Implementation of the General Data Protection Regulation: Case of Higher Education Institution

Renata Mekovec*, Dijana Peras
Faculty of Organization and Informatics Varaždin, University of Zagreb, Pavlinska 2, 42000 Varaždin, Croatia.

* Corresponding author. Tel.: +385 42 390 869; email: renata.mekovec@foi.hr
Manuscript submitted October 30, 2018; accepted March 29, 2019.
doi: 10.17706/ijeeee.2020.10.1.104-113

Abstract: The aim of the General Data Protection Regulation (GDPR) is to ensure the consistency of the protection of personal data across the European Union (EU). The GDPR imposes new rules that directly affect every Member State. The purpose of this paper is to identify the practical implications of GDPR and to discuss the changes that have the most practical relevance. The situation regarding the collection, processing and use of personal data at the higher education institution (HEI) in Croatia is analyzed with aim of alignment with the provisions of the GDPR. Accordingly, the areas within the HEI that are subject to change are identified, and measures implemented in order to align to the GDPR are presented.

Key words: GDPR, HEI, personal data protection, steps of implementation.

1. Introduction

The large amount of personal data collected over the years on various locations - from public and healthcare institutions to businesses, banks, insurance companies - as well as the rapid development of electronic processing of personal data and the trend of the availability of personal data on the Internet require a normative solution to commonly regulate personal data protection [1]. As a legislative approach to keep up with increasing collection, transfer and storage of user generated personal data, the European Union adopted the General Data Protection Regulation (Regulation 2016/679, GDPR). Effective from May 2018, GDPR prompted extensive changes in established processes of numerous organizations, demanding considerable financial and human resources. A wide range of documents, policies and procedures should be created, not only to meet the explicit requirements of the GDPR, but also to ensure the tangible proof of compliance for the supervisory authority. The GDPR introduces significant changes in personal data treatment and imposes new obligations to the controllers and the processors. This paper aims to identify the changes and discuss their practical relevance on the example of the implementation at the one HEI in Croatia.

The structure of the paper consists of an introduction, followed by the state of the art of the topic. The following section presents a review on the GDPR and its implementation, identifying the most important changes imposed by the introduction of the GDPR. The results of the implementation of the GDPR at HEI are presented and discussed in section 4, followed by the conclusions drawn from the project.

2. State of the Art

One of the requirements of GDPR is that all organizations handling personal data need to be designed

with data protection in mind [2]. This principle is called data protection by design, and it is described in the first paragraph of Article 25 GDPR, which states that appropriate technical and organizational measures should be implemented in an effective manner to meet the requirements of GDPR and protect the rights of data subjects. In order to achieve this objective, the data protection principles that are laid down in Article 5 GDPR (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability) shall be implemented. There are numerous papers dealing with specific provisions of data protection by design contained by GDPR. Related approaches, interpretation of provisions and potential impact on data processing in Europe were presented in [3]. Blix *et al*. [2] have used a design science research approach to construct a framework for systematic achievement of privacy by design. They presented examples of how the data protection principles can be concretely implemented, thus explicitly tackling privacy by design in systems development. Driven by the introduction of the GDPR, Kurtz *et al*. [4] conducted a systematic literature review of Privacy by Design approach. The results have shown a surprising lack of research in this field, although GDPR explicitly emphasizes this approach. Authors of the paper [5] have presented the results of the field study regarding the use of privacy impact assessments in practice in the Netherlands, and compared them to the theory and the requirements of the GDPR. Besides legal requirements regarding data protection, social norms and expectations were taken into account. The approach used is Privacy by Design. Another methodology facilitating Privacy by Design approach was proposed by Ahmadian *et al*. [6]. This methodology supports PIA by performing model-based privacy and security analyses in the early phases of the system development. A framework to model privacy threats was also provided. In order to develop a clear understanding of the existing work and to be able to identify the differences that are invoked by the GDPR, Huth [7] designed somewhat different approach. The approach combines the use of patterns, design theory and the concept of a design theory nexus to propose a process consisting of four steps: observe and conceptualize, pattern-based theory building, solution design and application, and evaluation and learning.

Some of the most important changes proposed by the GDPR were analyzed in [8], followed by critical assessment of proposed obligations related to data security and privacy breaches, the principles of data protection by design and the data protection impact assessments (DPIA). Similar research was done in [9], where the provisions and the application of the GDPR in public and private sector were presented, and in [10], where the new European strategy on personal data protection based on GDPR initiative and its economic and social impact were addressed. Tikkinen-Piri *et al*. [11] also carried out a review of the changes introduced by GDPR. The key practical implications of the changes were identified and classified, and a framework presenting twelve aspects of these implications was developed, as well as the guidance on how to prepare for the new requirements.

A more similar research to ours was conducted by Starčević *et al*. [1], who reported on the way in which all collected personal data are processed and used by all stakeholders in the company Atlantic Grupa d.d. Zagreb. A structured procedure for implementation of the provisions of the GDPR was described in order to achieve compliance of all members of Atlantic Grupa d.d. with the provisions of the GDPR. Another research was done by Lopes and Oliveira [12], who analysed the implementation of the GDPR in health clinics in Portugal. They identified three main stages towards the implementation of the GDPR: Gather, Analyse and Implement. After the conclusion of these stages, organizations have to ensure the continuity of their compliance with the GDPR through periodical compliance audits.

The GDPR was also analyzed from the perspective of controllers and Data Protection Officers (DPOs). Mikkonen [13] wrote about the perceptions of controllers on GDPR. The research analysed the awareness and willingness to achieve compliance regarding the proposed GDPR in Finland in 2013. The results indicated that all the companies that had sophisticated analytical capabilities have already established

privacy programs, relevant processes and documentation in place the GDPR will require. Loesch [14] has clarified the role and key obligations of data controllers and data processors, as well as their relationship with data subjects. He described the cases in which companies are considered a data controller or a data processor under the GDPR. The status of the Data Protection Officer was further discussed in [10], where the option of introducing a procedure of certification in order to confirm the required competences of the DPO was explored.

It is worth to mention the research carried out by Gellert [15], who used the notions of risk and risk analysis as tools for describing and understanding risk in the GDPR. One of the main findings is that the GDPR risk is about compliance risk (i.e. the lower the compliance the higher the consequences), and that the problems of compliance and risk to the data subjects rights and freedoms are deeply interconnected. The findings of the research should be considered before conducting GAP analysis and DPIA.

3. New Concept of Data Protection in Europe

Before starting to implement the GDPR, the roles and responsibilities of the employees should be determined, for example who initiates the tasks related to personal data protection, who carries them out and who approves them. The personal data that is collected, processed and stored by organization should be defined. Furthermore, all data processing activities should be reviewed in order to identify breaches in compliance with the GDPR and associated risks. If data processing is likely to result in a high risk for natural persons, Data Protection Impact Assessment (DPIA) is required. A high level of understanding of the current level of compliance is needed. Therefore, a detailed GAP analysis should be made along with the plan to resolve the problems. Phases of the implementation are described in Table 1.

Table 1. Phases of the Implementation of GDPR

	Implementation phase
1.	appointing personal data protection officer
2.	recording personal data and databases and identifying the legal basis for data collection and processing
3.	analyzing high-risk areas through the DPIA
4.	assessing the risk through the GAP analysis and defining the organizational and technical measures in order to reduce the risk
5.	defining forms for situations in which natural persons request the exercise of a particular right and procedures describing the manner of solving the request

3.1. Data Protection Officer

Article 37 GDPR introduces the controller's and the processor's new obligation to designate a DPO in the following situations [16]: the processing is carried out by a public authority or body; the core activities of the organization consist of processing operations requiring systematic monitoring of data subjects on a large scale; the core activities of the organization consist of processing special categories of sensitive data and personal data relating to criminal convictions and offences on a large scale; or the obligation is imposed by legal acts of an EU Member State or EU law.

The controller and the processor must ensure that the DPO is properly and timely involved in all problems relating to personal data protection. They have to provide the DPO with access to personal data, processing operations and resources. The DPO is bound by secrecy or confidentiality in performance of his or her tasks. The core tasks of DPO are as follows: informing and advising the controller, the processor and employees; monitoring the compliance with the GDPR and other data protection provisions and policies;

monitoring the performance of the DPIA; and collaborating with the supervisory authority.

3.2. Data Inventory and Records of Processing Activities

Organizations should document all personal data they possess, where it came from, where it is used and with whom is it shared. According to Article 30 GDPR, each controller or processor should maintain records of processing activities under its responsibility. Records should contain the following information [16]:

1) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
2) the purposes of the processing;
3) a description of the categories of data subjects and personal data;
4) the categories of recipients to whom the personal data is disclosed;
5) where applicable, transfers of personal data to a third party;
6) where applicable, the envisaged time limits for data erasure;
7) where applicable, a description of the technical and organizational security measures.

Organizations are required to maintain a record of processing activities internally and to make it available to supervisory authorities upon request.

3.3. Data Protection Impact Assessment

With the introduction of GDPR comes a legal obligation for data controllers to conduct a Data Protection Impact Assessment (DPIA). The execution of a DPIA is prescribed under the conditions of Article 35 GDPR. "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data [16]." Examples of a high risk are listed in Paragraph 3 of Article 35 GDPR:

1) data are systematically and extensively evaluated with aim to analyze the personality of a natural person based on automated processing, including profiling, and arising decisions produce legal or similarly serious effects for natural person;
2) special categories of data or personal data relating to criminal convictions and offences are processed on a large scale; or
3) publicly accessible areas are systematically monitored on a large scale.

According to [17], a DPIA consists of three elements:

1) Preparation Stage: the controller should consider if there is a legal obligation to carry out a DPIA. The goals and scope of the assessment should be laid out, as well as the target of evaluation. All persons affected by the use should be identified and involved. The results have to be documented in the form of a report.
2) Evaluation Stage: protection goals from the perspective of the data subject whose rights are at stake should be identified. Potential attackers and motives should be identified, including at least retroactive external supervision.
3) Report and Safeguards Stage: action plan should list selected safeguards, responsibilities, deadlines, resources and criteria to measure the results. A report on the findings should be documented and evaluated by an independent third party. A review should be made in case of changes in the risk which occur as a result of data processing.

Recital 83 GDPR states that the consideration should be given to the risks that may lead to physical, material or non-material damage, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. DPIA should help organizations to estimate the data protection impact of their data

processing, to identify the risk for data users and implement appropriate measures to remedy the risks identified, including safeguards, security mechanisms and measures to protect personal data. It should also help controllers to demonstrate compliance with GDPR, but more important, it should help them to avoid the expensive potential leaks of personal data.

3.4. GAP Analysis

GAP analysis should be conducted in order to determine which components and elements of GDPR are currently in force and which should be added or altered in order to achieve the desired level of alignment with the GDPR. The analysis involves the comparison of the GDPR requirements with the processes and resources of the organization and states the human resources necessary to reduce the risks. The analysis is a useful tool to understand how the GDPR affects the organization and to review the critical, weak areas of covered domains. It should help controllers to identify the risks within the processes related to GDPR compliance and to define the resources needed to implement improvements.

3.5. Procedures and Requirements

According to the Articles 15 to 21 GDPR, the data subject has the right to obtain the access to the personal data and information about the purposes of the processing, the categories of personal data, the recipients to whom the personal data is being disclosed and the period of storage. The data subject has the right to rectification or erasure of personal data or restriction of processing of personal data. Furthermore, the data subject has to be informed about the existence of automated decision-making and the logic involved, as well as about the consequences of such processing. The right to receive and freely transmit the personal data that the data user has provided to a controller has to be ensured. The data should be provided in a structured, commonly used and machine-readable format.

In order to meet those rights, forms for which the data subjects may request the exercise of their rights have to be defined. Moreover, the procedures describing the way of solving their request have to be created.

4. Implementation of GDPR at HEI

In this section, the results of the project are presented and discussed. According to [12], the time taken to implement the GDPR depends on the complexity of business activities, the maturity of the organization, the volume and variety of the possessed personal data, the adequacy and flexibility of information systems, and over all on employers willingness to implement the GDPR. To ensure the compliance with the GDPR, HEI started to take actions within the transitional period, more than half a year before the deadline. All the activities were finished before the reinforcement of GDPR, implying the reasonableness of the implementation period.

4.1. GDPR Team and Data Protection Officer

Team for GDPR implementation was created in order to align business processes of HEI with principles and regulations of GDPR. A team of experts from different fields has been created to ensure coverage of all activities that include personal data and take place within the Faculty. Team consisted of seven people/experts for privacy, security, business processes, IT developer, IT manager, law expert and one member of HEI management.

The DPO was designated based on professional qualities, expert knowledge of data protection laws and practices, and ability to fulfil the DPO's tasks.

4.2. Data Inventory and Records of Processing Activities

The first activity of the GDPR implementation team was to identify personal data collected, processed and

stored by HEI – this step was called Data inventory process. This included personal data about students, employees, project member, conference participants, lectures from the industry etc. Although different approaches to the performance of data inventory can be applied, it is decided to proceed through the organizational units. The leaders of the organizational units were tasked with defining the personal data used by their organizational unit. Collected data were: a) Department, b) Data storage (paper, digital and more), c) Responsible person, d) Where is the Data Stored (Physical Location for Paper, CD and similar. Primary/Secondary Server, Backup Location), e) Whose and which personal data are processed and stored?, f) Who uses the data?, g) For what purpose is the data used?, h) How long does the data have to be kept and what happens to the data after that?, and i) Which regulations regulate the use of the data?

After the data inventory was carried out, duplicate checks were performed. The last step of data inventory was to produce a Records of processing activities that is mandatory according GDPR Article 30. A total of 30 processing activities have been identified, where it is obligatory to check and validate the register if a new activity or process is defined that will involve processing of personal data.

4.3. Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) is a process designed to describe the processing, assess its necessity and proportionality, and to provide assistance in managing the risks to the rights and freedoms of individuals arising from the processing of personal data, their assessment and the determination of measures for their removal. Performing the impact assessment on data protection helps controller to prove that the necessary measures have been taken to ensure compliance with the GDPR.

The assessment of the effect on data protection includes four basic steps:

1) Define and describe the context of data processing activity;
2) Analysis of controls that ensure compliance with basic principles: proportionality and necessity of processing and protection of the data owner's right;
3) Assessing privacy risks related to data security and ensuring that risks are handled fairly;
4) Documentation of the Impact Assessment.

The GDPR does not require the implementation of an assessment of the effect on data protection for any processing that may cause risks to the rights and freedoms of individuals. Performing an assessment of the effect on the protection of data is only mandatory if processing is likely to cause a high risk to individuals' rights and freedoms (Article 35, paragraph 1, as explained in Article 35, paragraph 3, and supplemented by Article 35, paragraph 4). This assessment is particularly important when introducing new data processing technology.

If it is not clear whether an assessment of the effect on data protection is required, the Data Protection Working Party under Article 29 recommends that it is still implemented, because processing managers facilitate alignment with the data protection legislation.

4.4. GAP Analysis

GAP analysis was conducted to determine which components and elements of GDPR are currently in force, and which must be added or altered. The analysis involves comparing GDPR requirements with the existing processes and resources of the HEI, thus revealing the resources, structure and security solutions that exist in the system, as well as system failures that ultimately offer solutions to the implementation plan. The GAP analysis template provides guidelines for a good quality analysis of a complete organization and an existing state of GDPR. GAP analysis covers 15 domains in accordance with the requirements of the GDPR, which are listed in Table 2.

For each of the above mentioned areas, the following criteria are defined:

1) The requirements - defined in accordance with the GDPR,

2) The Regulation (articles, recital) - cites the recital or article of the GDPR which refers to the above requirements,
3) The current compliance with HEI - consists of four questions with pre-defined responses and the answer is chosen depending on whether the condition is met and to what extent it is consistent with the requirements of the GDPR:
   a) Yes (the request is fully satisfied);
   b) No (the request or part of it is not satisfied);
   c) The conformity assessment (low, medium or high) - an assessment of the current consistency with the GDPR, each one of the three levels;
   d) Targeted compliance (low, medium or high) - an assessment of the desired compliance with the GDPR, each request is assigned one of three levels,
4) Required activities - the activities to be undertaken to ensure compliance with the GDPR are listed,
5) Responsible person/department - names of persons or departments (e.g. center, team, office, administration) - appointed for the implementation of the above activities. People are selected in accordance with the required expertise and activity requirements.
6) Resources - a measurement unit ČD is defined, which measures the human resources needed to perform the above activities. 1 ČD stands for 1 person per day (8 hours worked), whereas 2 ČD stands for 2 persons per day (16 hours worked),
7) Comments - used to input internal notes about the progress of the activity.

GAP analysis identifies the components that need to be developed. The results obtained are the first step in the implementation of the GDPR, and by systematic analysis of the annual or semi-annual basis, the progress of the implementation and compliance of the Faculty with the requirements of the GDPR can be monitored.

Table 2. Domains Covered by GAP Analysis

	Domains	GDPR requirements
1.	Internal documents	refers to the Personal Data Protection Policy
2.	Awareness	refers to the level of awareness of the requirements of the GDPR within the organization, at the level of the Management Board and the employee level
3.	Education	refers to the implementation of education on GDPR within the organization
4.	Inventory of data	refers to the definition of sources, types and formats of personal data that are collected and how to deal with such data
5.	Personal Data Access	refers to processes for managing requests for access to personal data
6.	Data Protection Principles	refers to the principles defined by the GDPR
7.	Privacy Notice	refers to defining the status associated with the existence and use of the Privacy Notice
8.	Sensitive data	refers to special categories of data and the definition of special procedures for such data (e.g. medical records)
9.	Rights of the respondent	refers to the rights of the respondent defined by the GDPR (information, access to data, modification or deletion of data, processing limitation, objection, data transmission)
10.	Management obligations	refers to taking appropriate technical and organizational measures for the purpose of data protection, keeping records of processing activities, assessing the effect on data protection and other activities related to responsible management of personal data
11.	Consent	refers to the requests for consents defined by the GDPR
12.	Personal Data Protection Officer	refers to the appointment of a Personal Data Protection Officer within the organization

13.	Transferring data to third parties	refers to the definition of guidelines for sharing data with third parties
14.	Personal data breaches	refers to the procedure for notifying incidents
15.	Monitoring of external events	refers to the identification of valid privacy regulatory requirements

4.5. Procedures and Requirements

In order to meet the rights of the data subject defined in the GDPR Articles 15 to 22, forms are defined for which the respondents may request the exercise of a particular right, as well as procedures describing the manner of solving the request. Procedures are thus defined for:

1) resolving a request for deletion
2) resolving access request
3) resolving the request for correction
4) resolving the processing limitation request
5) resolving data transfer requirements
6) resolving an objection request
7) handling medical documents
8) deferring student obligations
9) data processing for direct marketing purposes
10) resolving an automated decision not to apply
11) resolving privilege attempts
12) data processing for scientific research purposes

The HEI is aware that the security of personal data is very important therefore the privacy of personal data is taken very seriously. The Privacy Policy is introduced for data subject to know what information is stored and how they are used. The Privacy Policy covering the fundamental principles and practices of data protection is posted on the HEI website.

5. Conclusion

In this paper a detailed theoretical elaboration of the GDPR with regard to the processing of personal data is presented. Furthermore, transparent presentation of the current state in this area on the example of HEI was given. Concrete activities and achieved outputs from the implementation of the GDPR were described. The following activities were described in detail:

1) the roles and responsibilities of the employees were determined, the team for GDPR implementation was created and the DPO was designated;
2) the personal data that is collected, processed and stored by the faculty was defined. After the data inventory was carried out, duplicate checks were performed and a Records of processing activities was produced. All data processing activities were reviewed in order to identify breaches in compliance with the GDPR and associated risks;
3) the Data Protection Impact Assessment (DPIA); and
4) the GAP analysis were carried out in order to prove that the necessary measures have been taken to ensure compliance with the GDPR.
5) the GDPR implementation implies the definition of procedures and creation of forms.

Established procedures can be used by controllers or processors in order to achieve the compliance with the GDPR.

The goal of a single digital market strategy is to increase confidence in digital services and their security. For this purpose, the key action was the reform of the data protection framework. A review of Directive

2002/58/EC ("the e-privacy directive") has been announced to ensure a high level of protection of the privacy of users of electronic communications services. This proposal revises the e-privacy directive as envisioned in the Digital Single Market Strategy objectives, ensuring compliance with GDPR. The new regulation would notably standardize the EU-based legislation regarding privacy within the electronic communications sector and all stakeholders (business that targets EU citizens) will be invited to comply.

References

[1] Starčević, K., *et al.* (2018). Implementation of the general data protection regulation in companies in the Republic of Croatia. *Econviews*.

[2] Blix, F., *et al.* (2017). Data protection by design in systems development: From legal requirements to technical solutions. *Proceedings of* 2017 *12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 98–103). Cambridge.

[3] Hansen, M. (2016). Data protection by design and by default à la european general data protection regulation. *Privacy and Identity Management,* 27–38. Cham: Springer International Publishing.

[4] Kurtz, C., *et al. Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors*, 11.

[5] Puijenbroek, J., & Hoepman, J.-H. *Privacy Impact Assessment in Practice*, 9.

[6] Ahmadian, A. S., *et al.* (2018). Supporting privacy impact assessment by model-based privacy analysis. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing - SAC '18* (pp. 1467–1474). Pau, France.

[7] Huth, D. (2017). *A Pattern Catalog for GDPR Compliant Data Protection*, 7.

[8] Kosta, E., & Cuijpers, C. (2014). The draft data protection regulation and the development of data processing applications. *Privacy and Identity Management for Emerging Services and Technologies*, 12–32. Berlin, Heidelberg: Springer Berlin Heidelberg.

[9] Čizmić, J., & Boban, M. (2018). Učinak nove EU Uredbe 2016/679 (gdpr) na zaštitu osobnih podataka u Republici Hrvatskoj. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, *39(1)*, 377–406.

[10] Martínez-Martínez, D.-F. (2018). Unification of personal data protection in the European Union: Challenges and implications. *El Profesional de la Información*, *27(1)*, 185.

[11] Tikkinen-Piri, C., *et al.* (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34(1)*, 134–153.

[12] Lopes, I. M., & Oliveira, P. (2018). Implementation of the general data protection regulation: A survey in health clinics. *Proceedings of 2018 13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). Caceres.

[13] Mikkonen, T. (2014). Perceptions of controllers on EU data protection reform: A Finnish perspective. *Computer Law & Security Review*, *30(2)*, 190–195.

[14] (2018). General data protection regulation. *A Guide to Financial Regulation for Fintech Entrepreneurs,* 187–194. Chichester, UK: John Wiley & Sons, Ltd.

[15] Gellert, R. (2018). Understanding the notion of risk in the general data protection regulation. *Computer Law & Security Review*, *34(2)*, 279–288.

[16] UREDBA (EU) 2016/ 679 EUROPSKOG PARLAMENTA I VIJEĆ - od 27. travnja 2016. - o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/ 46/ EZ (Opća uredba o zaštiti podataka), 88.

[17] Bieker, F., *et al.* (2016). A process for data protection impact assessment under the European general data protection regulation. *Privacy Technologies and Policy*, *9857*, 21–37. Cham: Springer International Publishing.

Renata Mekovec is associate professor at Faculty of Organization and Informatics. Her educational background is a PhD in the field of information and communication science in 2011, a master's degree in the field of information science in 2006 and a bachelor's degree in information systems (informatics) in 1997, all at the Faculty of Organization and Informatics, University of Zagreb, Croatia.

She has published research papers in national and international journals and conference proceedings and has contributed several international and national projects. Her research interests lie in the fields of 1) privacy and personal data protection, 2) e-service quality and evaluation of e-service quality, 3) e-service users' perception of privacy and e-service quality.

Dijana Peras is a teaching assistant at the Faculty of Organization and Informatics, University of Zagreb, Croatia, and she is working toward her Ph.D. degree in the Department of Information Systems Development.

Her research interests include privacy and personal data protection and IT service management. was Her educational background is a master's degree in in the field of information science in 2010 and a bachelor's degree in information systems in 2008, all at the Faculty of Organization and Informatics, University of Zagreb, Croatia