (2022). *Uradni list RS*, (163/22).

Zakon o visokem šolstvu (ZViS) [Higher Education Act]. (1993, 1995, 1998, 1999, 2001, 2003, 2004, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2014, 2016, 2017, 2020, 2021, 2022, 2023,). *Uradni list RS*, (67/93, 39/95, 18/98, 35/98, 99/99, 64/01, 100/03, 63/04, 94/06, 59/07, 15/08, 64/08, 86/09, 62/10, 34/11, 40/11, 78/11, 40/12, 57/12, 109/12, 85/14, 75/16, 61/17, 65/17, 49/20, 152/20, 175/20, 13/21, 42/21, 57/21, 54/22, 100/22, 95/23, 102/23).

Zakon o visokem šolstvu (ZViS-1). [Higher Education Act]. (2025). *Uradni list RS*, (56/25).

About the Authors:

Mojca Tancer Verboten, PhD, University of Maribor, Faculty of Law, E-mail: mojca.tancer@um.si

Kristina Pavli, alumna of the University of Maribor, Faculty of Criminal Justice and Security, E-mail: kristina.pavli@student.um.si

Miha Dvojmoč, PhD, University of Maribor, Faculty of Criminal Justice and Security, E-mail: miha.dvojmoc@um.si