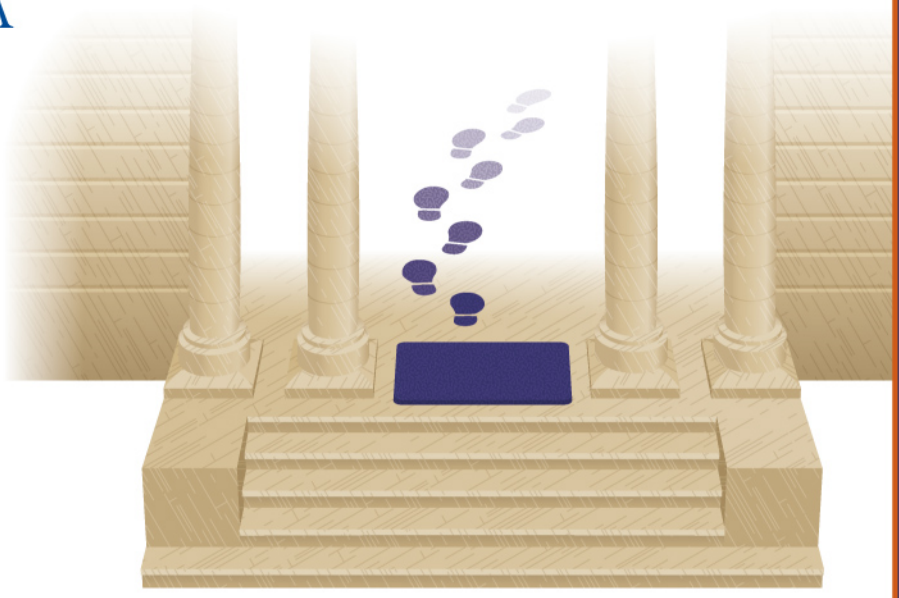
PARTNERS for Democratic Change SERBIA

CHRIS
Mreža Odbora za ljudska prava u Srbiji CHRIS
The Network of the Committees for Human Rights in Serbia CHRIS



Protection of **PRIVACY** in Serbia

Analysis of Implementation of the Personal Data Protection Law

THIS PROJECT IS FUNDED BY THE EUROPEAN UNION

USAID FROM THE AMERICAN PEOPLE | SERBIA

PARTNERS FOR DEMOCRATIC CHANGE SERBIA

PROTECTION OF PRIVACY IN SERBIA

Analysis of Implementation of the Personal Data Protection Law

March 2013

Authors:
Uroš Mišljenović
Blažo Nedić
Ana Toskić

Published by:
Partners for Democratic Change Serbia

For the Publisher:
Blažo Nedić

Design and layout:
Stefan Ignjatović

Print:
Manuarta, Belgrade

Copies:
500

This publication is made possible by the support of the Delegation of the European Union to the Republic of Serbia and American people through the United States Agency for International Development (USAID) Judicial reform And Government Accountability Project and does not necessarily reflect the views of the European Union or USAID or the United States Government.

* * *

All terms used in the text in the male grammatical gender include the male and female individuals to which they relate.

CONTENTS

1
FOREWORD

Protection of privacy still represents a relatively new concept in Serbia. Although the right to protection of personal data is one of the basic human rights guaranteed by the Constitution, the basic legal framework in the Republic of Serbia was established in October 2008[1], with the adoption of the Law on Personal Data Protection (the Law). This Law introduces a broad range of duties for a large number of subjects and establishes the central role of the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner) as an independent state body responsible to ensure protection of the right to privacy through a second instance procedure, as well as to monitor the implementation of the Law. Following the adoption of the Law, the Commissioner, in addition to performing its statutory authority, undertook a series of activities aimed at promotion of the implementation of the Law and provision of information to the public and subjects of the Law on the provisions, rights and obligations contained therein.

The right to protection of personal data and the adequacy of the protection of this right is of paramount importance in the process of Serbia's EU accession. This is indicated by a special Article of the Stabilization and Association Agreement (Article 81) that Serbia signed in December 2007.

From November 2010, the Partners for Democratic Change Serbia (Partners Serbia) took an active part in promoting the right to privacy, awareness raising and capacity building of data controllers and civil society organizations for effective implementation of the Law and the protection of personal data in accordance with the highest international standards. Through cooperation of Partners Serbia with the Commissioner's Office and other organizations, several projects have been conducted and a series of activities performed: as part of the project supported by the Open Society Foundation, Serbia (OSF), on 28 January 2011, for the first time in Serbia a conference was organized to mark the Personal Data Protection Day, and the 30th anniversary of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, a variety of promotional activities was organized, a number of seminars

1 Previous Law on Personal Data Protection in 1998 (Official Gazette FRY 24/98) did not have a single case of practical implementation.

and panel discussions for representatives of state authorities, local self-government, organizational units and the Ministry of Interior, civil society organizations, media organizations and journalists' associations and centers for social work; within the project supported by the EU Delegation in Serbia and OSF, a specialized training was organized for 40 representatives of civil society organizations to build capacity for the implementation of the Law in practice, and training for monitoring, advocacy for effective implementation of the Law, and provision of legal aid to citizens in this area; in collaboration with the Network of Committees for Human Rights in Serbia (CHRIS Network) a number of activities was organized in 6 cities in Serbia and an electronic newsletter was launched to promote privacy and awareness of the need for a comprehensive implementation of the Law; in January 2013, an internet platform was launched (www.partners-serbia.org/privatnost) with the aim of raising public awareness on the protection of personal data, exchange news, information and experience regarding protection of privacy, and provision of free legal aid to citizens in the field of personal data protection.

According to the estimations of the Commissioner, there are between 300,000 and 350,000 data controllers, subjects of the Law on Personal Data Protection in Serbia. However, a comprehensive analysis of the implementation of the Law, as well as the analysis of the actions of data controllers upon the Commissioner's decision, which are binding, final and enforceable, has never been conducted in Serbia so far. Also, there is no aggregate information on whether data controllers take technical and organizational measures to protect personal data from abuse, which is also one of the obligations stipulated by the Law.

As a part of the Project for the promotion and advancement of the Law on Personal Data Protection, supported by the Delegation of the European Union to the Republic of Serbia (DEU), and USAID Judicial Reform and Government Accountability Project (JRGA), Partners Serbia and CHRIS Network conducted a study on the implementation of the Law on Personal Data Protection in practice. The aim of this research, with the results presented in this report, was to examine whether selected personal data controllers comply with the provisions of the Law, the Commissioner's decisions, and whether they improve their internal procedures for personal data processing, in order to protect the privacy of their customers, clients and employees. The research included 51 data controllers from eight cities and municipalities within the territory of the Republic of Serbia.

This publication contains an overview of the legal framework governing the protection of personal data in Serbia and presents the methodology and results of the research on the implementation of the Law, including presentation of actions of data controllers' upon Requests for exercising the rights regarding personal data processing, the Commissioner's decisions upon appeals, actions of data controllers upon decisions of the Commissioner, the analysis of internal documents of data controllers and

undertaken measures of personal data protection, as well as four case studies selected by the authors during the six months of the research.

The authors would like to thank the representatives of the institutions and organizations participating in the research, the respondents who complemented this analysis with their experience and points of view, as well as the researchers who carried out activities in the field. We express special gratitude to the Office of the Commissioner for Information of Public Importance and Personal Data Protection for help and advice during the implementation of the research.

Blazo Nedic
Partners for Democratic Change Serbia

2
PERSONAL DATA PROTECTION IN SERBIA

2.1. The right to privacy

The right to privacy has deep roots in history[2], but in our region, after a decades-long trend of subordinating individual interests to the collective one, insisting on the protection of individual privacy only recently appeared. The right to privacy becomes particularly important due to IT developments and technological achievements enabling almost unlimited possibilities for the invasion of privacy of an individual, as well as violations that may arise from the misuse.

The meaning of the term privacy has not always been the same. At the end of the nineteenth century, Louis Brandeis and Samuel Warren defined privacy as "the right to be left alone," which included the protection of personal autonomy, moral and physical integrity, the right to choose lifestyle and ways of life, interactions with other people and so on. Over the time, this perception was supplemented with the mechanisms for practicing these rights. Alan Westin, one of the first and highly respected scientists who investigated the issue of privacy in the information age, argued that privacy involves more than the right to be left alone. It is the ability to control how much information we reveal about ourselves to others, as well as how and when we are doing it.

The right to privacy nowadays undoubtedly represents one of the basic human rights, but there are still different interpretations of its content, hence it is considered to be one of the fundamental rights which is most difficult to define, deeply conditioned by broader cultural and social context. In many countries, the concept of privacy is identified with the right to data protection, which is actually interpreted in the light of privacy of personal information management. However, in case the concept of privacy is considered more broadly than the protection of personal data, several aspects can be identified:

2 It is considered that some forms of the right to privacy existed in early Hebrew, Chinese and classical Greek culture.

- Data privacy, which involves the establishment of rules for the collection and processing of personal data;
- Privacy of the body, which means protecting the human body from invasive procedures (such as involuntary medical testing);
- Privacy of correspondence, which involves security and privacy of letters, telephone conversations, e-mail and other means of communication;
- Privacy of the territory – which includes setting boundaries for entry of third parties into the personal space of an individual.

With the development of information technology, during the sixties and seventies of the 20th century, there is a growing interest worldwide about the right to privacy, followed by the adoption of national and international documents that recognize and regulate the protection of privacy. Primarily, this is performed in the constitutions, and subsequently in special laws.[3]

Nowadays, this right is recognized and protected by the most important international instruments for the protection of human rights, starting with the United Nations Universal Declaration of Human Rights[4], the International Covenant on Civil and Political Rights[5], the UN Convention on the Rights of the Child[6], the European Social Charter[7], and the Charter of Fundamental rights of the European Union.[8] Perhaps the most comprehensive protection is provided by the Article 8 of the European

---

3 The first data protection law was passed in the German federal state of Hesse in 1970 and was followed by the adoption of the law in Sweden (1973), USA (1974), Germany (1977) and France (1978).

4 Article 12 of the Universal Declaration: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or the attacks against honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. ".

5 Article 17 of the Covenant provides that "no one shall be subjected to arbitrary or illegal interference with his private life, family, home or correspondence, or illegal attacks against honor and reputation", while Article 23 protects the family and the right to marriage and foundation of a family, and Article 24 governs the rights and protection of children and minors.

6 Article 16 of the Convention it is stated that "no child shall be subjected to arbitrary or unlawful interference with his/her privacy, family, home or correspondence, or unlawful attacks against honor and reputation."

7 Article 16 of the Charter guarantees the protection of marriage and family life.

8 In the Article 7, entitled "Respect for private and family life", the Charter states: "Everyone has the right to have his or her private and family life, home and communications respected"

Convention for the Protection of Human Rights and Fundamental Freedoms, under which a rich jurisprudence of the European Court of Human Rights developed over time:

The right to respect of private and family life

Everyone has the right to respect his/her private and family life, home and correspondence.

Public authorities shall not interfere with the exercise of this right, unless it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or moral, or the rights and freedoms of others.

In addition to these, umbrella tools envisaging protection of privacy, two documents have set the basis for the majority of the national laws in this field: Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data [9] in 1981 and the Guidelines of the Organization for Economic Cooperation and Development (OECD) governing the protection of privacy and cross-border flows of personal data[10] in 1980. These documents, principally the Council of Europe Convention, have had major impact on the development of a legal framework for the personal data protection in Serbia as well.

2.2. Legal framework

Despite the established basis of the legal framework, protection of individual privacy in Serbia remains a new concept, while it appears that the right to privacy has not been on the forefront state authorities' priorities for many years. In 1998, the Federal Republic of Yugoslavia adopted the Law on the Protection of Personal Data ("Official Gazette FRY" no. 24/98), which was a part of the legal order of the State Union of Serbia and Montenegro after the dissolution of Yugoslavia, and subsequently of the Republic of Serbia. However, this Law remained known as a regulation

9 http://www.poverenik.org.rs/index.php/yu/pravni-okvir-zp/medjunarodni-dokumenti-zp/1359-konvencija-o-zastiti-lica-u-odnosu-na-automatsku-obradu-podataka.html

10 http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

that was in effect for about ten years, with no attempt of any competent authority and/or the individual to use its protective mechanisms in practice. This figure illustrates the position of the state towards the right to privacy as a fundamental human right of citizens guaranteed by major international acts, starting with the Universal Declaration of Human Rights[11].

The Constitution of the Republic of Serbia in several articles guarantees the rights arising from the right to privacy, including, inter alia, the right to inviolability of the home, the right to secrecy of letters and parcels, and the protection of personal data. For the purposes of this study, the Article 42 of the Constitution governing the protection of personal data is the most relevant:

Personal data protection is guaranteed.

Collecting, keeping, processing and use of personal data shall be regulated by law.

It is prohibited and punishable to use personal data for purposes other than those for which they were collected, in accordance with the law, except for the purposes of criminal proceedings or protection of the security of the Republic of Serbia, in the manner provided by law.

Everyone has the right to be informed about the data collected about his/her personality, in accordance with the law, and the right to judicial protection against their abuse.

Due to pressures to harmonize domestic legislation with the European standards, Serbia adopted a new Law on Personal Data Protection (PDPL, the Law) on 23rd October 2008 ("Official Gazette" no. 98/08), and the implementation of the Law commenced on 1st January 2009. In addition, Serbia signed and ratified the Council of Europe Convention No. 108 on the Protection of Individuals with regard to automatic processing of personal data in September 2005, which came into force in the RS on 1st January 2006, and in October 2008 signed and ratified the Additional Protocol to the Convention 108 regarding supervisory authorities and transborder data flows ("Official Gazette – International Treaties", no. 98/2008).[12]

---

11 http://www.un.org/en/documents/udhr/index.shtml Article 12 of the Declaration: "No one shall be exposed to arbitrary interference with his privacy, family, home or correspondence, nor to attacks against honor and reputation"

12 Office for European Integration of the Republic of Serbia, the National Program for the Adoption of the acquis *(2013-2016)*, available at: http://seio.gov.rs/upload/documents/nacionalna_dokumenta/npi_usvajanje_pravnih%20tekovina.pdf, strana 451.

The 2008 Law establishes a broad range of responsibilities for a number of subjects, and envisages "the conditions for the collection and processing of personal data, the rights of individuals and the protection of individuals whose data are collected and processed, restrictions on personal data protection, the procedure before the competent authority for the personal data protection, data security, records keeping, transfer of data from the Republic of Serbia and supervision over the implementation of this law."[13] The Law also establishes the central role of the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner) as an independent state body, responsible for second-instance proceedings providing protection in the field of personal data protection, as well as for monitoring of the implementation of the Law.[14]

It is important to note that the aim of the Law "is not personal data protection itself, but the protection of the individual to whom the information relates, and thus part of his/her so-called informational privacy. PDPL does not cover the entire spectrum of the rights to privacy of an individual, but only the part of the right to privacy related to his personal data."[15]

The law defines personal data as any information "relating to a natural person, regardless of the form of its presentation or the medium used (paper, tape, film, electronic media etc.), regardless on whose order, on whose behalf or for whose account such information is stored, regardless of the date of its creation or the place of its storage, regardless of the way in which such information is learned (directly, by listening, watching etc., or indirectly, by accessing a document containing the information etc.) and regardless of any other characteristic of such information[16]

Next, the Article 3 of the PDPL defines that data processing is "any action taken in connection with data, including: collection, recording, transcription, multiplication, copying, transmission, searching, classification, storage, separation, crossing, merging, adaptation, modification, provision, use, granting access, disclosure, publication, dissemination, recording, organizing, keeping, editing, disclosure through transmission or otherwise, withholding, dislocation or other actions aimed at rendering data inaccessible, as well as other actions carried out in connection with such data, regardless whether those actions are automated, semi-automated or otherwise performed".

13 Article 1, Para 1 PDPL.

14 *Ibid*, Art 1 Para 3.

15 Nataša Pirc Musar, *Guide through the Law on Personal Data Protection, Commissioner for Information of Public Importance and Personal Data Protection*, Belgrade, 2009, page 15.

16 *Ibid*, Art 3, Para 1.

In the following analysis of the implementation of the Law on Personal Data Protection, we will see that an understanding of these two fundamental concepts essentially determines the actions of the controllers of citizens' personal data.

Moreover, the Law defines a set of individual's rights in terms of personal data protection. These rights include[17]:

- The Right to Give or Not Give Consent to Personal Data Processing – Every natural person has a right to give or not give consent to personal data processing to the controller, if the controller is not conducting the processing according to his/her legal mandate;
- The Right to Information on Personal Data Processing – The data subject has the right to request to be fully and truthfully informed by the controller about whether the controller is processing data on him/her, which data is being processed, to what purpose the aforementioned data is processed and on what legal ground it is being processed, and, who the data is collected from, that is, who the source of data is; in what filing system the data is included, who the recipients of the aforementioned data are, which data is being used, to what purposes and on what legal grounds; to whom the data is transferred, to what purposes and on what legal grounds; as well as other issues outlined in Article 19 of the Law on Personal Data Protection;
- The Right to Insight – The data subject is entitled to request from the controller to have insight into data concerning him/her. The right to insight into data concerning him/her includes the right to see, read and hear the data and the right to take notes;
- The Right to Copy – The data subject is entitled to request from the controller a copy of the data concerning him/her, while the necessary costs of making and transferring of the copy of data shall be borne by the data subject; The Rights of Data Subject Regarding Insight Performed – The data subject has the right to request from the controller the correction, amendment, updating, and erasure of data, as well as the termination and temporary recess of processing, if the conditions outlined in Article 22 of the Law on Personal Data Protection have been met.

In accordance with the Law, the Government of the Republic of Serbia adopted the Decree on the Form for and Manner of Keeping Records of Personal Data Processing ("Official Gazette" no. 50/2009 of 10.07.2009), but it is of particular concern that the Government has not yet adopted a bylaw to regulate the manner of storage and measures for protection of particularly sensitive data of the citizens, i.e. data relating to nationality, race,

17 See: http://poverenik.rs/sr/s-prava.html

sex, language, religion, political party affiliation, union membership, health, social assistance, victim of violence, criminal charges and sexual life.[18] The deadline for enactment of this act had already expired in April 2009.

The legal framework for the protection of personal data also involves the Decision of the Constitutional Court of the Republic of Serbia 68/2012[19], from 18.07.2012, which determined that certain provisions of the PDPL[20], stipulating that a legal basis for the processing of data can be determined in a bylaw, are not in accordance with the Constitution.

This Constitutional Court's decision is important for the practice of all data controllers insofar as it confirms the rule of the Constitution that the legal basis for data processing can be determined only by law and not in bylaws. It is therefore important that all data controllers harmonize their practices with the decision of the Constitutional Court as soon as possible, hence to cease establishing the grounds for processing of personal data by the documents of lower legal force than the law. However, the practice indicates that there are still a large number of such bylaws in place and in force.

Full respect of the right to personal data protection depends on several factors: an adequate legal framework, capacity and willingness of the subjects to comply fully with legal requirements, as well as the capacity of the Commissioner to fulfill the duty of the supervisory and appellate authority. In addition, it is essential that the subjects are aware of their legal obligations, but also to keep the public informed of the rights provided by the aforementioned law.

18 Article 16 PDPL.

19 http://www.uzzpro.gov.rs/doc/biblioteka/BiltenBr7-2012.pdf

20 Article 12 Para 1 Item 3) in a part that reads: "any other regulation promulgated in accordance with the law", Article 13 in a part as follows: "or any other regulation" and Article 14 Para 2 item 2) in a part as follows: "or any other regulation promulgated in accordance with the law"

3
RESEARCH ON THE IMPLEMENTATION OF THE LAW ON PERSONAL DATA PROTECTION IN SERBIA

The research on the implementation of the Law on Personal Data Protection was carried out in the period from October 2012 to March 2013, as part of the project supported by the USAID Judicial Reform and Government Accountability (JRGA) and the European Union Delegation to the Republic of Serbia. The research was conducted by ten researchers, representatives of Partners for Democratic Change Serbia, Committee for Human Rights Network CHRIS and the Association of Serbian Sign Language Interpreters, who were participants of a five-day specialized training on the protection of personal data for the civil society organized during 2011 and 2012.[21] The research team included: Milan Krstev, Dragan Djordjevic, Marija Mirkovic (Nis), Enes Beranac (Novi Pazar), Svetlana Stankovic (Negotin), Ljiljana Galovic (Novi Sad), Marija Nikolic and Jovana Vujic (Valjevo), Marija Berta, Ana Dešić, Ana Toskić, and Uros Mišljenović (Belgrade). The research was conducted in eight cities and municipalities in Serbia: Belgrade Loznica, Negotin, Nis, Novi Pazar, Novi Sad, Sabac and Valjevo.

3.1. The aims and reasons for the Research

According to the estimations of the Office of the Commissioner, there are between 300,000 and 350,000 data controllers – subjects of the Law on Personal Data Protection in Serbia. A comprehensive analysis on the action of controllers under the provisions of the PDPL in Serbia has not

21 The trainings were organized by Partners for Democratic Change Serbia in cooperation with the Commissioner. See more about the trainings at: http://www.partners-serbia.org/sr/arhiva-vesti/65-obuka-o-zatiti-podataka-o-linosti.html i http://www.partners-serbia.org/sr/component/content/article/102.html.

been performed so far. In addition, the Law on Personal Data Protection defines the competence of the Commissioner, whose decisions upon the citizens' appeal are binding, final and enforceable, but a comprehensive analysis of controllers' actions upon the Commissioner's decision has not been conducted yet. Furthermore, there are no aggregate data on whether the controllers undertake organizational and technical measures to protect personal data from misuse, which is also one of the obligations of each controller, provided by the Law.

The aim of this research was to investigate whether the selected personal data controllers in the sample comply with the provisions of the Law on Personal Data Protection, the decisions of the Commissioner for Information of Public Importance and Personal Data Protection, and whether controllers are developing their internal procedures for processing personal data, in order to protect the privacy of their customers, clients and employees.

Based on the information collected during the research, recommendations are made for a wide range of stakeholders in order to improve the protection of citizens' privacy. Moreover, a methodology for monitoring and analysis of the implementation of the PDPL, as well as the actions of data controllers upon the Commissioner's decisions, can be used as a basis for other researchers interested in the field of personal data protection in the future.

In the long term, the results of this research should influence the selected controllers, as well as those who were not involved in the research, to improve internal procedures of the processing of personal data of their customers, clients and employees.

The results of the research can be useful for a wide range of stakeholders, specifically:

a) For **individuals** – This Analysis includes specific advice on how the citizens can exercise their rights regarding personal data protection. Although PDPL contains certain flaws (more on this below), this Law provides specific guarantees for the protection of rights with respect to the processing of personal data by the controllers, which are still insufficiently utilized by the citizens.

b) For **controllers of personal data** – this Analysis represents the best practices in the actions of the controllers in terms of personal data protection, pointing out the identified obstacles that exist in practice. Insight into best practices may assist other controllers to improve internal policies and procedures for the processing of personal data of their customers, clients and employees. This may be particularly important for companies operating in developed markets, where protection of customers' privacy may be a comparative advantage, or when failures in personal data processing could endanger the reputation of the controllers. For

controllers handling the particularly sensitive personal data[22], which imply a higher degree of protection in line with the Law, this Analysis may be significant since it represents some of the solutions in the field of data protection.

c) For **civil society organizations** – This Analysis provides guidance for future monitoring activities of personal data controllers, in particular those controllers who are also subjects of the Law on Free Access to Information of Public Importance (public sector).

d) For **representatives of the legislative, executive and judicial power** – this analysis represents the identified weaknesses of the existing legislation, and offers some suggestions for amendments.

e) For **the media** – this Analysis will contribute to the promotion of the protection of citizens' privacy in the field of the media, and motivate the media to focus on specific cases of violation of the rights, as well as to use their reporting and research to affect the representatives of the executive and legislative authorities to improve existing regulations and implement them consistently.

f) For **other independent bodies in Serbia** – The Commissioner for Protection of Equality, the Ombudsman, as well as other independent bodies, may use some conclusions of this research in their work on cases involving the infringement of citizens' privacy.

g) For **lawyers and other representatives and legal aid providers (including free legal aid)** – As the Commissioner does not have sufficient resources to act in the protection of citizens' privacy, and the jurisdiction of this institution does not extend to certain entities (e.g. the media), this Analysis may indicate new areas in which attorneys and other representatives can and must provide adequate legal advice and legal aid to their clients, both citizens and legal entities – subjects of the Law, and motivate lawyers to specialize in the field of privacy protection, which would also improve the judicial protection against abuse of personal data.

h) For **the Commissioner** – Given that the Commissioner does not have adequate resources to carry out its mandate in the area of

22 In the Article 16 of the PDPL it is stated that particularly sensitive data involve information relating to: nationality, race, sex, language, religion, political party affiliation, union membership, health, social assistance, victim of violence, criminal convictions and sex life.

personal data protection, this Analysis can be useful for the Office of the Commissioner, as it presents in detail the practices of selected controllers regarding personal data protection. Based on the results of the research, it is possible to identify gaps in acting of the controllers, which can influence the Commissioner to use the results in its work. Also, other weaknesses of the PDPL that hamper the work of the Commissioner are acknowledged.

3.2. Research Methodology

Information for this research was collected using the Requests for exercising the rights regarding personal data processing, the Request for access to information of public importance, questionnaires and semi-structured interviews.

At the beginning of the research, the selection of the controllers was performed. Considering that the rights provided by the PDPL can only be exercised in person or through a proxy [23], 51 controllers based in Belgrade, Loznica Negotin, Nis, Novi Pazar, Novi Sad, Sabac and Valjevo, have been selected by the researchers involved in the project as they previously reported a series of controllers for which they anticipated to have some information about them. Additional criteria for the selection of the controllers was that the sample should contain not less than 30 institutions entrusted with public authority, in order to use the opportunity provided by the Law on Free Access to Information of Public Importance in the later stages of the research, to obtain additional information on procedures for processing personal data by these controllers. Furthermore, for the purpose of the research 21 controllers were selected, among those who had already received an opinion, recommendation, warning, decision or experienced supervision by the Commissioner. The intention was to identify whether after the intervention of the Commissioner these controllers comply with the provisions of the PDPL to a greater extent, in relation to the controllers where the Commissioner had not intervened. Finally, three controllers were selected, due to the complex organization and the fact that they operate across the entire country and have offices, branches, administration offices in several cities and municipalities, so they had received the request of the same content via more than one local organizational units. In this way, the research team examined whether these operators have uniform practice in acting upon requests regarding personal data processing.

23 Article 34 PDPL.

Upon selecting the sample, the researchers conducted verification of registered data filing systems in the Central Registry on the website of the Commissioner.

As a next step, the researchers, each on his/her own behalf, submitted Requests for exercising the rights regarding personal data processing[24] to the selected controllers. The utilized research technique was content analysis of the responses to the requests. Certain number of the controllers who did not respond to the request was given the opportunity to do so by submitting a repeated request.

The researchers lodged an appeal to the Commissioner in cases where the controller did not respond to the request, or if the response contained inaccurate and incomplete information that did not provide the researcher with satisfactory answers to these questions. The appeals were primarily lodged to check the functioning of the system for the protection of the rights provided in the PDPL in order to obtain the information required in the requests.

During the next phase of the research, using the responses of the controllers, the researchers developed and submitted Requests for access to information of public importance to those controllers who are subjects of the Law on Free Access to Information of Public Importance (e.g. courts, educational institutions, health centers, etc.). These controllers were required to deliver information on measures undertaken for the protection of personal data within the institution. The questionnaire of the same content was sent to the controllers who are not subjects of the aforementioned Law[25].

Finally, the researchers sent letters requesting the organization interviews. The aim of these interviews was to gather information about the shortcomings of the existing legislation in the field of personal data protection, to determine the problems controllers are facing, and present some solutions for data protection to the controllers. Semi-structured interviews with representatives of the Office of the Commissioner and the Ministry of Internal Affairs were performed, as well as with the Commissioner for Data Protection in a company with headquarters in Austria.

Structuring the research sample

As noted above, for the purpose of the research, 51 controllers from eight cities and municipalities were selected. The total of 58 Requests for exercising the rights regarding personal data processing have been sent. The difference in the number of controllers and the number of requests

24 The sample of the Request is attached.

25 The sample of the Request is attached.

appeared due to the decision of the research team to send the requests to the Ministry of the Interior in six cities and municipalities, while two requests were sent to Telenor and Commercial Bank in order to determine whether these subjects have uniform procedures and methods of responding to requests in their local administrations and offices. The research team included in the sample at least one health facility in each city, local police departments, local or national public companies and other entities for which each researcher reasonably assumed to have information about him/her. The controllers from the private sector were also selected according to the same principle.

The following controllers were selected for the research:

- **Belgrade:** Institute of Student Health, Belgrade, Health Center Vracar, Ministry of Interior, Ministry of Agriculture, Forestry and Water Management, the City Municipality of Cukarica, Faculty of Law University of Belgrade, the Public Utility Company Gradska Cistoca, Basketball club Partizan Belgrade, Department of Laboratory Diagnosis "Konzilijum", Apex Technology Solutions, the Liberal Democratic Party, the Socialist Party of Serbia, the Serbian Progressive Party, Democratic Party, G17 +, the Democratic Party of Serbia (total of 16 controllers)

- **Nis:** Department of Student Health Center Nis, Police Department in Nis, the Public Utility Company Naissus, Public Utility Company Objedinjena naplata, Primary School Ivo Andric, School of Electrics Nikola Tesla, Telenor, OTP Bank (8)

- **Novi Sad:** Health Center Novi Sad, Police Department in Novi Sad, Public Transport Company GSP Novi Sad, the Public Utility Company Informatika, Elektrovojvodina Novi Sad, City Tax Administration Novi Sad, the Republic Fund for Pension and Disability Insurance, Banca Intesa, SBB, NIS Gazprom Neft (10)

- **Novi Pazar:** Health Center Novi Pazar, Police Department in Novi Pazar, the Public Utility Company Cistoca, Company "Electrosrbija" Ltd., Kraljevo (branch of Novi Pazar), Misdemeanor Court in Novi Pazar, Commercial Bank branch Novi Pazar, Travel Agency Znak. (7)

- **Valjevo:** Health Center Valjevo, Valjevo Police Department, Telekom Serbia, the Public Utility Company Toplana Valjevo, National Health Insurance Fund, Universal Bank, Telenor, Basic Court in Valjevo (8)

- **Negotin:** Negotin Health Center, Police Station Negotin, the Public Utility Company "Badnjevo" the Public Utility Company

"Elektrotimok" Zajecar, Negotin Municipality, Commercial Bank, Travel Agency " Sedmica plus " (7)

- **Šabac:** Basic Court in Sabac (1)
- **Loznica:** Basic Court in Loznica (1)

3.3. Analysis of the research results

3.3.1. Actions of Data Controllers upon Requests for exercising the rights regarding personal data processing

Article 19 of the PDPL defines the right of the citizen to be fully and truthfully informed about the processing of his/her data by the controller, including information on:

- whether the data is processed;
- which processing action is performed;
- what data are processed;
- from which source the data was collected or who is the source of data;
- the purpose of processing data;
- the legal basis of processing data;
- in which filing systems data is included;
- whether the data is provided to someone else;
- who are the users of data;
- what is the time period of processing data (which refers, inter alia, to the retention period).

The citizens exercise this right by sending the Requests for exercising the rights regarding personal data processing to the controller. Article 24 PDPL defines that the Request must contain: *information about the identity of the applicant (name, name of a parent, date and place of birth, personal identification number), address of permanent or temporary residence, as well as other necessary contact information*. Also, it is necessary that the citizen (the applicant) provides a detailed description in connection with data processing, primarily to clarify the context preceding the data collection by the controller, so that the controller could respond to the request in the event that the data is in the non-automated filing systems of personal data. The application may be submitted by mail, e-mail or delivered to the office of the controller. Article 25 of the PDPL provides that the controller, upon receiving the request, must issue a notice of processing without

delay and no later than 15 days from the date of submission. The same article of the Law provides that, if the controller denies the request, he/she shall issue a decision with advice on legal remedies. If the controller is not processing any information about the applicant, the applicant shall be informed, and Article 32 PDPL provides that in such case the request is forwarded to the Commissioner, *unless the applicant objects*, and subsequently the Commissioner shall check whether the controller processes the requested data.

The responses obtained from the controllers are briefly presented below.

Ministry of Interior

Ministry of Interior (MoI) is the largest data controller in Serbia. On the day of the conclusion of this Analysis, the number of reported filing systems in the Central Registry on the website of the Commissioner was 126, while the MoI states that this number may be doubled in the future because the Ministry regularly enters new filing systems in the Central Registry. A large number of the filing systems are established by law.

Researchers addressed the local police stations or departments with the request including a question about the processing of personal data provided by the researchers to the MoI for the purpose of issuing identity cards or passports. Since it is a filing system that is established by law (Identity Card Law, and Law on Travel Documents), the type of data collected by the MoI is defined by law.

The request that was sent to the **Police Department Valjevo** was responded directly by that department within the prescribed time limit. The response stated that data processing for the purpose of issuing identity cards was performed on the basis of the "voluntary consent", which was not quite correct as the Identity Card Law stipulated that every citizen is obliged to have an ID, and consequently had the obligation to provide the required data to the Ministry of Internal Affairs in order to issue the ID. Hence, this case does not involve personal data processing on the basis of consent. It is further stated in the response that the information given by the researcher was in the "written and electronic form" and "it is kept in a unique information system of the Ministry of Interior of the Republic of Serbia, and under Article 12 and 13 of the Law on Personal Data Protection, may be used or processed by other state authorities without your consent".

The reference to Articles 12 and 13 PDPL as a basis for data processing without individual's consent is interesting because of the content of these provisions, since the parts of these provisions have been found by the

Constitutional Court as inconsistent with the Constitution[26]. The Constitution of the Republic of Serbia in the Article 42 stipulates that data processing can be performed only on two grounds – if it is prescribed by specific law or with the consent of the individual. The cited provisions of the PDPL provided the opportunity to data controllers, including the MoI, to process personal data of citizens without consent and without legal basis for the purpose of carrying out activities within "*its jurisdiction*" defined by "other regulation". It is therefore important that the MoI harmonize its bylaws with the decision of the Constitutional Court without delay. However, practice demonstrates that some of these bylaws are still in force and acted upon. For the purposes of this study, one such bylaw is cited – Instruction on the method of collection, processing, recording and using data from the Ministry of Interior that entered into force in 1998, which is classified as a top secret document, so it is not accessible to the public (see the response of the PU Valjevo to the Request for access to information of public importance that is attached below).

Police Department in Novi Pazar responded to the request within the statutory deadline. The researcher was informed that the police entered the records into the central registry and that the answers to the requested information could be found there, which was generally a satisfactory answer, since the purpose of the Central Registry implied that a citizen could find answers to questions about data processing without sending a request to the data controller. However, it is recommended to provide the applicant with the answers to a request, not just refer him/her to the registry. A response with a similar content was submitted by **the Police Department Nis**, while **the police station in Negotin** responded in a similar manner six days after the expiry of the deadline (application submitted in person at PS Negotin on 9th October, the response made on 30th October and delivered by mail 7th November 2012). Since the answer had an overall satisfactory content, the researcher did not lodge an appeal to the Commissioner due to late submission.

Response with analogous content was also delivered to the researcher from Novi Sad, but in this case **the Police Department Novi Sad** forwarded the request to **the Bureau for information of public importance at the Ministry of Internal Affairs** and informed the researcher in a written form. In response by the Bureau, it was stated that all the answers to the questions in the request could be found in the appropriate filing system in the Central Registry on the website of the Commissioner.

The researcher from **Belgrade** addressed the Ministry of Internal Affairs of the Republic of Serbia through a request seeking information on whether the MoI had data about him, as a holder of a season pass of a sports club, as he had been informed by the club that the data about him had been collected by the club but then forwarded to the MoI. Ministry of Interior stated in the

26 The decision of the Constitutional Court of the Republic of Serbia 68/2012, http://www.uzzpro.gov.rs/doc/biblioteka/BiltenBr7-2012.pdf

response that they did not have these data about the researcher. This area was explored in detail and presented in the part related to the Case study II.

From the above, it is evident that the practice of acting of the MoI upon the Requests is partially harmonized. The answers have satisfactory content, but it is perceived that some of the Police Departments respond to requests themselves, while others forward the requests to the Bureau for Information of Public Importance. The researchers discussed this with a representative of the Ministry of Interior, which would be addressed in more detail in the following analysis.

The courts

This research included: the Basic Court in Valjevo, Basic Court in Loznica, Basic Court in Sabac and Misdemeanor Court in Novi Pazar.

The basic courts in Valjevo, Loznica and Sabac were approached by the researcher who cooperated with these courts as a court interpreter. The response of **the Basic Court in Sabac** represents an example of good practice[27], as the request of the researcher has been responded to promptly, thoroughly and systematically, with a very detailed explanation in response to all the questions asked.

On the other hand, the responses of **the Basic Court in Loznica** and **the Basic Court in Valjevo** were not adequate. These courts informed the researcher that they did not process any data about her. The researcher had been cooperating with these courts for years in the same way as with the Basic Court in Sabac, and had therefore expected a response of the same or similar content. Thus, she lodged an appeal against these data controllers to the Commissioner. Subsequently, the Office of the Commissioner informed the researcher that the Basic Court in Valjevo and Basic Court in Loznica did not submit the request to the Commissioner's, even though it was the obligation of the controller when not processing data about the applicant.[28] Acting of the Commissioner upon these appeals is in progress.

Misdemeanor Court in Novi Pazar stated that it did not have the data about the researcher, because the data on the researcher "do not appear in the last two years", which was the moment when automated data processing was established in this Court. However, the court failed to inform the Commissioner about this response, which was the obligation of the controller when not processing data of the applicant[29].

---

27 Response is attached.

28 Article 32 PDPL: "When the controller is not processing the data, it shall forward the request to the Commissioner, unless the applicant objects."

29 Ibid.

Health system

Health Center Negotin did not respond to the request within the prescribed time limit. Repeated request was sent by another researcher which was answered in a satisfactory manner. The response states which information the health center has, that the ID number of the researcher is used for statistical purposes and to perform the activities of the institution, that the institution has medical records of the researchers and that this data is transferred to the branch of the RFZO with which the health institution signs an agreement each year for the provision and financing of health care services as a part of compulsory health insurance, in line with the Law on Health Insurance. It is also stated that the termination of insurance results in ending of data processing, and delivery of data from the medical records of the patient to the competent authorities is provided by Article 37 of the Law on Health Care.

Health Center Novi Sad responded in due time but the response consisted of a series of citations of several laws and bylaws that govern personal data processing, without answering the specific questions from the request. The researcher lodged an appeal which was accepted by the Commissioner and the controller was ordered to submit full and truthful response.

Health Center Valjevo responded to the request of the researcher in due time and the response contained the required information.

Department of Student Health Nis responded to the request within the prescribed time limit, but the response contained contradictory and inaccurate information. The response stated that the Department did not process information about the researcher. However, the statement in the response that the data from the researcher‘s medical records is exclusively available to "the chosen physician" of the researcher, denying the aforesaid institution‘s statement that it does not process data on the researcher, since the processing of personal data implies different actions, including data storage and access to the data. Upon the new request, in which the researcher drew attention to the institution, that he was not satisfied with the response, providing the controller an opportunity to reconsider the request, the response contained the same contradictions. The researcher lodged an appeal to the Commissioner.

Health Center Vracar informed the researcher that the verification of the protocol found that there were no data about him, which was accepted as a truthful answer by the researcher. However, the health center failed to refer the response to the Commissioner, which was its obligation if it had no data about the applicant.[30]

Health Center Novi Pazar responded to the request incompletely. The response states that the health center has the researcher’s medical

30 Article 32 PDPL.

record, which is only available to the health center services, and it is not used for other purposes.

Department of Student Health Belgrade, also responded that they did not process data on the applicant, although the response stated that they had certain data about the applicant and that the data was archived. After receiving the response, the researcher also drew attention of the Department to the contradictions in response. Subsequently, the Department sent a full and truthful response to the request, containing the answers to all the questions.

Education

Faculty of Law, University of Belgrade was approached by the former student of the Faculty, demanding to be informed whether the Faculty processes some data about her, which data is processed, on what legal basis, and what are the retention periods of data on former students. The response of the Faculty was unsatisfactory; since it initially stated that the faculty did not process any data on this former student, however, also noting in the response that data about her was archived. The answer was contradictory, but the researcher decided not to lodge the appeal to the Commissioner, as part of the response contained answers to some of these questions. In any case, it can be concluded that data controller is not fully familiar with the contents of the Law, which may cause concern, taking into account the volume of data it is expected to possess and the fact that it is the largest institution for education of lawyers in Serbia.

The School of Electrical Engineering Nikola Tesla in Nis replied as follows, "In relation to your Request for information of public importance and information on the protection of personal data, we inform you that we do not process any information about you [...]." First of all, it is not clear why the data controller refers to the Law on Free Access to Information of Public Importance. However, it is further stated in the response that the information about the researcher could be found in the school book that was permanently stored, the data was not available to others, except upon personal request or ex officio to the authorized bodies in accordance with law and evaluating each case. Even though the response contained contradictions, an appeal was not lodged to the Commissioner because the researcher concluded that the response provided the answers to several questions from the request.

Elementary School Ivo Andric in Nis did not respond to the request and the researcher lodged the complaint to the Commissioner. The Commissioner‘s decision ordered the school to respond to the request, and the school did so. The response contained the information requested by the researcher.

Public and Public Utility Companies and Public Institutions

Republic Health Insurance Fund provided detailed answers to all the questions of the researchers within the prescribed time limit.

Republic Fund for Pension and Disability Insurance stated in the response that the Fund kept several records, including the records that were not registered in the Central Registry. The Fund refers to "records on the facts that have an impact on the acquisition and exercise of rights under this insurance", which is not registered in the Central Registry. Since the researcher did not receive answers to the questions, nor was he able to receive them by searching the registry, he lodged an appeal to the Commissioner. The Commissioner upheld the appeal and issued a decision ordering the data controller to respond to the request.

Public Enterprise Elektrotimok Zajecar fully responded the request within the prescribed time limit.

The Public Utility Company Badnjevo in Negotin did not respond to the request and the researcher lodged an appeal to the Commissioner.

The Public Utility Company Naissus in Nis responded to all the questions from the questionnaire, and provided specific information held about the applicant.

The Public Utility Company Objedinjena naplata in Nis responded to all the questions from the questionnaire, but the response contained certain contradictions, primarily as to the meaning of the term "data processing". This company states that "the data about you is processed for the purpose of records keeping and printing bills [...] as well as for the delivery of the bills" and data is kept "in the database in our headquarters." It is than stated that the institution "does not perform any data processing about you." However, the researcher was able to gain insight into the methods of processing information of the data controller from the response obtained.

Elektrovojvodina Ltd. from Novi Sad fully responded to the request within the prescribed time limit.

Telekom Serbia stated in the response that "it does not process any of the service users". However, further in the response it is stated that the data controller has data on the applicant, the source of data is provided, as well as the purpose of processing and the conditions under which the data is provided to a third party. The researcher obtained the answers to some questions, but it was concluded that the data controller was not sufficiently familiar with the PDPL concerning the meaning of certain terms. The researcher repeated the request seeking answers to all the questions, but the response was not received due to which a complaint was lodged to the Commissioner.

The Public Utility Company Gradska čistoća Novi Pazar provided the data it held on the applicant in the response, stating that this data is not transmitted to third parties and that it is "not used for any purpose," which

is a rather unusual formulation, as in the case of termination of the purpose of processing data, the reasons for deleting data would arise.

The Public Utility Company Gradska čistoća in Belgrade, responded to all the questions in the request, but provided contradictory information that the data "is not processed and is used exclusively in the service of public relations and marketing."

The Public Enterprise PTT "Serbia" provided the answers to all the questions in a detailed response to the request.

Public transportation company "Novi Sad" responded that the required information could be found in the records that had been reported to the Commissioner and were registered in the Central Registry. However, the applicant was not referred to a specific record. Instead, the list of records that are registered in the Central Registry was given. However, in spite of the incomplete responses, by searching the Registry, the researcher obtained the answers to the issues raised.

The Public Utility Company Informatika provided detailed response listing all the required information.

A company "Elektrosrbija" Ltd. Kraljevo, branch ED Novi Pazar responded to all questions in the request.

The Public Utility Company Toplana – Valjevo is not fully aware of the meaning of certain terms of the PDPL, particularly as to the meaning of the term "data processing", but the response contained all the necessary information.

City tax authority of Novi Sad has fully responded to the researchers' request.

State administration and local self-government

Negotin Municipality fully responded to the request of the researchers.

City Municipality Čukarica forwarded the request of the researchers to the Public Attorney's Office of this municipality. The response stated that the PDPL does not apply to the researcher's data processed by the municipality, "since it involves information that is available to everyone and published in the public paper, in line with the Article 5 of the PDPL". However, the response did not specify to which data this information applies, in fact, it did not specify what data the Municipality has about the researcher and whether the scope of the data is equal to the scope published in the public paper.

Ministry of Agriculture, Forestry and Water Management provided a full and truthful response to the request. The response contained the answers to all the questions from the request, and enclosed a copy of the submitted data that this Ministry has on the researcher, stating the specific registry where the data is located.

Political parties

The Requests for exercising the right regarding personal data processing were submitted to: Serbian Progressive Party, Democratic Party, the Socialist Party of Serbia, G17 + (which still operates as a separate political entity), the Liberal Democratic Party and the Democratic Party of Serbia. The Requests contained the question whether the party had data on the applicant in the copies of the voters' lists or other collections of data on voters. The Request specifically stated the municipality in which the researcher was entitled to vote, in order to facilitate the data controller to act upon the request, if the controller considered that consulting the local municipal board for preparing the response was necessary.

The request was responded to within the prescribed time limit by the Socialist Party of Serbia and the Democratic Party, while the remaining four parties failed to do so, which was why the researchers lodged an appeal to the Commissioner against the Serbian Progressive Party, G17 +, the Liberal Democratic Party and the Democratic Party of Serbia.

In response of the Democratic Party it is stated that it does not have any information about the researcher. It is also stated that the filing system on party members is the only data collection owned by this controller. However, it seems that this is not entirely true, because data collection on staff also represents a collection of personal data that the Democratic Party certainly has[31].

In response of the Socialist Party of Serbia, it is stated that this party does not have any information about the researcher, other than the data collected by the reception of the request.

Commercial subjects (banks, mobile phone operators, travel agencies, etc.)

The researchers sent two requests of the same content to the **Commercial Bank**. Both branches, in **Negotin** and **Novi Pazar**, have provided satisfactory and complete answers to the questions, citing the information requested.

Universal Bank provided complete answers to all the researcher's questions and thoroughly informed the researcher.

OTP Bank fully responded to the researcher's request.

Banca Intesa has responded to all questions in the request.

Telenor was sent two requests. In the response of the call center, the applicant is referred to the contract signed by Telenor and the user, which

31 http://www.danas.rs/danasrs/politika/tadic_zaposlen_u_ds_plata_148000_dinara.56.html?news_id=251893

defines the area of the use of data. It is also stated that Telenor is not phone tapping the users or reading SMS communication. At the request sent from Valjevo, no response was received. The researcher lodged an appeal to the Commissioner, upon which the Commissioner ordered Telenor to respond to the request, which Telenor did shortly after, delivering the response to all the questions in the request.

Travel Agency Znak in Novi Pazar fully responded to the request. The response states that the data on the client is deleted "upon realization of the arrangements and covering of the material costs."

Travel agency "Sedmica +" from Negotin responded to all questions in the request. The response states that the data is "processed until the expiry of the arranged services and the only data that remain in our archives is the data in the travel certificate".

Serbia Broadband (SBB) stated in the response that the requested data could be found in the relevant filing systems that were registered in the Central Registry. It also said that the contract signed between the applicant and the SBB defined the area of personal data processing in detail, but this data controller correctly decided to provide all the answers to the questions.

Department of Laboratory Diagnosis Konzilijum stated that the field of data processing is regulated by relevant laws on records keeping in the field of health and health care and adequate bylaws adopted in line with such laws. The response also stated that the controller "keeps proper records, but does not perform any processing of the data, neither about you (the applicant, author's comment), nor for the patients, as there is no need to do so." The response did not contain answers to all the questions in the request, but the researcher was able to gain insight regarding the regulations which should be consulted in order to answer the questions raised in the request.

Apex Technology Solutions has responded to the request, specifying the data it holds on the researcher. It was also stated for which purpose the information was used, and that it was not provided to third parties.

Basketball club Partizan informed the researcher that it did not have any data about him, in fact, that it had forwarded data to the Ministry of Interior shortly after collecting them.

Taking into account the obtained responses to the Requests of the researchers, the following can be concluded:

- A significant number of data controllers are not familiar with the meaning of certain terms of the Law. This particularly refers to the term processing (personal data), which, as it turned out, is often misinterpreted or not understood by a significant number of data controllers. Such data controllers, probably intuitively, consider that storing, securing and archiving data, represent actions that

do not involve physical manipulation and editing, and not data processing, which is wrong. Due to such interpretation of the term, data controllers tend to respond that they do not process data on the applicant, and are therefore unable to provide answers to questions about the retention period, processing operations, the legal basis and the purpose of processing, which makes their response incomplete and inaccurate.

- Furthermore, the method in which the data controllers acted while considering the received requests, gives the impression that a number of data controllers did not have experiences with such requests until then. One data controller forwarded the request to the competent Public Attorney; the second returned the request to the applicant noting that in its submission the addressee was not named, etc. Unlike the Law on Free Access to Information of Public Importance, which has been in force since 2004 and has widespread use, the Law on Protection Personal Data is still insufficiently known by the citizens and data controllers, so the data controllers have not yet developed adequate procedures for handling incoming requests. The responses often indicated that the subjects had a person authorized to act upon the requests for access to information of public importance, but they did not have the person authorized to act upon the requests stipulated by the Law on Personal Data Protection. Therefore, one of the conclusions is that that each data controller should determine specific service or person to act upon such requests.

- Some data controllers believe that the request should be answered by referring to the laws that govern personal data processing related to the issues in the request. Instead, complete and truthful response should contain specific answers to the questions in the request, that is, it is necessary to specify which data controller has, which processing actions are undertaken, which are the retention time limits, etc.

- Finally, it is noted that data controllers in the private sector tended to show a higher degree of awareness of their own obligations under the Law, even though there were also examples of good practice in the public sector. The authors of the publication believe that due to business market, where customers can be won or lost, private subjects have an incentive to coordinate their actions with the provisions of the PDPL. However, it must be noted that the provision of complete and accurate responses to the request for exercising the right does not necessarily mean that the controller is completely lawful in acting with personal data of their clients, customers or employees.

3.3.2. Actions of the Commissioner upon Appeals

Article 38 of the PDPL stipulates that the applicant may file an appeal regarding processing [of personal data] to the Commissioner. Article 39 PDPL defines the acting of the Commissioner upon appeal in more detail. This article, inter alia, envisages that "the Commissioner decides upon appeal within 30 days from lodging the appeal." Throughout the implementation of the project, the researchers filed 14 appeals to the Commissioner. Compared to the 58 submitted requests, the appeals were filed in 24% of cases, indicating that a high percentage of the selected data controllers were not aware of their obligations. The number of appeals could have been even higher, as in several cases the requests were repeated because there was no response to or because the response contained some contradictions or false statements. Considering that the Commissioner has very limited resources, the intention of the researchers was not to file an appeal in every case that contained some flaws, but it was done only when the request had not been answered at all, or if the response prevented clear identification of the data controllers' methods of processing the researcher's data. Table 1 demonstrates actions of the Commissioner upon appeals.

Table 1: Actions of the Commissioner upon appeal

Data controller	Reasons for the appeal	Date of the appeal	Actions of the Commissioner	Date of the Commissioner's Decision
Elementary school Ivo Andrić, Niš	Data controller did not respond to the request	13.11.2012.	The Commissioner submitted a copy of the request and the appeal to the data controller for comment and instructed the data controller to respond to the request.	28.11.2012.
Telenor	Data controller did not respond to the request.	13.11.2012.	The Commissioner accepted the appeal, and issued a decision ordering the data controller to respond to the request.	26.11.2012.
Department for Student Health Niš	Response of the data controller is incomplete and untruthful.	28.11.2012.	11/3/2013 The Commissioner informed the researcher that due to the excessive number of cases, the appeal was not resolved	
NIS Gazprom Neft	Data controller did not respond to the request	29.11.2012.	The Commissioner accepted the appeal, and issued a decision ordering the data controller to respond to the request.	23.1.2013.
Helth center Novi Sad	Response of the data controller is incomplete.	5.12.2012.	11/3/2013 The Commissioner informed the researcher that due to the excessive number of cases, the appeal was not resolved.	

Data controller	Reasons for the appeal	Date of the appeal	Actions of the Commissioner	Date of the Commissioner's Decision
Republic Fund for Pension and Disability Insurance	Response of the data controller is incomplete.	5.12.2012.	The Commissioner accepted the appeal, and issued a decision ordering the data controller to respond to the request.	11.3.2013.
Public utility company Badnjevo, Negotin	Data controller did not respond to the request.	6.12.2012.	The appeal has been lodged, but until the day of the conclusion of this analysis it is not known whether the appeal has been acted upon.	
Telekom Serbia	Response of the data controller is incomplete. The repeated request was not answered.	20.12.2012.	11/3/2013 The Commissioner informed the researcher that due to the excessive number of cases, the appeal has not been resolved.	
Basic court in Valjevo	Response of the data controller is incomplete and untruthful.	25.2.2013.	The appeal has been lodged, but until the day of the conclusion of this analysis it is not known whether it has been acted upon.	
Basic court in Loznica	Response of the data controller is untruthful.	25.2.2013.	The appeal has been lodged, but until the day of the conclusion of this analysis it is not known whether it has been acted upon.	
Liberal Democratic Party	Not responded within statutory deadline.	25.3.2013.	The deadline for acting of the Commissioner upon the appeal has not expired.	
Democratic Party of Serbia	Not responded within statutory deadline.	25.3.2013.	The deadline for acting of the Commissioner upon the appeal has not expired.	
Serbian Progressive Party	Not responded within statutory deadline.	25.3.2013.	The deadline for acting of the Commissioner upon the appeal has not expired.	
G17+	Not responded within statutory deadline.	25.3.2013.	The deadline for acting of the Commissioner upon the appeal has not expired.	

Throughout this research, processing of appeals was the subject of discussions with the Commissioner on several occasions. The annual European Commission Progress Reports on Serbia of 2009 when the Commissioner for Information of Public Importance expanded authority in the field of protection of personal data, reported that "The office of the commissioner lacks staff and funding, which prevents effective supervision."[32]

32 See European Commission Progress Report on Serbia in *2009*, available at http://www.seio.gov.rs/upload/documents/sporazumi_sa_eu/progress_report_2009.pdf, page 55.

Similar statements were repeated in the reports for 2010[33], 2011[34] and 2012[35] indicating that inadequate resources represented a continuous problem that institution faced. The report of the Commissioner for 2011 supported that "due to a lack of suitable premises, the Commissioner is unable to employ anyone other than to replace those who departed, even though the actual work requires it, and systematization, staffing plan and allocated resources allow so".[36]

Unfortunately, even in 2012, there was no progress in this area. According to the Monthly Statistical Report, [37] the Office of the Commissioner, on 28 February 2013, resolved the total of 18,265 cases, with a total of 2865 cases from both areas of its jurisdiction in progress. Only in February 2013, the Commissioner received 428 new cases, 106 of which were in the field of personal data protection. Through communication with the Commissioner's Office, the researchers found out that "[...] up to date, there have been no changes in terms of premises in which the Commissioner works, which means that there are a total of 44 employees, including elected officials, working in less than 500m² on two locations with inadequate conditions and monitor the implementation of the Law on Access to Information of Public Importance and the Law on Personal Data Protection.

The Rulebook on internal organization and job classification in the Office of the Commissioner, has the total of 69 employees systematized. This number does not include elected officials.[38] The Office of the Commissioner indicated that due to these housing conditions, this institution is unable to fill the systematization so that the monitoring of the implementation of the Law on Personal Data Protection is currently performed by the total of 12

---

33 European Commission Progress Report on Serbia in *2010* available at http://www.seio.gov.rs/upload/documents/Izvestaji/serbia_2010_progress_report.pdf, page 55.

34 *Analytic Report following the Notice of the Commission to the European Parliament and the Council – Commission Opinion on Serbia's application for membership in the European Union*, available at http://www.seio.gov.rs/upload/documents/eu_dokumenta/misljenje_kandidatura/sr_rapport_2011_en.pdf, page 104.

35 European Commission Progress Report on Serbia in *2012* available at http://www.seio.gov.rs/upload/documents/eu_dokumenta/godisnji_izvestaji_ek_o_napretku/sr_rapport_2012_en.pdf, page 51

36 Report of the Commissioner for 2011: http://poverenik.rs/sr/o-nama/godisnji-izvestaji/1332-izvestaj-poverenika-za-2011-godinu.html, page 48.

37 http://poverenik.rs/index.php/sr/o-nama/mesecni-statisticki-izvestaji/1542-zbirni-mesecni-statisticki-podaci.html

38 In the period between October 2012 and March 2013 the research team had several interviews with representatives of the Commissioner's Office, such as the deputy Commissioner Aleksandar Resanović and Secretary General Marinko Radić. The cited statements were given during these discussions.

individuals, while there is 21 staff systematized. This number of employees should monitor the implementation of the Law of over 300 thousand objects of supervision (controllers). The research team once again emphasizes that many controllers process data in multiple locations, while others, due to their complex organizational structures, have dozens, even hundreds of branches, departments, management, stations, local offices, sectors, and other organizational units that also process personal data, which indicates that data on citizens is processed in over a million places in Serbia, which should also be taken into account when evaluating the work of the Commissioner. Regarding the lack of funds, it is important to note that this is not necessarily a lack of financial resources. The Office of the Commissioner also stated that the institution was unable to hire new employees, because it actually lacked the space for desks and chairs. Restricted working conditions also prevent the Commissioner to develop and advance its competence. The minimum acceptable conditions for the Commissioner at this stage would be to have at least 25 officers in the supervision, while this number would certainly have to increase during time if we wish for quality and efficient protection of personal data.

This research empirically confirms that the Commissioner, with the current available capacity, cannot fully fulfill its mandate. In other circumstances, the fact that the Commissioner has been processing the four complaints filed during the present research for over three months (against the Department of Student Health Center Nis, Novi Sad of Health, the Public Utility Company Badnjevo Negotin and Telekom Serbia), would be a reason for criticism of this institution. However, due to the aforementioned reasons and without any fault, the Office of the Commissioner is unable to employ the necessary number of employees, although there are funds in the budget, so this institution has not been not fully realizing its budget for several years and the remaining funds will be transferred to the budget of the Republic of Serbia[39]. While this may appear to be the saving of public funds, it must be noted that, due to the failure of the executive branch to provide the Commissioner with the appropriate premises, these "savings" are achieved at the expense of the citizens' privacy.

3.3.3. Actions of data controllers upon the decisions and orders of the Commissioner

During the implementation of the project, the Commissioner ordered the controllers to respond to the request four times. Until the date of finalization of this Analysis, all the four controllers acted in line with

39 More details can be found in the annual report of the Commissioner. The report for 2011 indicates that during the last year the Commissioner utilized around 45% to 74% of total approved funds. The report for 2011, page 48

the orders and decisions of the Commissioner. These four cases indicate the importance of the institution of the Commissioner for Personal Data Protection, as the citizens would be unable to protect their privacy without such second-instance body. In all the four cases, the responses from the controllers appeared shortly after the Commissioner's decision.

Table 2: Actions of data controllers upon the orders and decisions of the Commissioner

Data controller	Actions of the Commissioner	Date of the Commissioner's Decision	Actions of data controllers
Elementary school "Ivo Andrić", Niš	The Commissioner submitted a copy of the request and the appeal to the data controller for comment and instructed the data controller to respond to the request.	28.11.2012.[40]	Data controller acted in line with the Commissioner's order and on 20/11/2012 delivered the response to the applicant.
Telenor	The Commissioner issued a decision ordering the data controller to respond to the request.	26.11.2012.	Data controller acted in line with the Commissioner's decision and on 4/12/2012 delivered the response to the applicant.
NIS Gazprom Neft	The Commissioner issued a decision ordering the data controller to respond to the request.	23.1.2013.	Data controller acted in line with the Commissioner's decision and on 6/2/2013 delivered the response to the applicant.
Republic Fund for Pension and Disability Insurance	The Commissioner issued a decision ordering the data controller to respond to the request.	11.3.2013.	Data controller acted in line with the Commissioner's decision and on 20/3/2013 invited the applicant to gain insight of the data.

3.3.4. Actions of the Data Controllers regarding the data collections entry into the Central Registry on the website of the Commissioner

Central Registry involves filing systems of personal data established and maintained by the Commissioner in order to provide citizens with information on the data processing about them. The search of the Registry, located at the website of the Commissioner[41], enables the citizens to find out what data is processed by the controller, how and for what purpose.

40 The Commissioner stopped further actions upon appeal as of 28/11/2012 since the data controller acted in accordance with the order.

41 http://poverenik.rs/registar/

The obligations of personal data controllers in regards to the Central Registry are defined in the Articles 48-52 of the Law on Personal Data Protection. Briefly, the controller is required to establish and maintain records on data processing, to deliver records of the filing systems to the Commissioner or announce the establishment of a new filing system by giving notice to the Commissioner. Article 57 of the PDPL stipulates the sanctions in the event of acting contrary to the Law.

The reporting filing system is a basic duty of each controller, and it can concurrently represent an indicator of the level of awareness of the controller's obligations in the field of personal data protection of its customers, clients or employees. In addition, the procedure of reporting the filing systems in the Central Registry is an effective way to familiarize the authorized persons who process personal data at the controller with the provisions of the Law on Personal Data Protection and may motivate the controllers to improve internal procedures for processing the data about their customers, clients and employees. When entering data in the Central Registry, the controller often considers for the first time: whose personal data I am processing, which processing actions I perform, do I have a legal basis for data processing, have I defined the retention period for the storage and use of data, have I undertaken adequate measures to protect the data, etc.

The Law on Personal Data Protection, Article 48 Para 2 provides that "Controllers shall not be required to set up and maintain records for the processing of [...]data processed for the purpose of maintaining registers required by the law; " (for example: birth registry, the data of the Agency for Business Registers, records in health care, voting lists, etc.). This means that the controllers are not required to report these records to the Central Registry, which may bring into question the purpose and scope of this registry, as citizens are unable to obtain information about the processing of their personal data in one place by searching the Central Registry.

Although reporting existing filing systems to the Commissioner represents a legal obligation, the number of controllers who fulfilled this obligation is very small. Among the estimated 300,000-350,000 controllers, until 28th February 2013, this obligation was fulfilled by only 888 controllers[42], i.e. less than three per thousand of the total number of the controllers, who entered the total of 4.915 data collections in the Central Registry.

In regards to the selected sample for this research, it is noted that the percentage of the controllers in the sample who reported data collections is significantly higher than the aforementioned percentage of all data controllers in the territory of the Republic of Serbia. The total of 27 controllers in the sample was registered, while 24 controllers were not.

---

42 Data available at: http://poverenik.rs/index.php/sr/o-nama/mesecni-statisticki-izvestaji/1542-zbirni-mesecni-statisticki-podaci.html

The authors believe that the information whether the controller has reported at least one filing system in a Central Registry can be an indicator to assess the level of awareness of the controller in terms of its obligations under the PDPL. In this context, it is of concern that, within the selected sample, the researchers had to lodge 14 appeals to the Commissioner, that is, in every fourth case.

3.3.5. Analysis of the internal acts/regulations of the Data Controllers and undertaken measures of personal data protection

The Law on Personal Data Protection stipulates in Article 47:

> *Data must be adequately protected from abuse, destruction, loss, unauthorized alterations or access.*
>
> *Controllers and processors shall take all necessary technical, human resources and organizational measures to protect data in accordance with the established standards and procedures in order to protect data from loss, damage, inadmissible access, modification, publication and any other abuse, as well as to provide for an obligation of keeping data confidentiality for all persons who work on data processing.*

Each data controller is obliged to protect personal data against abuse, destruction, loss, alteration or unauthorized access. Referring to the established standards and procedures, the legislator established the obligation of the controllers to get familiarized with international and national legal framework for personal data protection, stipulating therefore that each data controller must undertake technical, personnel and organizational measures to protect the data from the aforementioned actions. The legislator also provides that each data controller must determine the liability of persons who process data to maintain the confidentiality of data. This applies to any person who, in the course of their work, comes into any contact with the personal data of the citizens. The researchers examined whether and how data controllers comply with these statutory obligations.

The Law on Personal Data Protection does not envisage the obligation of the controllers to precisely determine the internal regulations on the method of processing personal information of clients and employees. However, these internal documents are certainly preferable, in order to enable the controller to make the first step towards fulfilling the obligations defined in the Article 47 of the Law. These regulations may prescribe who has the access (insight) into certain collections of personal data, the

transfer of personal data to third parties, etc. This method would increase the liability of persons who are in daily contact with personal information, reducing the discretion in their work and thus preventing potential abuse. It is of major importance to regulate this area for those controllers processing particularly sensitive personal data, which have a higher degree of protection, in accordance with Articles 16-18 of the PDPL.

In regards to protective measures, they are primarily related to relevant, current ISO standards (ISO 27001). However, such measures must be established by the controller and therefore the recommendation of this analysis is that controllers, especially those processing data of a large number of citizens, or particularly sensitive personal data, should specify a particular person competent for personal data processing in an internal bylaw; similar method is used for Law on Free Access to Information of Public Importance , where a person is delegated to act on behalf of the institution under this Law. Draft of the new Regulation on data protection in the European Union[43], provides the obligation of the "large data controllers" to establish the position of Data Protection Officer within the controller‘s office, which is an obligation that will eventually be prescribed for these controllers in the Republic of Serbia as well, in the process of harmonization of the legal framework with acquis communautaire.

In terms of the legal obligations of protection of personal data, it is necessary to protect the data from *destruction* (fire, flood, etc.). When the controller provides measures to protect data from destruction, this usually involves measures that do not relate only to the personal data, but also to all the documents relevant to the institution. However, the duty to protect personal data from *unauthorized access, alteration, disclosure and any other misuse* requires additional efforts not only in terms of security of the documents overall, but also in terms of the privacy of citizens (customers, employees).

Measures that can simultaneously ensure privacy of the users and security of data may include, for example: a user‘s password, safeguards against data theft, data protection against unauthorized access, etc. This area can be comprehensively arranged by making a privacy policy at the level of the controller. Such an act may constitute an umbrella act that governs the necessary actions to be performed in the area of privacy protection within a particular controller. Such privacy policy should include the standards for the protection of personal data of customers and employees. After adopting such general act, other compliant regulations can be made to prescribe procedures for processing of personal data within an organizational unit, bearing in mind the limits defined by the law, related primarily to the principles of proportionality and appropriateness of personal data

43 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

processing. Specific instructions can inform the employees how to process personal data. Such regulations must be sufficiently understandable and in this context rewriting the legal provisions should be avoided; instead, the specific field of personal data processing should be defined as clearly as possible. Also, internal documents can prescribe that persons authorized to act in line with the PDPL have certain obligation of continuous professional development in the field of personal data protection, for which the necessary resources should be made available. Also, it is beneficial to periodically organize trainings for all employees who process personal data of customers and employees.

Institutions included in the survey, which are subject to the Law on Free Access to Information of Public Importance, were sent the Request for access to information of public importance, which required them to state and provide information about internal procedures and regulations governing personal data processing, and specify data protection measures that have been implemented so far. Commercial entities were sent a questionnaire with the same content, to which they were not obliged to respond.

The institutions that did not submit responses within the prescribed time limit are: Health Center Vracar, Health Center Valjevo, Elementary School Ivo Andric in Nis, Faculty of Law in Belgrade, the Basic Court in Sabac, City tax administration Novi Sad, Public Utility Company Naissus from Nis, the Public Utility Company "Badnjevo" Negotin, Public Company "Elektrotimok" Zajecar, the Public Utility Company Toplana Valjevo, "Elektrosrbija " Ltd. Kraljevo. Against the institutions that did not submit a response upon the Request for access to information of public importance, an appeal will be lodged to the Commissioner[44].

Among the 7 questionnaires sent to the companies throughout this research (Telenor, OTP Bank Serbia Broadband (SBB), NIS Gazprom Neft, Banca Intesa, Commercial Bank, Travel Agency Znak, only one verbal response was received (Banca Intesa), referring the researchers to the reported filing systems in the Central Registry on the website of the Commissioner.

Below we present the protective measures undertaken by the institutions, as well as the content of internal regulations that govern the processing of personal data, based on the responses given by the participating institutions.

44 The appeals will be filed on the basis of the Law on Free Access to Information of Public Importance and thus are not subject to this analysis.

The Ministry of Interior (MoI)[45] is the largest data controller in Serbia; it has the largest number of data collections, and these collections often contain information about a large number of citizens. Members of the Bureau of Information of Public Importance of the Ministry of Interior have visited almost all police departments, and organized one-day trainings for all officers at all levels in the police offices, police stations and outposts, while training also covered all those who may come into contact with requests for access to information of public importance or other requests that can be addressed in line with the PDPL. It was determined who is acting in a particular case, with defined responsibilities and powers. Also, all organizational units have access to the intranet, containing all the issued documents regarding personal data protection, PDPL in particular, as well as guidelines and manuals published by the Commissioner. Internal act of the Ministry was used to inform all the relevant persons about the location of these documents and methods of accessing them. As far as responding to the request, the MoI established a rule that when the request relates to data processing of a certain police department, only that police department must act upon request. When it comes to a more complex matter or the jurisdiction of several organizational units is recognized, the request is forwarded to the Bureau of information of public importance that corresponds to the request. By submitting the requests to local police departments, the researchers sought to determine whether there is a consistent way of responding, and the conclusion of this analysis is that the area of responding to the requests is well regulated by the internal documents of the MoI; there are, however, some cases characterized by occasional divergences, which can be attributed to the fact that the field of personal data protection is extremely complex, and that the MoI consists of a large number of organizational units which, naturally, leads to some deviations.

Moreover, it is important that the MoI is trying to harmonize the acting of its organizational units, not only upon the request of the citizens to exercise their rights in regard to the processing of personal data, but also in cases when the Ministry is addressed by other entities, mostly government authorities, asking the MoI to provide them with information about citizens. This is mainly done by public utility companies, institutes, funds and other institutions. The Ministry developed guidelines for acting upon such requests, which have been forwarded to the organizational units.

The MoI reported that the protection of personal data has been improved in collaboration with the Commissioner. Collaboration referred to the provision of opinions, especially in the first year of the PDPL implementation when this area was completely new, and there

45 Acting of the Ministry of Interior regarding data protection was the topic of conversation with Jasmina Vasiljevic, Chief Inspector and Chief of the Bureau of Information of Public Importance in the MoI.

was not enough relevant literature and manuals. Representatives of the Commissioner had provided support to the MoI in developing bylaws. The Commissioner has repeatedly conducted monitoring in the MoI. The case of monitoring regarding an incident near the hall "Arena"[46] had advanced the field of handling video surveillance equipment, and as supported by the MoI representative, every measure that was technically feasible to apply in order to combat unauthorized actions, had been carried out in the period of two days upon completion of the inspection. In one case, monitoring lasted for a year at the headquarters of the Ministry, including all the records of the MoI. This monitoring helped the MoI to implement measures to further protect the data in those records, in accordance with the financial capacities of the Ministry. In the absence of funds, the Ministry of Interior is preparing a project proposal that would, if approved, be used to implement measures to protect the data stored in a non-automated manner (in paper form) in all organizational units of the Ministry (police departments, police stations, border police stations, etc.).

Misdemeanor Court in Novi Pazar reported that it did not have internal regulations governing personal data processing, but it kept records on "whether and who had access to the particular case, the way of recording any request for access to the case and the reasons for seeking the approval or disapproval of access are entered". The court provided the researchers with a sample of the Request to review documents [47] and the Request for photocopying[48].

Basic Court in Valjevo does not have internal documents, nor has it taken measures to protect the data. The Court does not keep records on who and when had access to the particular case, but the Court refers to the provisions of the Court Rules governing methods to get insight into the subject.

Basic Court in Loznica does not have internal documents and refers to the Court Rules. It is stated that "drafting of the Rules on the minimum anonymity of judicial decisions is in progress in the court". The area of use of video surveillance is not regulated by an internal act, but it is noted in the response that "the manager of the judicial police and court guard have access and insight into video surveillance".

---

46 http://www.rts.rs/page/stories/sr/story/135/Hronika/870122/Prijava+zbog+snimka+kod+Arene.html

47 Court rules ("Official Gazette RS", br. 110/2009), Article 328, Form 135,

48 *Ibid*, Form 136.

Department of Student Health Nis made an official record in response to the requests for access to information of public importance. The Department responded that they did not have internal documents, but said that in one case "the information was requested on the content of data from medical records by the Department for inspection – health inspector, which is registered in accordance with the regulations governing this matter ".

Health Center "Novi Sad" regulated the protection of personal data in more detail by the Statute of the Health Center, which reiterated the definition of professional secret from the Law on Health Protection, as well as procedures for handling such data. According to the statute the professional secret involves, inter alia, "a plan of physical and technical security of the Health Center". Health Center also states that the "software for the electronic health records used in the Health Center complies with the functional and technological requirements for the establishment of an integrated information system", as well as that "all measures of protection are undertaken in order to prevent illegal processing of personal data of patients and employees", without mentioning any specific measures.

Department of Student Health, Belgrade stated that it has the Business Ethics Code of the Institute[49] , which was distributed to the researchers. This Code stipulates that "any information learned by the health worker in exercising their profession about the patient's illness, family and other personal data, shall be kept as a professional secret." Each employee shall be handed a copy of the Code, the responsibilities for implementation of the Code are defined as well as the procedures in case of failure in the implementation of the Code. The Department further stated that "in the current process of accrediting health care facilities, certain procedures for the areas of operation and functioning of the institutions are established, and the segments of personal data protection will be addressed therein." Protective measures that have been undertaken within the Department refer to "establishment of an appropriate system for the facilities and organizational units, with a system of protection, safety and security of IT data that prevents unauthorized operation and access to information that is outside of the scope of certain operating units and employed therein (user accounts, granting certain rights, logging, etc.). Other appropriate actions "in terms of safe disposal and storage of business documents and prevention of unauthorized access (special cabinets, safes, locking the workspace, etc.)" are also performed.

49 From 21.1.2008. No. 176.

Health Center Negotin does not have internal regulations governing data protection, and it is not stated in the response which data protection measures have been undertaken.

Health Centre in Novi Pazar stated that it does not have any internal regulations that govern the processing of personal data, nor has it taken any measures to protect the data.

School of Electrical Engineering "Nikola Tesla" from Nis stated that the area of "misuse of personal data by students and employees is regulated through the disciplinary accountability under the Rules on disciplinary and material responsibility of students and employees," but the school did not submit this document although it had been required by the Request, so the researchers were unable to determine the content of the document by the conclusion of this Analysis. As for the protective measure undertaken, this school stated that "it keeps the register of data on students in steel counters and cabinets that are locked."

PUC Objedinjena naplata Niš responded as follows: "All the necessary information and documents in the field of personal data protection regarding abuse, destruction, loss, unauthorized access or changes, we have properly submitted to the Commissioner for Information of Public Importance and Personal Data Protection, and it is not a business policy of this company to submit documents regarding every question under this regulation ". It is not clear why this institution has decided not to submit the content of the documents because these documents are not published on the website of the Commissioner, nor the institution cited other location where such acts can be found (for example, on the website of the institution). These acts must be available to the citizens, since it is a public utility company whose work must be subject to public insight. There is an impression that this public institution considers that the right of the public is satisfied by submitting the documents to the Commissioner. This institution reported a total of four filing systems in the Central Registry. Describing the undertaken protective measures for all four filing systems, the controller stated that "the data storage is a work commitment." Responding further to the request, the controller stated that "only a person who is responsible for maintaining the database has access to it", that "the company keeps records" on who had access to certain information, and that "no one can access the database without prior legitimization of the authority and the scope of authority, which can only be the aforementioned persons", which was a measure that should be highlighted as an example of good practice. When asked what protective measures they have undertaken, it is stated that "all necessary measures to protect ... even fire protection", have been taken, without information on specific measures.

Company for Electricity Distribution Ltd Elektrovojvodina responded to the request stating that "all internal documents of the company [...] that more closely regulate this matter [...] are registered in the Central Registry." This controller entered a total of 10 filing systems. These records do not indicate the internal documents, but contain the undertaken protective measures concerning the automated processing of the filing systems which are secured "by a system of passwords for user authentication and authorization. The data can be processed only by authorized persons". Non-automated data collections "are kept in the premises of Elektrovojvodina Ltd. Novi Sad under a special lock mode, available only to the authorized person and the particular employees."

Public transportation company "Novi Sad", responded that they did not have internal documents, and referred the researchers to data protective measures, listed in the filing systems located in the Central Registry, where it was noted that "the filing system located in a computer is secured with a system of passwords for user authentication and identification for programs and data." It further states that "documents containing personal data are kept in a separate cabinet in the premises that are locked after the working hours." This company stated in the response that the Commissioner performed the inspection over the implementation of the PDPL, and did not find any irregularities in the procedure or order any special measures. Monitoring was conducted during the first half of 2012.

Public Utility Company Gradska čistoća in Belgrade did not adopt internal regulations, but stated that the data on the employees were "kept in a protected server", the access to which was held only by "authorized persons and persons who gain access by logging into the system by their user name and password." The company also uses video surveillance equipment and "material is taken depending on the movement up to 40 days, when the oldest video is automatically deleted. Users of these data are exclusively the employees in the security service". Finally, the company stated that it had taken measures to protect the privacy of participants in the recycling project. Each participant in the program is assigned a unique bar code that adheres to a bag of products for recycling. It is also stated in the response that "there is no possibility of pairing barcode owner information with the content of the recycling bags, and the bar code reader only has the option for validation and recording of the correct bags". It is further stated that "when the correct bar code information is read, the information is sent to the protected software, where the information that is paired with the IDENT number of the user is forwarded to PUC Infostan for exercising the right to discount."

Public Utility Company Gradska čistoća Novi Pazar stated in the response that internal regulations in this area had not been adopted, but that

"personal data (files) are kept locked" and they have determined "the person responsible for the storage and prevention of data abuse."

The only controller that responded to the Request stating that the protection of personal data is regulated by the Standard ISO/IEC 27001:20005 is the **Public Utility Company "Informatika"**. This company further responded that "all employees [...] signed the Contract on confidentiality of data when they entered employment." Personal information of the employees "is kept in the premises of the Department of Personnel and is accessible only by authorized employees."

Republic Health Insurance Fund, in a very detailed response to the request, stated that according to the Rules on Professional Secrets [50] it defines "data and documents that represent professional secret of the Fund [...] whose disclosure to unauthorized persons causes or may cause harm to the Republic Fund, the insured person to whom the information and documents relate. [...] processing materials considered confidential under this Rule involves receiving, labeling, production, recording, storage and destruction of these materials. " All the employees of the Fund, as well as members of the management bodies "who control data and documents that are considered confidential, must keep confidentiality and undertake the necessary security measures to prevent that data and documents [...] come into the hands of unauthorized persons". It is important to note that this document provides that "the duty of confidentiality does not cease even after the termination of employment[...]". The next Article of the Rules stipulates that "professional secret involves: data from the birth records of the insured[51], family members of the insured, subjects of compulsory health insurance, as well as the personal files of the employees".

The internal act states that "an employee working on the design, development, typing and copying documents and data which are confidential, is obliged to destroy traces of the concept, that is, to secure papers, indigo and matrices, or to protect the program and document on a computer and other materials that could reveal the contents of those documents". Records of data and documents labeled as confidential, which contain personal data, "are kept separately in steel cabinets and counters in a way that ensures their confidentiality." Further, this act regulates the procedure of destroying data, including the formation of a Commission established by the Director of the Republic Fund and the Director of the Regional Bureau. The Commission makes a record that contains: the name of the document that is being destroyed; the number and date under

50 01 number: 110-22/06

51 Closely defined: about: insured persons, family members of the insured; payers of compulsory health insurance.

which it is entered; the number of copies to be destroyed; marked degree of confidentiality; the date of delivery of the documents for destruction signed by the authorized person. This internal document regulates who and under what conditions (how) may disclose the contents of data that are considered confidential to the third parties. Separate records are kept on communication of data and, particularly important, "approval of documents, which are considered confidential to the third parties," and this internal document defines to whom the data are communicated or disclosed, which data is disclosed and communicated and when and for what purpose this is done.

The Fund states that "the process of adopting new Rules is currently in progress in order to comply with the provisions of the regulations in certain areas, issued after the applicable Rules", which indicates that this institution promotes the protection of personal data, that is, they harmonize the internal regulations with the new laws. The Fund has also stated that, "in establishing employment in the Republic fund, employees sign a confidentiality and non-disclosure of data agreements, which determine the duties of the employees in the area of data storage and non-disclosure of data. Statement on privacy policy and non-disclosure[52] contains the obligation of the employee to attend "the necessary trainings and lectures" aimed at "professional development [...] for the performance of duties or working tasks"; to handle "confidential information pursuant to the requirements of the employer and the provisions of applicable regulations", so the employee "shall immediately notify the employer in case of doubt that anyone else came into the possession of classified information, in order to take the necessary measures to further ensure confidentiality of information". The employee is obliged to "return all copies of confidential information in his/her possession" in case of termination of employment.

The Fund also noted that the procedures for handling the received Requests for exercising the rights regarding personal data processing are established in the internal document – Procedures for conducting legal transactions[53], which was adopted in the process of implementation of management systems in the Republic Fund for Health Insurance ". This act was also delivered to the researchers.

Veterinary Directorate at the **Ministry of Agriculture, Forestry and Water Management** stated in response to the request that "within its jurisdiction, in the field of protection of personal data [...] it acts in accordance with the Law on Personal Data Protection", without specifying whether and which protective measures have been undertaken in this field.

52 02/11 no. 112-/13, internal act.

53 Registered number: 07/5 no. 54-2913/12-51

Negotin Municipality stated that it did not have internal documents, noting that it was "not bound by the regulations of the Republic of Serbia to do so". The municipality did not respond to the question whether the measures for protection of personal data have been undertaken.

City Municipality Cukarica submitted the Code of Conduct for employees in the administration of the City Municipality Cukarica[54] to the researchers, stating that the employee is "obliged to protect personal data and other confidential information and documents acquired in the course of performing his/her duties or which have been incurred as a result of the job". It is also stated that "an employee may disclose only the information for whose disclosure he/she is authorized." The researchers' assessment indicates that this provision also applies to the disclosure of personal data. Likewise, "an employee should not attempt to access information if he/she is not authorized." The Code also states that "employees have an obligation to become familiar with this Code and to act in accordance with it"; that the manager "takes care of the implementation of the Code and takes measures for its respect," and that the rules in the Code "represent an integral part of the training and professional development of the employees."

The Guideline on Provision of Legal Aid of the City Municipality Cukarica regulates the process of providing these services, defining in a special provision which data is collected from the applicant. These data are classified as confidential in the Guidelines.

The presented responses of the data controllers indicate that the protection of personal data still represents a relatively new concept in Serbia, only partially understood and respected by the controllers. The very existence of internal documents does not imply that the data is necessarily protected by the controller, while the lack of such regulations does not imply that data is completely unprotected. However, the attached documents indicate that this field can be further regulated by internal documents, which must be presented to the employees, in order to improve the protection of personal data of the controller. The specific solutions that have been presented may motivate data controllers to study the experiences of others and thereby improve the level of data protection.

54 I-01 no. 110-4/12 from 09,11,2012

3.4. Case studies

Submitting the Request for exercising the right regarding personal data processing, as well as the Request for Access to Information of Public Importance, for the purpose of this Analysis the researchers focused on the four topics that are presented in more detail in the text below.

Records on holders of seasonal passes and tickets for sport events

"The organizer [of the sport events], in cooperation with sport clubs participating in sport events and clubs of their fans, shall ensure record keeping of the identity of persons to whom the tickets are sold, or provided through fan' clubs, and submit these records to the Ministry [competent for internal affairs]"[55].

The researcher submitted the Request for exercising the right regarding personal data processing to the Basketball club Partizan, asking whether the club has some of his data, given the fact that at the beginning of the competition season 2011/12 he had bought a season pass for the matches of this club, and at this occasion the officer of the club gathered information about him from the ID card. The answer of the club was the following:

Dear Sir,

The Basketball club Partizan, as the match organizer, is required under the Law on the prevention of violence and misbehavior at sports events, and according to the Article 13 of the same Law, to provide the Ministry of Interior the data on persons who have purchased tickets for our game. The lists of registered persons and photocopies of identity cards are submitted by the club to the Ministry of Interior – Department for the prevention of violence and misbehavior at sports events, upon the conclusion of the sale of tickets for each game. For each failure to submit the lists and photocopies, our club is financially sanctioned.

The Basketball club Partizan is only an intermediary, so we do not possess your personal information, process or deal with such matters.

55 Law on the Prevention of violence and misbehavior at sports events, Article 13

For further information on this issue, please contact the Ministry of Interior – Administration for the prevention of violence and misbehavior at sporting events.

Upon receiving the response of the Basketball club Partizan, the researcher addressed the Ministry of Interior in the Request for exercising the right regarding personal data processing, seeking information whether the MoI has data on him as the holder of the season pass. In the request, the researcher referred to the response delivered by the aforementioned basketball club.

The response of the MoI was the following:

Dear Sir,

Further to your request for information concerning the processing of personal data that you submitted to this Ministry on 29.11.2012, we inform you that the Ministry of Interior, Police Directory, Police Department, the Department for monitoring and preventing violence at sport events, do not keep records of persons who own seasonal pass BC "Partizan" for season 2011/12.

On the basis of the responses of the two controllers, the researcher could not determine what happened to his personal data, that is, whether the data was actually forwarded to the MoI. Therefore, during the next phase of the research, the Ministry of Interior was sent the Request for access to information of public importance, which read:

Does MoI have records on holders of tickets and season passes for the games of sport clubs? Which records the MoI has (for which sport club and which competition season)? If such records exist, please provide us with the answers to the following questions:

- *What personal data is processed in these records?*
- *For which purposes the data is processed?*
- *What type of data processing is performed?*
- *What is the legal basis for processing these data?*
- *How long the data is processed, and is termination of processing (delete) data in a certain period determined?*

The Request sent to the Ministry was also submitted to the Police Departments in Nis, Novi Pazar and Valjevo, in order to assess consistency in acting upon the received requests. The Police Department in Nis answered the following:

The MoI has no record on holders of tickets and season passes for the games of sport clubs. In accordance with the Article 13 of the Law on the Prevention of violence and misbehavior at sports events, the records are kept by the organizers.

The response of the Police Department Valjevo was the following:

The Police Department in Valjevo has no data or records on holders of tickets and season passes for the games of sport clubs.

The response of the Police Department in Novi Pazar was the following:

The Police Department in Novi Pazar has no record on holders of tickets and season passes for the games of sport clubs, and in line with the Law on the Prevention of violence and misbehavior at sports events, we are not obliged to keep such records, they are kept by the organizer.

It is not clear why the PU Valjevo and the PU Novi Pazar responded in this way, reducing the response to the work of the local police department, given that the question was addressed to the Ministry of Interior as a single entity, the data controller in terms of the Law on Personal Data Protection, that is, the subject of the Law on Free Access to Information of Public Interest. The same objection applies to the response of the Police Department in Novi Pazar.

A series of state authority bodies of the Republic of Serbia emphasizes suppression of violence at sport events as a priority of their work [56], which is the reason why the National Council for the Fight against violence at sporting events was formed. Serbian Prime Minister and Minister of Interior supported that "violence at sport events threatens the national interests of Serbia"[57]. However, the responses of organizational units of the Ministry of Interior indicate that the MoI does not keep records on holders of tickets and season passes, although the Law on the Prevention of Violence and Misbehavior at Sports Events in the Article 13 stipulates the obligation of clubs to forward the data of the ticket holders to the MoI.

This brief overview of the activities of the researchers and organizational units of the MoI indicates that this area is still not properly regulated. Article

56 http://www.novosti.rs/vesti/naslovna/aktuelno.289.html:404501-Alisa-Maric-Huligani-nece-proci

57 http://sport.blic.rs/Ostali-sportovi/229355/Dacic-Nasilje-na-sportskim-terenima-ugrozava-nacionalne-interese ". Combating violence is an imperative to preserve Serbian sports, safety of the athletes and fans who would like to enjoy with their families in sports competitions ", it was stated at the meeting of the Council for the Prevention of Violence in Sport, which was held on March 6, 2013.

13 of the Law stipulates the obligation of the organizers to collect data on ticket holders, but it is not specified what information should be collected. On this occasion, the Commissioner noted that the practice of photocopying IDs of the ticket holders[58] represents a violation of the principle of proportionality, that is, it entails excessive processing of personal data, and on this occasion he warned "all entities that exercise the above processing of personal data, that this is illegal and needs to stop immediately".[59] Concurrently, the response of the Ministry indicates that clubs do not provide such records to the MoI, while the selected club in the research team claims the opposite.

In an interview with representatives of the Ministry of Interior, we learned that the new Draft Law on Police provides for the establishment of such filing system, which includes specifying the scope and type of data collected, method of processing and data retention periods.

Meanwhile, until the adoption of the new Law on Police, the researchers suggested the Commissioner to perform monitoring of the clubs that have the highest number of fans, and to determine whether the clubs collect data on ticket holders, do they retain this data or they forward them soon after collecting to the MoI without making copies for internal records. Moreover, it is recommended that the Commissioner perform monitoring in the MoI and determine whether this Ministry has data on ticket holders, as well as to ascertain which data processing operations are carried out by the Ministry; when the data is destroyed and under which conditions, etc. During monitoring, particular attention should be paid to security checks, as this area of data processing remains unspecified by a special law in Serbia.

Records of the Ministry of Interior on personal identity checks

> *"The guidelines on the method of collection, processing, recording and using data from 01.10.1998 ... we are unable to deliver because it represents a strictly confidential internal act of the MoI"*. The response of the PU in Valjevo (No. 037-3/13-1) to the request for access to information of public importance, received in this research.

58 http://www.b92.net/sport/kosarka/vesti.php?yyyy=2012&mm=11&dd=27&nav_id=663702

59 http://partners-serbia.org/privatnost/aktuelno/nezakonito-prikupljanje-fotokopija-licnih-karata/

Serbian citizens, especially young people who find themselves on the streets after midnight, may experience the practice of the members of the Ministry of Interior who carry out verification of their identities and on such occasion enter data from the identity cards in their notebooks. The legal basis for the verification of the citizens' identity is not questioned, because the Law on Police provides that, *in performing police duties authorized officers have police powers, which, inter alia, include verification of the identity of the person and object identification* (Article 30). The purpose of this research was not to review the provisions of the Law on Police which determine the conditions for verifying the identity of the person (as defined in the Article 42 of the Law on Police), but to examine the procedures and data processing after such data is collected. Therefore, the researchers addressed the Ministry of Internal Affairs with the Request for access to information of public importance, which included the following questions:

Does MoI have records on individuals whom they asked to show identification cards? (This refers to the practice of asking people to show their identification cards in the streets and entering data from the IDs into the notebooks)

If such records exist, could you please answer the following questions?

- *What personal data is processed in these records?*
- *For which purposes the data is processed?*
- *What type of data processing is performed?*
- *What is the legal basis for processing these data?*
- *How long the data is processed, and is termination of processing (deleting) data in a certain period determined?*

Police Department in Nis stated in the response:

The Ministry of Interior has records of people who were asked to show their identification cards by the MoI officers. This area is regulated by the Law on Police, the Rules on Police Powers (Official Gazette No. 54/2006) and the Code of Practice in Police Affairs (Official Gazette of RS, No. 27/20007).

Police Station in Negotin forwarded the request to the Bureau of Information of Public Importance of the MoI, which sent a response with the same content.

Police Department in Novi Pazar responded as follows:

MoI makes records based on the Law on Police.

Any insight into the data processing is registered electronically and use of electronic databases is regulated by law.

Answer the police station in Valjevo was the following:

Each PU within the Ministry of Interior and the PU in Valjevo has records of persons who have been asked to show their IDs. The records contain basic personal information contained in the ID:

- *Name, surname, father's name, date of birth, identity number, home address and the time and place of identification.*
- *In line with the Article 76 Para 1 Item 6 of the Law on Police, the data is collected and processed in order to perform searches and operational checks necessary for the performance of police activities.*
- *Data is processed manually by completing the forms and data is entered electronically into a single system.*
- *The legal basis is contained in the said provisions of the Law on Police.*
- *The deadline for data storage is 10 years or they can be deleted earlier if the conditions are met (death, termination of the reasons for recording), the Regulation on the registration material with retention period Official Gazette RS 44/93.*
- *The User's Manual of the MoI determines precisely who can perform legitimization and how, processing and control processing of personal data, as well as the Guideline on the collection, processing, recording and using data from 01.10.1998, the provisions of which we are unable to deliver because it represents a strictly confidential internal act of the Ministry of Interior.*

The presented responses to the identical requests include notably different statements. It is not clear why the PU in Valjevo stated that the deadline for data storage is 10 years (with the caution that they may be deleted earlier if conditions are met), since the Law on Police, in the Article 81 governing the deadlines for personal and other data storage in the records, provides that the data contained in the records "verification of persons' identity" are kept *for two years after the completion of the authentication*. Judging by the response of the PU in Valjevo, this police department stores the specified data for longer than the prescribed time limit. Reference to the above Regulation on the registration material with retention period is hardly a justification to keep personal data for longer than required by the Law on Police.

In addition, the response of the PU Valjevo is also important because it is stated that the information on persons asked to show their IDs is processed manually by completing the forms, and data are subsequently entered electronically into a single system. The existence of a single

electronic system provides the citizens the opportunity to search and obtain information as to whether their personal data is contained in these automatically processed records. In this sense, every citizen may submit the Request for exercising the right regarding personal data processing to the Ministry of Interior and ask whether police has some data on him/her in the records of persons asked to show their IDs. If the MoI responds that his/her data are stored in the register, the citizen may request that the MoI present the reasons for keeping such data in the database and, if the purpose of data processing is fulfilled, demand that information about him/her is deleted from these records.

Finally, the answer of the PU in Valjevo is also interesting because this police department did not provide the researchers with the Guidelines on the collection, processing, recording and using data, referring to the fact that this internal document is classified as top secret. Article 14 Law on Data Secrecy[60], provides that the level of classification "TOP SECRET" is determined "in *order to prevent serious harm to the interests of the Republic of Serbia*". It is not clear under what criteria is this general act classified as top secret. Since the contents of this Guideline are inaccessible to the public, it may only be assumed on the basis of its title that it governs the area of personal data processing, which represents practice that has been declared unconstitutional in the decision of the Constitutional Court 68/2012.

The response of the PU in Valjevo causes concern, as it states that the data on citizens asked to show their IDs are typically stored for 10 years, contrary to the provisions of the Law on Police; it is not precisely defined how the causes for keeping records on citizens stop; and also because it states that the field of citizen data processing is regulated in a bylaw (although this practice was declared unconstitutional) which is concurrently unavailable to the public.

After the expiry of the statutory period of 15 years (1/10/2013) the researchers will submit the Request for access to information of public importance to the MoI, asking them to send the requested document.

The researchers lodged an appeal to the Commissioner at the beginning of March 2013 against the decision of the PU in Valjevo not to provide them with the content of the said Guideline, and the epilogue of this appeal would be presented on the website of the Partner Serbia (www.partners-serbia.org/privatnost), given that the Commissioner did not make a decision on the appeal until the conclusion of this publication. At this point, since this guideline is unavailable to the researchers, who are therefore unable to reflect on its content, it is noted that the Data Secrecy Law provides that the document classified as top secret becomes available to the public 15 years after entry into force (Article 19), unless there are reasons that the data are still kept secret (Art. 20).

60 Data Secrecy Law, Official Gazette RS", no. 104/2009

Establishment of a centralized database of medical patients

In an interview to the Daily Press on 8th November 2012[61], the Minister of Health Slavica Djukic-Dejanovic said that the Ministry was planning to establish a centralized database of patients' data. As stated in the introduction of the interview, "the database will contain all the data, analysis and results of the insured, performed in the private or public institutions, which will prevent the repetition of the procedures, shorten the path to timely health care and facilitate patients' treatment, concurrently saving the costs for the Serbian health system". According to the Minister, this will represent "a centralized software system in which all the health institutions will be networked, and will contain records of each of us. A patient coming to a hospital will not have to do the analysis that were previously done unless necessary, because the database will contain all the results of the analysis, diagnosis from any institution in which they were made. The doctor would just click on a button and have medical biography of each individual". When asked by the journalist, when this database would be made and how it would be paid for, the Minister said: "The plan is to initially start networking all the health centers and create a database during the next year (2013. – author's note). Networking would be covered from the money from an international project".

While this database could contribute to the efficiency of the health system, which can improve the quality of services, the Law on Personal Data Protection in the Article 16 stipulates that health information and data on disability are treated as particularly sensitive personal data and as such require a higher degree of protection. Until the publication of this Analysis, the Serbian Government has not adopted secondary legislation that would regulate the practical mechanisms and policies for the protection of particularly sensitive data, despite being obliged to do so, in line with the Article 16 Para 5 of the Law on Personal Data Protection, within 6 months from the entry of the Law into force[62] (this deadline expired in April 2009).

Testing the acting of the health care institutions as personal data controllers, the researchers concluded that such institutions were usually not sufficiently aware of their obligations to protect patients' privacy. Some institutions have not responded to the request, others have responded incompletely, while in response to the Requests for access to information of public importance, some health authorities have indicated that they have not taken any measures to protect the data, although it is their legal obligation.

---

61 http://www.pressonline.rs/info/politika/250931/nase-zdravstvo-nije-najvece-leglo-korupcije.html

62 Article 60 of the PDPL.

Given the delay of the government to enact appropriate bylaws and the results of this research, the authors of this Analysis express their concern for the privacy of the citizens in regards to the protection of their health data, which may be threatened during the implementation of the intentions of the Ministry of Health to establish a centralized database of patients' data.

Therefore, in the forthcoming period, it is important to determine whether there is a clear legal basis for establishment of such data collection, and in case of initiation of its development, adequate preventive measures protecting patient privacy should be provided. In this process, the Commissioner's role as the supervisory authority is of major importance. The research team invited the Ministry of Health for an interview on 1st March 2013 to present these questions to the public, however, until the conclusion of this Analysis no response was received from the Ministry.

Political parties and personal data protection

The political parties in Serbia are also subject to the Law on Personal Data Protection. Their duty is to uphold the Constitutional principles governing the processing of personal data. In this regard, the processing of personal data by political parties is permitted only if there is a legal basis or the consent of the citizen.

The citizens of Serbia had the opportunity to receive calls and pamphlets of the political parties, in which the parties urged them to exercise their right to vote. There were cases of delivering greeting cards for the 18th birthday, which invites citizens to exercise their voting rights acquired after attaining majority. It is also believed that the political parties have data collections on the so-called "certain voters", members of electoral committees delegated by the parties, as well as other filing systems. The use of filing systems on citizens formed by the state authorities by the political parties, was addressed by the Commissioner on several occasions, noting that the data from the voting lists must not be reproduced, that is, the use of such personal data for the purposes other than those for which they were established represents "a punishable offense, and under certain circumstances, even a criminal offence".[63]

This research analyzes the actions of the six political parties represented in the National Assembly of the Republic of Serbia. It is devastating that only two parties responded to the

Requests for exercising the rights regarding personal data processing , as stated above. The researchers lodged an appeal to the Commissioner against the parties that have failed to do so, and the epilogue of the appeal will be presented on the website of the Partners Serbia (www.partners-serbia.org/privatnost).

63 http://www.dnevnik.rs/politika/sabic-stranke-da-postuju-licne-podatke-gradjana

Acknowledging that political parties are extremely complex entities, which operate on the whole territory of the country, with some having more than a hundred party branches (the boards), and that none of the parties from the research sample fulfilled the basic obligations from the PDPL of reporting filing systems to the Central Registry on the website of the Commissioner, the authors suggest that the potential misuse of citizens' personal data by political parties should not be neglected. In this sense, the research team sent a proposal to the Commissioner to conduct monitoring and to determine, primarily, if political parties have records which are not provided by law, and which contain data on citizens processed without their consent.

4
CONCLUSIONS AND RECOMMENDATIONS

It appears that the area of privacy protection has not yet received sufficient attention of the citizens, the media and experts. This is evidenced by the fact that, in contrast to the significant engagement of civil society especially in promoting and monitoring the realization of the rights under the Law on Free Access to Information of Public Interest, so far there were no activities of monitoring the implementation of the Law on Personal Data Protection, nor the analysis of the practice of the Commissioner for Information of Public Importance and Personal Data Protection in this area.

4.1. Methodology of monitoring and analysis of the controllers' actions

One of the challenges and the task of this research was to develop a methodology for the monitoring and analysis of the implementation of the PDPL, as well as the acting of the data controllers upon the Commissioner's decisions. The developed methodology may be useful for the Commissioner's Office, as well as for civil society organizations, the media and citizens who are interested in this area.

- In **determining the sample of the research**, it is necessary to be guided by certain criteria, which may include:

  - The territorial distribution of data controllers,
  - Acting of data controllers regarding the entry in the Central Register kept by the Commissioner,
  - Status of the data controllers (authority, company, association, etc.),
  - Preliminary acting of the Commissioner towards data controllers in the field of protection of personal data (whether the Commissioner intervened earlier regarding this controller).

- **Submitting the** Requests for exercising the rights regarding personal data processing to the selected data controllers, and monitoring of acting of data controllers upon the submitted requests. If the data controller has provided a response to the request, the researcher analyzes the response. Against data controllers who have not responded to a request or submitted false or incomplete answers, the researcher may **appeal to the Commissioner**.

- **Actions of the Commissioner upon appeals**. At this stage, the researcher monitors whether the Commissioner has accepted the appeal or not. It should be noted that the Commissioner, in carrying out its responsibilities, undertakes different types of interventions (issuing opinions, cautions, rulings, conducting supervision). The Commissioner has the authority to make different types of decisions, such as to temporarily ban any processing carried out contrary to the provisions of this Law, to order deletion of data collected without proper legal grounds, to order rectification of such irregularities within a specified period of time, to pass a ruling ordering a controller to decide on a request, etc. Unlike other independent bodies in Serbia, such as the Ombudsman and the Commissioner for the Protection of Equality, the decisions of the Commissioner for Information of Public Importance and Personal Data Protection are final, binding and enforceable, and against a decision of the Commissioner administrative dispute may be initiated.

- **Actions of the data controllers upon decision (order) of the Commissioner**. If the Commissioner determines that the appeal is justified and makes the decision ordering data controller to act upon the request within a specified period, the researcher follows the controller's actions, primarily in terms of whether an answer to the request has been delivered, access to the data allowed (depending on the content of the request) and so on.

- **Submission of Requests for Access to Information of Public Importance**. This Request is used by the researcher to address a public institution in order to examine whether the controller has and respects the internal procedures and undertakes technical, personnel and organizational measures for data protection. This information is public in nature and institutions are obliged to make them available, at the request of citizens, the media and civil society organizations, upon which the analysis of the submitted documents and responses can be performed, as well as determination whether the controller acted upon the decisions of

the Commissioner, or, has taken adequate measures to improve the privacy of users, clients or employees. Additionally, the Request can be utilized to ask the controller to specify which measures are taken after the intervention of the Commissioner in the specific case, which can indicate whether the controller has undertaken specific measures in this period, that is, whether the intervention of the Commissioner motivated the responsible person at the controller to pay due attention to the privacy of users, clients, and employees, not necessarily in the domain related to the specific intervention of the Commissioner.

- **Submission of the questionnaire**. Assessment of the acting of the controllers who are not state authorities, and are therefore not subject to the Law on Free Access to Information of Public Importance, can involve sending the request to the controller to complete the questionnaire and respond to questions posed by researchers. The questionnaire can contain the same or similar questions that are addressed to public institutions in the form of Requests for access to Information of Public Importance. An example of the questionnaire is given in the Appendix.

- **Organizing interviews**. Finally, in order to obtain information on the measures of data protection of the controller, as well as to determine whether and how the controller complied with the Commissioner's decision, the researcher may send the request to organize the interview with a representative of the data controller. The process of such conversation can often provide more information than submitting a request and questionnaires.

The research team believes that the scope of analysis of the PDPL implementation, and acting of the controllers upon the decisions of the Commissioner, is greater when the object of the research involves state authorities, since these controllers are also subjects of the Law on Free Access to Information of Public Importance. This analysis presented the method of utilizing the Law on Free Access to Information of Public Importance in order to obtain information from the authorities on personal data processing. Such methodology can be used not only in monitoring and analysis of acting of the data controllers upon decisions of the Commissioner, but also in analyzing the acting of any other authorities with regard to the processing of personal data.

4.2. Recommendations

The experience of this research pointed to several fundamental problems in the field of personal data protection in Serbia, based on which it is possible to make recommendations for further action in this field:

- A significant number of personal data controllers are not yet familiar with the contents of the Law on Personal Data Protection, and in particular with the meaning of certain terms of the Law. Therefore, it is necessary to continue informing and educating the controllers and the general public, about the rights and obligations arising under the Law.

- Most controllers have not yet developed adequate mechanisms for acting upon the requests for exercising of rights in regard to personal data processing. It is recommended that each controller designates a service or a person to act upon such requests, particularly given the same trend in the legal framework of the European Union, with which our legislation will be harmonized.

- Since the measures of data protection entail a legal obligation of each controller, it is recommended that each controller undertake such measures, and produce internal documents that would precisely regulate the field of data protection.

- The executive authorities, despite over four years of implementation of the Law, have not yet adopted appropriate bylaws in the area of personal data protection, particularly those governing the method of storage and measures for protecting particularly sensitive data (ethnicity, religion, health, sexual life, etc.). It is necessary to exert further pressure on the government to adopt these bylaws as soon as possible, and to provide adequate protection for particularly sensitive data of citizens.

- In view of the Decision of the Constitutional Court of the Republic of Serbia 68/2012[64], of 18.07.2012, which determined that certain provisions of the PDPL[65], stipulating that the legal basis for data

64 http://www.uzzpro.gov.rs/doc/biblioteka/BiltenBr7-2012.pdf

65 Article 12 Para 1 Item 3) reads in part: "any other regulation promulgated in accordance with the law", Article 13 in part as follows: "or any other regulation" and Article 14 Para 2 item 2) in part as follows: "or any other regulation promulgated in accordance with the law".

processing can be established in a bylaw, are not in accordance with the Constitution, it is necessary that all data controllers harmonize their practice as soon as possible with the Decision of the Constitutional Court, or not to establish grounds for processing personal data in the acts of lower legal force than the law. Legislative, executive and judicial authorities should further support the work of the Commissioner to enable this body to fulfill its mandate in the area of personal data protection. This support should include the timely adoption of necessary bylaws, provision of additional financial and technical conditions for the operation, as well as acting of the competent authorities in accordance with the decisions and initiatives of the Commissioner, with the improvement of case law in this area.

- Citizens are not yet familiar with the rights contained in PDPL and the possibilities for their realization. Therefore, it is necessary to improve public awareness through campaigns on the importance of privacy protection.

- Legal aid providers (lawyers, free legal aid services, civil society organizations, etc.) should be additionally trained in this area, in order to be able to adequately protect the rights of citizens, which would prevent misuse of personal data.

- Civil society organizations have not yet sufficiently recognized the importance of protecting privacy in the light of improving the general state of human rights in Serbia. Therefore, it is necessary to further strengthen the capacity of these organizations to monitor and report on the acting of the data controllers and personal privacy policies in general.

- Adoption of the new Law on Personal Data Protection, announced by the Ministry of Justice and Public Administration, should correct and remove the deficiencies of the existing law, primarily to include regulation of the areas of video surveillance, biometric data, direct marketing, and security checks. However, if the intention of the legislator is to promote the protection of personal data of citizens of Serbia, the new law would have to contain significantly clearer and more understandable provisions upon which the controllers would perceive their obligations and act accordingly.

* * *

After more than two years of performing promotional and educational activities in the field of personal data protection in Serbia, the authors of this Analysis are forced to conclude with regret that the situation in this area has not significantly improved.

Nevertheless, given the fact that the Law on Personal Data Protection requires data controllers to truthfully and fully inform the citizens about the processing of their personal data, this right can be widely used by the citizens by referring the relevant requests to all the controllers that are reasonably assumed to have the information on them. The methodology for monitoring the acting of data controllers upon the request may be based on the model presented in this research. Therefore, in addition to the need to improve the legal framework which was already discussed in this document, it is necessary to continue indicating the citizens the importance of personal data protection, data controllers on their obligations under the Law, and the decision-makers on the need to further support the institution of the Commissioner for Information of Public Importance and Personal Data Protection, responsible for enforcing the Law. These efforts should not solely depend on the process of harmonizing the national legal framework and practice with the standards of the European Union, but also on the efforts of our society to protect one of the basic human rights of its citizens and enable them to live in dignity. We hope that this Analysis at least partially contributes to this goal.

5
APPENDICES

Appendix 1. Department for student health – Request to exercise the rights in regards to personal data processing

Department for student health, Krunska 57, Belgrade

R E Q U E S T
to exercise the rights in regards to personal data processing

Pursuant to the Article 24 Para 1 of the Law on Personal Data Protection ("Official Gazette RS ", no.97/08 and 104/09 - other law), the above data controller is requested to provide me with information on personal data processing.

I was treated several times in the students' polyclinic in the period from 2003 to 2008. I would like to be informed by providing me the answers to the following questions:

1. Do you process data about me?
2. Which data about me you process?
3. What types of data processing do you perform?
4. From which source the data was collected or who is the source of data?
5. What is the purpose of data processing?
6. In which filing systems the data is included?
7. Is data about me transferred (provided) to other data controllers or processors? On which legal basis and for what purpose this data is transferred?
8. What is the time period of data processing and whether termination of processing data is determined in a certain moment?

Searching the Central Registry at the website of the Commissioner for Information of Public Importance and Personal Data Protection, I was unable to find whether you filed a report on the existing filing systems, and therefore I kindly ask you to inform me on the abovementioned information within the prescribed time limit in a written form by answering each of the questions. Please reply by mail, or email.

Respectfully,

Belgrade,

Name (Father's name) Surname
Date of birth: --.--.----.
Personal identification number: ----------
Address: ----------

21.11.2012.

----------@----.---

Appendix 2. Answer given by Basic Court in Sabac (original document)

Република Србија
ОСНОВНИ СУД У ШАПЦУ
Број: Су VIII-42-6/2013
Датум: 12.02.2013.године
Ш а б а ц

У поступку по поднетом захтеву за доставу обавештења о обради података о личности, подносиоца [redacted] на основу одредбе члана 19, и 25 Закона о заштити података о личности (Службени гласник РС 97/08, 104/09...107/12) обавештава се подносилац

[redacted]

Овај суд обрађује податке о лицу које је у својству судског тумача регистровано од стране Министарства правде и државне управе, и коме је решењем поступајућег судије одређена исплата за ангажовање у одређеном судском поступку (трошкови и награда), односно податке о лицима која су у својству судског тумача ангажавана у судском поступку пред овим судом. Обрада се врши у односу на следеће информације о личности: име и презиме, адреса становања, контакт телефон, јединствени матични број, број рачуна и назив банке код које се воде рачун и на који се има извршити исплата, износ исплате (бруто и нето) који је извршен или треба извршити на терет буџетских средстава. Радње обраде су следеће: прикупљање, бележење, преписивање, потхрањивање, обједињавање, разврставање, коришћење. Подаци се прикупљају од лица на које се односе (непосредно, и посредно- увид у решење о одређивању исплате на име ангажовања у судском поступку), и то само они подаци који су неопходни ради вршења законских обавеза суда. Подаци се обрађују у сврху извршења законских обавеза, и то вршења исплате накнаде и награде ангажованим стручним лицима, и у вези извршених исплата, вршења обрачуна и плаћања пореза и доприноса за обавезно социјално осигурање, у складу са Законом о порезу на доходак грађана, Законом о доприносима за обавезно социјално осигурање, Законом о пореском поступку и администрацији, и донетим подзаконским актима. Подаци се налазе у евиденцијама и помоћним рачуноводственим књигама: именик судских вештака и тумача који су били/јесу ангажовани у судским поступцима у овом суду- интерна књига која се налази у рачуноводству суда, искључиво намењена за попуну обавезних података у прописаним обрасцима (пријаве), и у збирци – регистратору у коме се налазе пријаве које су достављене надлежним државним органима, и то: Појединачна пореска пријава о обрачунатом и плаћеном порезу и доприносима за обавезно социјално осигурање по одбитку на терет примаоца прихода – образац ППП (за период од годину дана, збирно за сва запослена и ангажована лица у суду; електронски облик); Пореска пријава о обрачунатом и плаћеном порезу на приходе спортиста и спортских стручњака и на друге приходе (уговор о делу, допунски рад, трговинско заступање, волонтерски рад, примања чланова управног и надзорног одбора, накнада посланицима и одборницима, накнада по основу послова одбране и заштите, примања стечајних управника, судских вештака, судија поротника и судских тумача и друга примања када се обрачунавају доприноси за обавезно социјално осигурање)- образац ПП ОПЈ-6; Пријава о уплати доприноса по основу уговорене накнаде, односно накнаде по основу уговора о допунском раду и висини те накнаде- образац М-УН. Подаци се прослеђују у пријавама које је суд по закону дужан да достави и то надлежној филијали Пореске управе (обрасци ППП, и ПП ОПЈ-6), и надлежној филијали фонда за пензијско и инвалидско осигурање (образац М-УН). Подаци се обрађују док лице не буде брисано из регистра судских тумача, односно буду ангажовани од стране суда у појединачном судском поступку. Обрађени подаци, односно пријаве чувају у складу са општим роковима прописаним за чување рачуноводствене документације.

В.Ф.Председника суда
Владимир Јокановић,с.р.

Тачност отправка тврди и оверава:

Appendix 2. Answer given by Basic Court in Sabac (translation)

REPUBLIC OF SERBIA
BASIC COURT IN SABAC
Number Su VII-42-6/3013
Date 12/02/2013
Sabac

In the proceedings upon request for delivery of information regarding personal data processing of the applicant [*applicant's identity deliberately hidden*] in line with the provisions of the Article 19 and 25 of the Law on Personal Data Protection ("Official Gazette RS" NO. 97/08, 104/09...107/12), we inform the applicant

[*applicant's identity deliberately hidden*]

That this court processes data about the person registered as court translator at the Ministry of Justice and Public Administration, for whom the fee was determined by the court decision for the engagement in specific judicial proceedings (the expenses and reward), that is, data on persons who appear as court translators in the proceedings before this court. Processing is performed regarding the following personal data: name and surname, address, contact phone, personal identification number, account number and the name of the bank which has the account in which the payment should be made, the amount of the fee (gross and net) that is paid or will be paid at expense of the budget.
The processing actions are the following: collection, recording, replication, storage, merger, sorting, usage. Data is processed for the purpose of executing legal obligations, that is conducting payment of the fees and rewards to the engaged experts, and in connection with payments, accounting and paying taxes and benefits for mandatory social insurance, in line with the Law on taxes on citizens' income, Law on benefits for mandatory social insurance, Law on tax proceedings and administration and adopted bylaws. Data is kept in the records and additional accounting books: the registry of the court translators and interpreters who are/were engaged in the court proceedings before this court – internal book which is kept at the court accounting section, made solely for the purpose of fulfilling mandatory data in the prescribed forms (applications), and in the filing system – registry, in which there are applications submitted to the competent state bodies, including: single tax declaration on the calculated taxes and benefits for mandatory social insurance withholding tax at the expense of the recipient – form PPP (for the period of one year, the total for all the employees and engaged persons at the court; electronic form); Tax declaration on the calculated and paid taxes on the income of the sport players and experts and other income (Contract on the provision of services, additional work, business representation, volunteering, income of the members of the executive board and supervisory board, fee for the MPs and deputies, fee on the basis of the work for defense and protection, income of the bankruptcy administrator, court experts, lay judges and court interpreters and other income when mandatory social insurance benefits are calculated) – form PP OPJ-6; declaration on payment of benefits on the basis of agreed fee, that is on the basis of the contract on additional work and the amount of that fee – form M-UN. The data that is transferred in the applications for which the court is legally obliged to submit to the competent Tax Administration (forms PPP and PP OPJ 6) and to the competent centre of the Republic Fund for Pension and Disability Insurance (form M-UN). Data is processed until the individual is deleted from the registry of court translators, or engaged by the court in the specific proceedings. Certain data or applications are kept within the generally prescribed time limit for records keeping on accounting documents.

Acting President of the court
Vladimir Jokanovic

Appendix 3. Health center Vracar –
Request for access to information of public importance (page 1)

PARTNERI
za demokratske promene
SRBIJA

Svetozara Markovića 9, I sprat, 11000 Beograd, Srbija
Tel: 011/3231 551 • Fax: 011/3231 553
office@partners-serbia.org , www.partners-serbia.org

Health Center Vračar
Bojanska 16
11000 Belgrade

Belgrade, 14 February 2013

Dear Sir/Madam,

Topic: Request for access to information of public importance

Partners for Democratic Change Serbia and the Network of Committees for Human Rights in Serbia have been conducting the project "Personal data protection as a basic human right" in the period from 2012 to 2013. The Project is supported by the EU Delegation in Serbia and the USAID program JRGA.

As part of the project, we are conducting a research on the implementation of the Law on the Personal Data Protection. Within the research, we collect information acting of personal data controllers and on the measures undertaken by data controllers to protect the right to privacy of their users, clients and employees.

Attached is the Request for access to information of public importance. Please provide us with the answers to the stated questions. The research results will be presented in April 2013, and the responses you provide will be used for the preparation of the final publication.

Respectfully,

Blažo Nedić,
Partners for Democratic Change Serbia

Appendix 3. Health center Vracar –
Request for access to information of public importance (page 2)

Health center Vracar, Bojanska 16, Belgrade

R E Q U E S T
For access to information of public importance

In line with the Article 15 Para 1 of the Law on Free Access to Information of Public Importance ("Official Gazette RS" no. 120/04), please provide us with the required documents and requested information of public importance in a written form within the prescribed time limit.

1. Is there an internal act of the institution governing the field of personal data protection against misuse, destruction, loss, alteration or unauthorized access? If so, please provide us with the specific act or the part of an act governing this area.
2. Does some internal act of the institution specify who and under which conditions may have insight into a medical record? If so, please provide us with the specific act or the part of an act governing this area.
3. Does the health center keep records regarding who and when had access to a medical record? If yes, please provide us with additional information about the type and manner of records keeping. We emphasize that we do not need to be provided with the specific records
4. The health center uses video surveillance equipment? If so, is there an internal act of the institutions specifying how the recorded material is used, who has access to the material, when the recorded material is deleted? If such documents exist, please provide us with the specific act or the part of an act governing this area.
5. Whether protective measures and which ones (human resources, technical and organizational) have been undertaken to prevent illegal actions regarding personal data of patients and staff which are necessary in order to protect data from loss, destruction, unauthorized access, alteration, disclosure, and any other abuse?
6. Are there other internal documents of the institution that regulate the method of personal data processing of the patients and staff? If so, please provide us with the specific act or the part of an act governing this area.
7. Is there an internal act closely regulating the procedures for handling the received requests for exercising the rights in regards to personal data processing or other requests provided by the Law on Personal Data Protection? If so, please provide us with the specific act or the part of an act governing this area

14 February 2013
Belgrade

Partners for Democratic Change, Serbia
Svetozara Markovica 9, Belgrade
Phone: 011 3231551
Email: office@partners-serbia.org