Đorđe Krivokapić[1], Danilo Krivokapić[2], Ivan Todorović[1], Stefan Komazec[1]
[1]University of Belgrade, Faculty of Organizational Sciences
[2]Share Foundation, Novi Sad

UDC: 005.336.5:004
005.922.1:351.076(497.11)

Mapping Personal Data Flow and Regulatory Compliance in Serbian Public Institutions

DOI: 10.7595/management.fon.2016.0018

Personal data protection is becoming a major research topic in the last decades. With the technological advances, this issue was given a completely new perspective, due to increased possibilities for both use and misuse. Personal data have become a very valuable resource for different organizations worldwide in various sectors. However, regardless the efforts and constant legislation processes, personal data protection has still not been adequately managed, especially in developing countries such as Serbia. The motivation for this research was the big leak of personal data collected by the Serbian Privatisation Agency that occurred in 2014. During the research we analyzed legal, organizational and technical aspects of personal data management in six public institutions that are the largest personal data processors in Serbia. In this paper we provide the overview of the current situation and the recommendations for policy makers related to personal data protection in Serbia with a focus on the public sector.

Keywords: Data protection, personal data, privacy, public administration, public sector management, organizational measures, IT security

1. Introduction

Personal data represent an important currency in the new millennium (Schwartz, 2004, Krivokapić 2016.) and are a global issue today (Long & Quek, 2002). The notion of data protection originated in Europe and is now widely accepted throughout the world. Although it is not explicitly mentioned in the articles of the conventions regulating the right to privacy, the Human Rights Committee in its General Comment 16 on Article 17 of the International Covenant on Civil and Political Rights (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)[1] included this concept as an integral part of the right to privacy as early as 1988. The Committee stated that "the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law", and that "every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files". If such files contain "incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination".

Today, the EU is a global leader in setting data privacy standards (Heisenberg, 2005, Schoch 2016.). Open data policies represent a persistent topic in the EU (van Loenen, Kulk & Ploeger, 2016). Serbia is currently in the process of adjusting its legislation with the EU directives in many areas (Komazec, Todorović, Krivokapić & Jaško, 2013). Most jurisdictions, including that of the Republic of Serbia, accepted the EU approach and addressed personal data protection by special legislation (Law on Personal Data Protection, Official Gazette of the Republic of Serbia 97/2008, 104/2009, Cvik & Pelikánová 2016.).

[1] The UN Human Rights Committee General Comment 16 on Article 17 of the International Covenant on Civil and Political Rights (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) 1988. Retrieved June 21, 2016, from http://ccprcentre.org/doc/ICCPR/General%20Comments/HRI.GEN.1.Rev.9%28Vol.I%29_%28GC16%29_en.pdf

Recent advances in computer technology and e-government have provided almost instantaneous transmission of personal data (Huie, Laribee & Hogan, 2002, Graham, Gooden & Martin, 2016.) and caused an increased collection and exchange of such data (Stoica & Safta, 2015, Gang-Hoon, Trimi & Ji-Hyong 2014). Consequently, technology still is, and will continue to be, the preeminent driving force behind legal developments in the field of data privacy (Kuner, Cate, Millard & Svantesson, 2014; Schoch, 2016; Zharova, 2016). On the other hand, information technology misuse has increased the vulnerability of personal data (Toval, Olmos & Piattini, 2002, Borgesius, Gray& van Eechoud, 2015) while privacy impact assessment studies (Wadhwa & Rodrigues 2013.) are not yet conducted in many countries such as Serbia. Although the new technologies offer considerable benefits to consumers, businesses and governments, there is a growing concern that their widespread use may threaten the privacy of personal information (Pearce & Platten, 1998; Waxman & Barile 2016). Public agencies are increasingly required to collaborate with the private sector (Fan 2016) and one another in order to provide high-quality e-government services, and since personal data handled by governments are often very sensitive, most governments have developed some sort of legislation focusing on data protection (González, Echevarría, Morales, & Ruggia, 2016). Such legislation also affects businesses in the EU (Allison, 2016), but outside the EU as well (Gilbert, 2016). Technology helped modernisation of the EU legislation related to personal data protection (de Terwangne, 2014). However, due to a rapid development of information technologies and internet communication, many of the laws are still not in line with the current state of technologies (Sidgman & Crompton, 2016) and that is why they should be revised in order to set personal data protection on an appropriate level and to enable an efficient protection of reputation (Calzolaio 2016.). As a consequence, the European Union has decided to review its legal framework by updating current Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, that until now have had a decisive impact on the development of the personal data protection. The General Data Protection Regulation (GDPR) will be applied from mid 2018 and is expected to significantly improve the protection of personal data and citizens' rights.

This research was motivated by the case of the Serbian Privatization Agency in 2014, when a huge amount of personal data about citizens of Serbia became publicly available on the Internet. In the next chapter we will describe this case and its implications. Chapter 2 will explain the methodology used in the research. Chapter 3 provides the overview of key findings, while more details of research results are presented in chapter 4 on an actual example. Chapter 5 brings our recommendations and the final, chapter 6 offers the conclusions and guidelines for future research.

1.1. The Case of Serbian Privatisation Agency

In December 2014 the SHARE Foundation has discovered and informed the public[2] about the major leak of personal data in Serbia so far. A document containing personal information (including Unique Master Citizen Number, JMBG) of 5,190,396 citizens of Serbia was publicly available on the official website of the Privatization Agency for more than 10 months without any legal basis. During that period, according to the Agency officials, the document was downloaded by unknown individuals "many times". Having in mind that JMBG is widely used and is an essential part of virtually every personal data collection in Serbia, it is still difficult to fully grasp the consequences of this case. Nevertheless, it is particularly worrying that many data controllers still use JMBG as a tool for authentication. For example, "The Register of Unpaid Fines"[3] is an online database where, in order to check if a person has any unpaid fines, the only required information for the search are the name and the JMBG, exactly the information that was made publicly available by the Privatization Agency.

The case of the Privatization Agency revealed the risks to which our data are exposed, but it also emphasized the lack of reliable knowledge about the practical and technical conditions in which the citizens' data

[2] SHARE Foundation (2014, December 24) Personal data of more than 5 million citizens of Serbia unlawfully published. Retrieved June 21, 2016, from http://www.shareconference.net/en/defense/personal-data-more-5-million-citizens-serbia-unlawfully-published
[3] The Register of Unpaid Fines. Retrieved June 21, 2016, from https://rnk.sipres.sud.rs/

are collected, processed and stored. All operators should take appropriate organizational and technical measures to ensure the protection of personal data and privacy (Weber, 2010). It could be said that this case symptomatically depicts a worrisome state of affairs regarding personal data protection in Serbia. In the 2015 annual report, the Commissioner for Information of Public Importance and Personal Data Protection[4] noted that in the area of personal data protection the situation is "very troubling" and that "numerous incidents concerning the violation of the rights to personal data protection, some of them extreeme in size or in character, imperatively demand a complete change of attitude in the government and in the society as a whole towards the protection of personal data and privacy in general''.

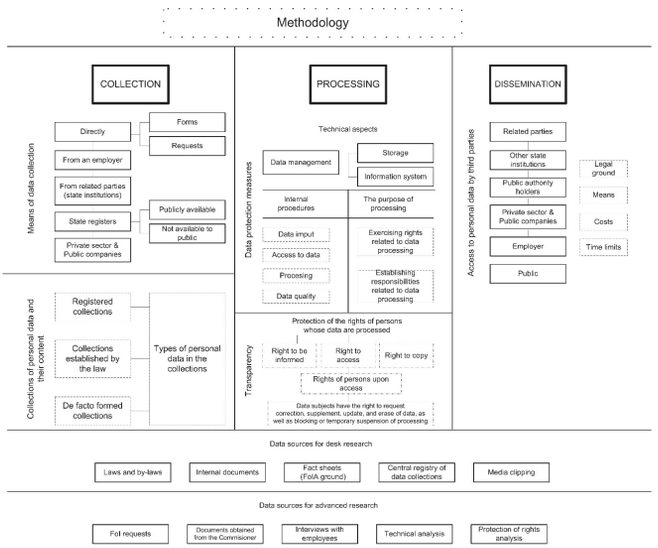
2. Methodology of Research

Our research started in April 2015 and included six public institutions: the Business Registers Agency, the Center for Social Work Belgrade, the Central Registry of Social Insurance, the National Health Insurance Fund, the Pension and Disability Insurance Fund and the Tax Administration. These are all very important and significant data controllers owning huge databases, while some of them process especially sensitive data such as health information, data about adopted children, etc.

In the initial phases of research the main sources were publicly available databases and regulations. We analyzed dozens of laws, bylaws, regulations and various documents regulating data processing in targeted institutions. The analysis included a review of relevant and international legal and policy framework. This was followed by desk research which included collection and analysis of data from public sources, technical investigations and documents and information we received via customized requests for access to information of public importance. We sent 20 formal requests to targeted institutions with more than 200 relevant questions. We also investigated procedures for access, copy and information of processed personal data in targeted institutions. We received 52 various documents regarding targeted institutions with more than 250 pages from Commissioner's office. During research we held 15 different meetings with targeted institutions (Commissioner included). In the meantime, a team of journalists searched the archive of print media from 2003 onwards, looking for coverage on privacy and data protection issues in the targeted institutions.

Each targeted institution has been investigated in relation to the processes of collection, processing and dissemination of personal data. The research plan, presented in the table below, was fully executed.

Table 1 : Research plan - Methodology



[4] Commissioner for Information of Public Importance and Personal Data Protection, Annual Report (2015). Retrieved June 21, 2016, from http://www.poverenik.rs/sr/izvestaji-poverenika/2328-izvestaj-poverenika-za-2015-godinu.html

The research team has been composed of various legal, organizational and technical experts. The entire process including completion of outputs was supported by journalists and visualization experts.

The results were verified through a two day long meeting and continuous communication with representatives of the Commissioner's office and targeted institutions. All the results have been published at the website www.mojipodaci.rs.

3. Key Findings

The overall conclusion is that personal data of Serbian citizens are multiplying and that the same data are located in many of the targeted institutions. For example, data about personal residence or personal salary are located in databases of 4 out of 6 institutions. This is the risk for information quality, but, more importantly, it is a risk for data security, as the case of the Privatization Agency demonstrated, data leakage in one of the institutions can compromise data security in all of the others.

One of the main findings is that all these institutions have their own database servers which are based in Serbia, usually in their headquarters, which means that they have a basic prerequisite to have control over the data. None of the institutions use cloud services.

During the course of our research, none of the institutions had a data protection officer, the employee responsible for personal data protection. Although this is not a legal requirement at the moment, it will become one in the near future, having in mind that this obligation of public institutions is prescribed by the new General Regulation on Data Protection in the EU as well as by the new draft Law on data protection in Serbia[5]. Education of employees regarding data protection issues is not at a satisfactory level in a majority of institutions and this is why it seems that awareness about privacy as a value and significance of data protection procedures is something that should be raised among the employees of public institutions. All institutions, except the Center for Social Work Belgrade, have some sort of a system of roles when it comes to permissions to access personal data of citizens, which is a very good practice.

Our main conclusion when it comes to personal data protection in these institutions is that the overall conditions are actually good in many areas, while there is room for further improvement. The institution that stands out is the Center for Social Work Belgrade. Although this institution processes the most sensitive data (data about adopted children, data about persons who experienced violence, etc.), our research revealed it has insufficient means in terms of funds and technical and human resources in order to adequately manage the risks concerning data protection. We also understand that the other five institutions are advanced and have a lot of resources, having received major financial support for development. They are certainly the best examples in Serbia, among more than 11,000 public institutions, and we fear that in smaller ones the situation is far worse than what we were in a position to see during this research.

4. Example of Research Findings - The Case of the Central Registry of Obligatory Social Insurance (CROSO)

The Central Registry of Social Insurance (hereinafter: "The Central Registry") was founded in 2010 and became operational in 2013. This institution maintains the central database with personal data of all socially insured citizens in Serbia (hereinafter: "The Central database") and this system, in accordance with the Law on the Central Registry of Obligatory Social Insurance (Zakon o centralnom registru obaveznog socijalnog osiguranja, "Sl. glasnik RS", br. 30/2010, 44/2014 - dr. zakon i 116/2014), is the main source of personal data for databases at the National Health Insurance Fund and at the Pension and Disability Insurance Fund, but is also used by Tax Administration and the Business Registers Agency. Namely, a big volume of personal data is now gathered by submitting a single electronic registration to the Central Registry. The Central Reg-

[5] Personal Data Protection Draft Law. Retrieved June 21, 2016, from http://www.paragraf.rs/dnevne-vesti/041115/041115-vest19.html

istry also provides electronic links to other registers and databases, which are kept in the Republic of Serbia, and have significance for social insurance.

The Central database contains more than 20 different kinds of information about every socially insured citizen, such as the place of residence, the name of the employer, degree of education etc. This information was initially taken over from other institutions such as The National Health Insurance Fund, the Tax Administration and others, and today this information is gathered by submitting a single electronic registration to the Central Registry.

The Central Registry does not hold data in the paper form, everything is stored in the electronic form in the Information System of the Central Registry (hereinafter: "IS"). The entire IS was developed internally and in cooperation with other public institutions. Within the IS there are two database servers for the collection, processing and storage of personal data, as well as Web servers and security servers. All servers are located in the server room in the Headquarters of the Central Registry, and are owned by the Central Registry.

Access to the Central database is provided to the following categories of users:[6]

- **Employees of the Central Registry** access the Central database through the designated portal and through special applications of the Central Registry, and with the use of qualified electronic certificates. Every employee is assigned with certain privileges in the IS based on the type of work he/she is conducting.
- **Citizens** can access the Central database and see only their own data. At this moment there are three types of verification for this access: 1) through qualified electronic certificate, 2) using the ID card or 3) entering username and password.
- **Companies** can access the Central database with the use of qualified electronic certificates and carry out various actions in the system, such as viewing information, registration and deregistration of citizens, but only for their own employees.
- **Public institutions** that need data from the Central database communicate with the Central Registry through the Virtual Private Network (VPN), the maximum protected mechanism for the electronic exchange of data via the Web, and FTP services. VPN connections between all institutions are part of the network of the Administration for Joint Services of the Republic Bodies (UZZPRO).
- **Maintenance** of the IS is done through a dedicated computer and in order to access the IS it is necessary to be physically present in the Headquarters of the Central Registry .

Every access to the Central database is recorded in the logs. Logs are kept for a year.

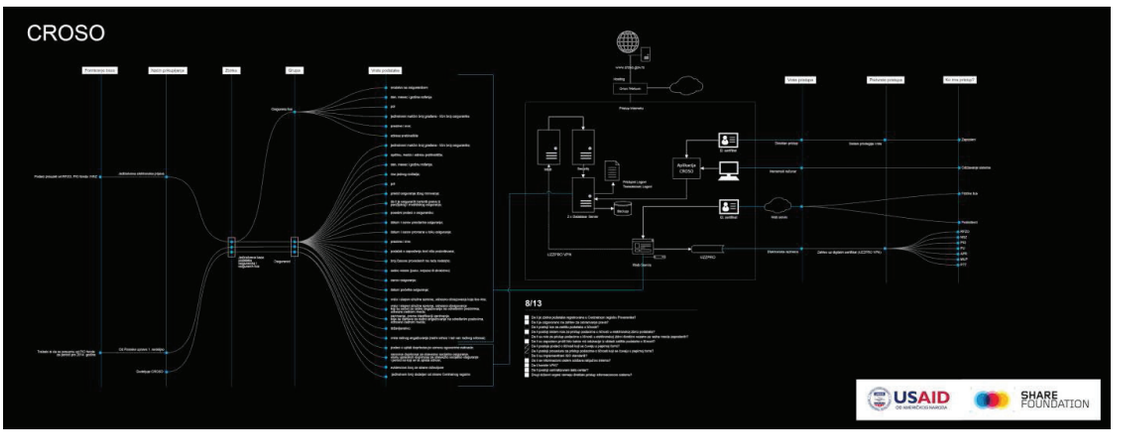


Figure 1: Map of the Central Registry of Obligatory Social Insurance (CROSO)

[6] My Data Project. Retrieved June 21, 2016, from https://mojipodaci.rs/croso/

5. Discussion and Recommendations

5.1. Replacing Unique Master Citizen Number (JMBG)

After the major breach of privacy with the publication of unique personal numbers of more than five million citizens of Serbia, it has become clear that this type of identification should be abandoned altogether. Moreover, it should never again be used as a means of authentication for access to personal data.

As an appropriate substitute there is already in use a personal social security number (LBO) assigned by the Central Registry and owned by the majority of citizens of Serbia. Unlike the JMBG, most of the digits contained in the LBO are randomly generated and have no relation to the personal traits of the owner. The number is permanent and it can be used as a unique identifier for all relevant purposes.

5.2. Data Centralization and Shared Infrastructure

The Administration For Joint Services of the Republic Bodies (UZZPRO) already manages a variety of shared government resources and is an obvious choice of agency to take on tasks related to building and maintaining shared infrastructure. These would include running a state data cloud for the purpose of data centralization.

As for now, it is common that chief data controllers gather and process the same personal information redundantly, thus exposing it to unnecessary security risks. Aside from reducing the exposure, the data centralization would enable uniform protection measures and access protocols.

Furthermore, centralized data pave the way to upholding a higher quality of information while improving interoperability and efficiency in the open data regime.

5.3. Open Data

It is imperative to establish a legal framework for exercising the right to re-use of the public sector information. This can be implemented swiftly by following the existing solutions applied in Croatia, namely by amending the current Law on Free Access to Information of Public Importance. In such a manner, the open data regime would be kept within the present framework and under the authority of the Commissioner for Information of Public Importance and Personal Data Protection.

5.4. Organizational Measures for Personal Data Protection

All institutions that collect, process and store personal data must take a set of formal organizational measures to secure personal data protection.

The initial one is the adoption of the Internal Act on the Personal Data Protection, which should regulate the issues related to the data collection and processing, personal data security, notification of the manner of exercising rights regarding personal data processing and protection, access to personal data and liability for their unlawful processing and use, as well as keeping the register of processing records for each data collection.

We also advise the institutions to act proactively and to appoint the data protection officer although it is currently not a legal requirement, since it will be obligatory when the new Law on Personal Data Protection is adopted. Such person should be on a higher hierarchical level of organizational structure, in the top management if possible, in order to have enough authority and power to secure the implementation of the General Act on the Personal Data Protection within the whole institution.

A further recommended measure is to define access levels to personal data for all potential stakeholders: 1) employees, 2) other institutions, 3) persons whose data is collected and 4) general public, in accordance

with the Law on Personal Data Protection. It is necessary to secure that access to the collected personal data is granted only to those who have a legal basis for their processing, and to ensure that each action is recorded.

Finally, a recommended measure is also to align the Rulebook on Internal Organization and Systematization of Job Positions and Integrated Management System (IMS) documents with the Internal Act on the Personal Data Protection and the role system for personal data access.

5.5. Education

A successful development and advancement of e-government depend on an up-to-date education and continual training of the public sector employees in the areas of personal data protection, information privacy and digital security. We propose dual education from the field of personal data management and protection: 1) in employment, 2) annual examination for all employees who deal with personal data. Given the present situation, it is recommended that gamified online courses are developed and offered to various public employee categories.

5.6. Legal Framework

A new Personal Data Protection Law is required, without any further delay, drafted in line with the new EU General Data Protection Regulation and based on the Commissioner's Model. It should also be noted that a new Strategy for personal data protection is needed, followed immediately by the adoption of a relevant Action Plan without which the Strategy would be useless.

Once a new Personal Data Protection Law is passed, a series of relevant by-laws would be required, describing in detail the necessary procedures and protocols to enforce the Law itself.

Conslusion

As main results of this research, we have written in-depth reports regarding data processing for each targeted institution. These reports were made using the same methodology and they consist of 5 main parts: 1) legal aspect of data processing (compliance with the law), 2) organizational aspect of data processing (which are the organizational measures for data protection), 3) technical aspects of data processing (which are the technical measures for data protection), 4) media coverage of data protection in institutions and 5) documents received from the Commissioner's office.

Also, our publication "A Guide for Public Authorities – Personal Data Protection" (Krivokapić et al., 2016) includes best practices and procedures of data protection that are applied in the analyzed institutions, but also a rich experience of the Commissioner in this area, as well as knowledge and innovation of the SHARE Foundation, which specifically deals with privacy issues in the digital environment, and policy and organizational design experts from the Faculty of Organizational Sciences at the University of Belgrade. The Guide is available for free and can be used under a Creative Commons license.

We have developed a research methodology[7] for preparing reports on personal data processing in public authorities applicable to any public authority in Serbia. This methodology captures the essence of the research process and, when implemented, it can give the answers to the essential questions: What personal data are processed by a public authority and why? What are the organizational measures for data protection and what are the technical measures for data protection? It can be used by other researchers who deal with the issues of privacy and personal data protection, but can also be used by competent state authorities, and, of course, the citizens interested in these issues themselves.

[7] SHARE Foundaation, Research Methodology. Retrieved June 21, 2016, from http://www.shareconference.net/sites/default/files/u742/metodologija_za_izradu_izvestaja-1_1.pdf

REFERENCES

[1] Allison, P.R. (2016). What EU Data Protection Rules Mean for Business. Computer Weekly, 7/19/2016. pp. 20-23.

[2] Borgesius F. Z,, Gray J. & van Eechoud M., (2015). Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. Berkeley Technology Law Journal. 2015, Vol. 30 Issue 3, p2073-2131. 59p. DOI: 10.15779/Z389S18

[3] Calzolaio s. (2016) Digital (and privacy) by default. Constitutional identity of e-government, Journal of Constitutional History (Giornale di Storia Costituzionale). Jan 2016, Issue 31, p185.

[4] Commissioner for Information of Public Importance and Personal Data Protection, Republic of Serbia (2015). Annual report on implementation of the Law on Free Access to Information of Public Importance and the Law on Personal Data Protection.

[5] Cvik E. D. & Pelikánová R. M. (2016). Implementation of Directive 2014/17/EU and its Impact on EU and Member States Markets, from not only a Czech Perspective. 19th International Conference Enterprise and Competitive Environment 2016, Procedia - Social and Behavioral Sciences 31 May 2016 220:85-94. DOI: 10.1016/j.sbspro.2016.05.472

[6] de Terwangne, C. (2014). The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data. International Review of Law, Computers & Technology, 28(2). pp. 118-130. DOI:10.1080/13600869.2013.801588

[7] European Parliament (1995). Directive 95/46/EC. Official Journal L 281, 23/11/1995, pp. 31-50.

[8] Fan M. (2015). Private Data, Public Safety: A Bounded Access Model Of Disclosure. North Carolina Law Review; 2016, Vol. 94 Issue 1, p161-207, 47p

[9] Gang-Hoon K. Trimi S. & Ji-Hyong C. (2014), Big-Data Applications in the Government Sector, Communications of the ACM. Mar2014, Vol. 57 Issue 3, p78-85. 8p. 1 Diagram, 1 Graph., doi:10.1145/2500873

[10] Gilbert, F. (2016). EU General Data Protection Regulation: What Impact for Businesses Established outside the European Union. Journal of Internet Law, 18(11). pp. 3-8.

[11] González, L., Echevarría, A., Morales, D., & Ruggia, R. (2016). An E-government Interoperability Platform Supporting Personal Data Protection Regulations. CLEI Electronic Journal, 19(2). p. 8.

[12] Graham F. S., Gooden S. T. & Martin K. J. (2016), Navigating the Transparency–Privacy Paradox in Public Sector Data Sharing. American Review of Public Administration. Sep2016, Vol. 46 Issue 5, p569-591. 23p. DOI:10.1177/0275074014561116

[13] Heisenberg, D. (2005). Negotiating privacy: The European Union, the United States, and personal data protection. Boulder, USA: Lynne Rienner Publishers.

[14] Huie, M. C., Laribee, S. F., & Hogan, S. D. (2002). Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues. Tulsa Journal of Comparative & International Law, 9(2), pp. 391-470.

[15] Komazec, S., Todorović, I., Krivokapić, Đ., & Jaško, O. (2013). Capacities of Local Self-Governments in Serbia for Compliance with EU Directives on Public Procurement. Management - Journal for Theory and Practice, 2013(69), pp. 15-23. DOI: 10.7595/management.fon.2013.0030.

[16] Krivokapić, D., Krivokapić, Đ., Todorović, I., Komazec, S., Petrovski, A., & Ercegović, K. (2016). A Guide for Public Authorities – Personal Data Protection. Novi Sad, Serbia: SHARE Foundation. Retrieved from http://www.shareconference.net/sites/default/files/u742/8_-_vodic_jrga_final.pdf

[17] Krivokapić, Đ. (2016), Sukob zakona i nadležnosti koji proizlazi iz povrede reputacije putem Interneta, PhD Thesis, UDK: 316.774:34

[18] Kuner C., Cate F. H., Millard C., & Svantesson D.J.B. (2014). The (data privacy) law hasn't even checked in when technology takes off, International Data Privacy Law, 2014, Vol. 4, No. 3, 175, doi:10.1093/idpl/ipu01

[19] Law on Free Access to Information of Public Importance (2010). Official Gazette of the Republic of Serbia, No. 120/04, 54/07, 104/09 and 36/10.

[20] Law on Personal Data Protection (2012). Official Gazette of the Republic of Serbia, 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012.

[21] Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. Journal of European Public Policy, 9(3), pp. 325-344.

[22] Pearce, G., & Platten, N. (1998). Achieving Personal Data Protection in the European Union. Journal of Common Market Studies, 36(4). pp. 529-547. DOI: 10.1111/1468-5965.00138.

[23] Schoch, T. P. (2016). EU privacy regulations' impact on information governance. Information Management Journal, 50(1). pp. 20-25.

[24] Schwartz, P. M. (2004). Property, privacy, and personal data. Harvard Law Review 117(7), pp. 2056-2128.
[25] Sidgman, J., & Crompton, M. (2016). Valuing Personal Data to Foster Privacy: A Thought Experiment and Opportunities for Research. Journal of Information Systems, 30(2). pp. 169-181. DOI:10.2308/isys-51429
[26] Stoica, C. F., & Safta, M. (2015). Theoretical and practical issues relating to the right to the protection of personal data. Juridical Trib., 5. p. 88.
[27] Toval, A., Olmos, A., & Piattini, M. (2002). Legal requirements reuse: a critical success factor for requirements quality and personal data protection. In Proceedings of IEEE Joint International Conference on Requirements Engineering, pp. 95-103.
[28] United Nations, Human Rights Committee (1966). International Covenant on Civil and Political Rights.
[29) van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union. Government Information Quarterly, 33(2). pp. 338-345. DOI:10.1016/j.giq.2016.04.002
[30] Wadhwa K. & Rodrigues R. (2013). Evaluating privacy impact assessments. Innovation: The European Journal of Social Sciences. Mar-Jun2013, Vol. 26 Issue 1/2, p161-180. DOI: 10.1080/13511610.2013.761748
[31] Waxman S. S. & Barile F. G. (2016). "Eye in the Sky": Employee Surveillance in the Public Sector, Albany Law Review. 2016, Vol. 79 Issue 1, p131-149.
[32] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review, 26(1). pp. 23-30.
[33] Zharova, A. (2016). The salient features of personal data protection laws with special reference to cloud technologies. A comparative study between European countries and Russia. Applied Computing and Informatics, 12(1). pp. 1-15.

Receieved: June 2016.
Accepted: September 2016.

About the Author

Đorđe Krivokapić
University of Belgrade, Faculty of Organizational Sciences
krivokapic@fon.bg.ac.rs

Dr Đorđe Krivokapić, LL.M., is an associate lecturer at the Faculty of Organizational Sciences at the University of Belgrade where he teaches courses on business law and IT law. Before his faculty position, he was employed as a legal associate at the law office of Karanović & Nikolić where he was involved in numerous successful transactions and projects in the Balkan region. Before joining Karanović & Nikolić, Đorđe Krivokapić graduated with a degree in law from the University of Belgrade, earned an LL.M. degree from the University of Pittsburgh School of Law and a PhD from the University of Belgrade, Faculty of Law. As of 2013 Đorđe serves as a Policy & legal director of the SHARE Foundation.

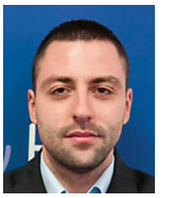
Danilo Krivokapić
Share Foundation, Novi Sad
danilo@sharedefense.org

Danilo Krivokapic graduated from the University of Belgrade, Faculty of Law. After working in the Belgrade City Administration for 5 years, he passed the bar exam and joined the SHARE Foundation, where he works as a Coordinator for privacy and data protection. He led the “Personal Data in the Public Sector” Project during 2015-2016. His research is also focused on topics such as implementation of new privacy and data protection regulations and policies in domestic legal framework, data economy and its impact on privacy, new types of cybercrime etc.

Ivan Todorović
University of Belgrade, Faculty of Organizational Sciences
todorovic.ivan@fon.bg.ac.rs

Ivan Todorovic works as a teaching assistant at the University of Belgrade, Faculty of Organizational Sciences. His research area includes organizational design, restructuring, organizational change and business process management. He has participated in more than 15 consulting projects, in companies such as Victoria Group, EMS, Milsped, Parking Service Belgrade, GSP Belgrade, Transnafta, and in several research projects financed by international institutions like the EBRD, UNIDO and USAID. He is a co-author of 3 books and more than 40 articles in international monographs, journals and conference proceedings. From 2011 to 2013 he was a visiting lecturer at the University of Maribor, Faculty of Organizational Sciences, in Slovenia. He was member of the team that won the HULT Global Case Challenge 2012 in London, and he won the Balkan Case Challenge 2010 in Vienna. He was also a mentor to students on numerous projects and a jury member at several international and local business case study competitions.

Stefan Komazec
University of Belgrade, Faculty of Organizational Sciences
komazec.stefan@fon.bg.ac.rs



Stefan Komazec is a teaching assistant at the University of Belgrade, Faculty of Organizational Sciences. Currently he teaches “Organizational Theory”, “Organizational Design”, “Quality Engineering” and “Quality Planning” to undergraduates and several subjects to master students. His major research interests are business process management, standardization, quality management, organizational change and restructuring. As an author or co-author, he has published 3 books and more than 40 articles from these areas in scientific journals and conference proceedings. He was involved in more than 15 business consulting projects in organizations like Milsped, GSP Belgrade, Transnafta, EMS, Victoria Group and Parking Service Belgrade, as well as in several research projects under the patronage of international institutions such as the UNIDO, EBRD or USAID. He is one of the founders and a project leader of international student sport tournament EuroBelgrade, which is organized by the Faculty of Organizational Sciences every year.