PARTNERI SRBIJA

Овај пројекат финансира Европска унија

#ЕУ ЗА ТЕБЕ

Privacy and Personal Data Protection in Serbia

- An Analysis of Selected Sectoral Regulations and Their Implementation -

SHARE FONDACIJA

A 11 INICIJATIVA ZA EKONOMSKA I SOCIJALNA PRAVA

BOŠ BEOGRADSKA OTVORENA ŠKOLA

ATINA

DA SE ZNA!

Publisher:
Partners for Democratic Change Serbia (Partners Serbia)
https://www.partners-serbia.org/

For the publisher:
Ana Toskić Cvetinović

Editor:
Uroš Mišljenović

Authors:
Damjan Mileusnić
Danilo Ćurčić
Dunja Tasić
Jelena Adamović
Kristina Kalajdžić
Miloš Kovačević
Mihailo Pavlović
Nina Nicović
Uroš Mišljenović

Reviewer:
Ana Toskić Cvetinović

Translator:
Vera Gojković

Proofreading and editing:
Tamara Ljubović

Belgrade, April 2021

This publication was published with the financial assistance of the European Union. The content of the publication is the sole responsibility of Partners for Democratic Change Serbia, SHARE Foundation, „Da se zna!" Association, Belgrade Open School, ATINA NGO and A11 Initiative, and can in no way be taken to reflect the views of the European Union.

***

All terms used in the masculine gender refer equally to the masculine and feminine genders of persons they refer to.

Table of Contents

Introduction

The right to privacy is a right which is deemed to be in the very heart of human freedom. It is inextricably linked to the type of political system in a society. Societies based on the rule of law and human freedom ideas are usually leaders when it comes to respecting citizens' privacy. Conversely, societies inclined towards authoritarian types of government apply different mechanisms with the aim of disrupting citizens' private lives.

In this context, privacy is similar to the concept of personal autonomy and freedom of choice, which is usually associated with independent decision-making about one's own body and the expression of one's own identity. In addition to this, the private can be perceived as the opposite of the public. In the private domain, individuals are free from the influence and interference of others, they are left to themselves, their feelings, needs or whims. This understanding of privacy implies that physical boundaries are imposed to prevent third parties from entering an individual's personal space. Next, privacy is often discussed in the context of personal data processing and our right to have our data processed lawfully, to have the processing adapted to the purpose sought by the processing, to ensure the security of processing through established accountability mechanisms for those who are processing the data, to make the processing circumstances known to the data subject, etc. These are some of the principles that were introduced in our legal system after the adoption of the Law on Personal Data Protection in 2008, and additionally reinforced by the (new) 2018 Law.

These aspects of privacy are in the focus of this publication. Its purpose is to present, from the authors' aspects, the key issues and challenges for the privacy right protection faced in the implementation of public policies in the Republic of Serbia which either emerged in 2020 or had existed for years, but became particularly prominent in the year as specific as the one behind us.

The year 2020 was marked by the COVID-19 pandemic, which, in addition to its obvious impact on our health, also affected the way we think and shape interpersonal relationships, as well as relations between the state and individuals. The fight against the virus has brought about new challenges for privacy and data protection, primarily owing to the establishment of extensive databases on the infected and ill citizens, as well as citizens who have applied for vaccination.

Alongside problems and challenges concerning citizens' privacy that appeared in the context of the pandemic in 2020, long-term problems remained in place, both those concerning shortcomings in the legal framework in the field of privacy and those in the implementation of regulations guaranteeing citizens privacy protection. Within their joint project "Preserve Privacy - Resist Pressure," Partners Serbia, Share Foundation, A11 Initiative, *Da se zna*, Atina Association and Belgrade Open School in 2020 initiated the monitoring procedure of privacy right violations in Serbia. Registered privacy violation cases have been available in the online database at https://monitoring.mojipodaci.rs/ since December 2020. The database will represent an open public service for future research and monitoring of trends in this area.

Judging by the registered privacy violations, we can observe that their number in the fields of health and public administration was larger than average, which is especially problematic during a public health crisis such as the COVID-19 pandemic, as well as that this was also the case in the security sector, labor relations, media reporting and consumer relations.

Continuous monitoring of privacy violations and unlawful personal data processing is important for several reasons. First of all, it provides an insight into the current situation or changes in certain trends, making it possible to observe high-risk situations that require attention. Additionally, this overview may be used as a source for follow-up research of identified problems

and more detailed research and analysis. Furthermore, in the case of serious or major violations, information gathered in this way may be used for initiating or facilitating strategic litigation in the field of personal data protection.[1]

Finally, examples of violations of the right to privacy are also important for analyzing the quality of implementation of the existing public policies in this area. This publication presents concise analyses of personal data processing in several sectors in which the organizations implementing the project have had many years of experience.

Specifically, the introduction of the publication is followed by an analysis of the actions undertaken by public prosecutors' offices and courts in the Republic of Serbia in personal data protection cases. In our opinion, improvements in this area represent a necessary precondition for improving the implementation of sectoral regulations. Next, we will first present an analysis of personal data processing in the healthcare sector in the context of the COVID-19 pandemic. Then, we will shed light on the implementation of personal data protection standards in the education sector within the Unified Information System in Education. After that, we will present the troubling practice pertaining to the establishment of video surveillance in public areas. The publication will continue with two analyses pertaining to the departure from personal data protection standards in the case of vulnerable groups – beneficiaries of social assistance under the new Law on Social Cards and LGBT persons under the Rulebook on detailed conditions, criteria and manner of selection, testing and assessment of providers of reproductive cells and embryos. The publication ends with an analysis of the rules and practices of personal data transfer from the Republic of Serbia.

The selection of these thematic units shows that the publication does not claim to offer a comprehensive overview of legal gaps or issues in the implementation of the legal framework on privacy and personal data protection in our country. Such an effort should constitute a part of a comprehensive reform of the relevant legal framework, which has been entrusted to competent institutions under the Action Plan for Chapter 23 (Revised July 2020 Action Plan[2]) as activity 3.9.1.2, which envisions the implementation of an analysis of sectoral regulations and development of a plan for their harmonization with the new Law on Personal Data Protection by the last quarter of 2020. Since we did not find out by the time of issuance of this publication (March 2021) whether this analysis had been made, we must point out that the envisaged deadline has expired. The same can be said about the failure to fulfill the obligation referred to in the Law on Personal Data Protection, to "harmonize the provisions of other laws pertaining to personal data processing with the provisions of this law by the end of 2020."

In that regard, the purpose of this publication is to help understand the weaknesses of existing regulations and their implementation in specific sectoral areas and to provide recommendations on how to improve the identified situation.

Finally, the selection of the relevant thematic areas reflects a high level of commitment to human rights by the organizations implementing the project, the observation of which extends beyond the right to privacy and personal data protection. We hope that, in addition to their main purpose, the presented analyses will help ensure better understanding of the importance of the right to privacy and personal data protection as preconditions for the protection of other rights and freedoms, such as freedom of expression and the right to protection from discrimination, as well as reaffirm the unbreakable ties between privacy and human dignity.

[1] https://monitoring.mojipodaci.rs/methodology
[2] https://www.mpravde.gov.rs/tekst/30402/revidirani-akcioni-plan-za-poglavlje-23-22072020.php

The activity of public prosecutors' offices and courts in the Republic of Serbia in personal data protection cases

(Summarized version of the analysis with main findings, conclusions and recommendations. The full version is available in the Serbian language)

Authors: Nina Nicović, Mihailo Pavlović, Uroš Mišljenović, Damjan Mileusnić, Partners Serbia

Introduction

In this analysis, we review the actions of competent judicial institutions in personal data protection cases. At the beginning, we present the case law regarding the criminal offense of *Unauthorized Collection of Personal Data* referred to in Article 146 of the Criminal Code. This is followed by the activity of public prosecutors' offices on criminal reports submitted in the period between 2015 and July 2020 by the Commissioner for Information of Public Importance and Personal Data Protection (hereinafter referred to as: the Commissioner). Finally, we analyze the case law of misdemeanor courts on the implementation of the Law on Personal Data Protection, which started in 2019.

The purpose of the analysis has been to determine whether the criminal law mechanisms ensuring the protection from violations of the right to protect personal data are effective in the Republic of Serbia, and to identify effects of the adoption and implementation of the new Law on Personal Data Protection (LPDP) when it comes to judicial protection and sanctioning of violations of rights guaranteed by the LPDP after the first year of implementation of the Law.

Case law on Article 146 of the Criminal Code (Unauthorized Collection of Personal Data)

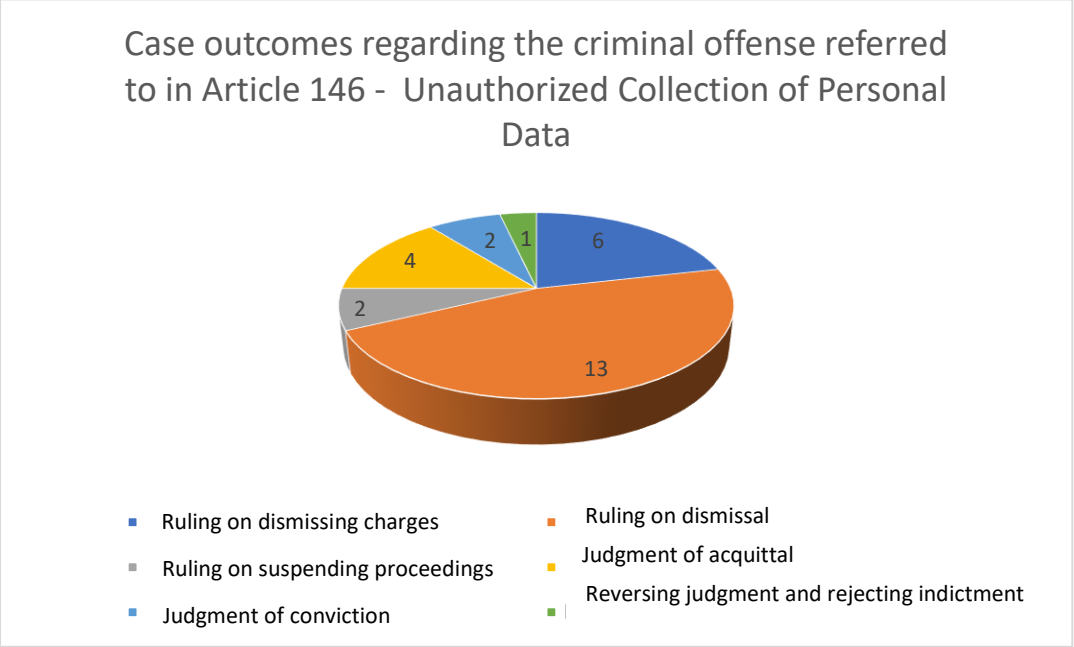
This segment of the analysis refers to the activities of competent courts regarding the criminal offense referred to in Article 146 of the Criminal Code - **Unauthorized collection of personal data**.

In order to analyze the case law on this criminal offense, researchers sent to all basic courts in Serbia (66 courts in total) requests for free access to information of public importance. In the requests, they asked the courts whether any criminal proceedings under Article 146 of the Criminal Code (CC) were currently held before the court; whether proceedings for this criminal offense had been held between January 1, 2015 and the date of receipt of the request (July 2020), and, if there had been such cases, to provide decisions in those cases. The requests asked for both final and non-final judgments, as well as second-instance court decisions on appeals, if there had been any.

On the basis of information, i.e., documentation provided by the courts, the text below presents the main characteristics of the case law on Article 146 of the CC.

Between 2015 and July 2020, a total of 28 cases were initiated at 14 basic courts in Serbia. Two cases were initiated on the basis of motions to indict issued by competent public prosecutors' offices, while the remaining 26 were initiated as a result of private lawsuits.

Rulings to dismiss charges were issued in six cases, rulings to reject charges were issued in 13 cases, while rulings on staying the proceedings were issued in two cases. Two cases ended with judgments of conviction, judgments of acquittal were issued in four cases, while one court reversed the judgment and rejected the charges.



Charges referred to in private lawsuits were dismissed by a ruling (in 6 cases) because of procedural reasons and the private prosecutor's failure to correct them at the order of the court (name of the court, personal data, etc.) as well as the timeliness of lawsuits (failure to observe the time frame of three months from the date when the injured party learned about the crime).

When it comes to cases where private lawsuits were rejected by the court (13 cases, or almost 50% of the research sample), we can notice that in four of the cases, the court, right after reviewing the lawsuit, sent an order to the private prosecutor to supplement or correct it within three days. This means that some private lawsuits in the area regulated by Article 146 of the CC contained such omissions which, in the opinion of the court, prevented it from acting on the lawsuits unless omissions were corrected.[3] It turned out that, after such a court order, the majority of private prosecutors had observed the time frame for supplementing or correcting the lawsuit, but either withdrew or supplemented, i.e., specified the lawsuit in such a way that they were rejected in the first and second instance. Most frequently, the court explained its decision by saying that the lawsuit insufficiently described, i.e., specified the elements which the court had pointed out.

When it comes to judgments of acquittal, one of the cases was initiated at the motion to indict of the public prosecution, while three others were initiated by private lawsuits.

Two judgments of acquittal were handed down by the First Basic Court in Belgrade and the other two by the Basic Court in Pančevo.

As for the cases that ended with convictions, two suspended sentences were imposed. One case was held before the Basic Court in Zrenjanin, while the other before the Basic Court in Novi Sad.

[3] E.g., see the ruling of the Basic Court in Subotica 6K. 817/2016

The Basic Court in Jagodina handed down a first-instance judgment of conviction against a police inspector who had processed the personal data of the injured party (Jagodina Police Administration commander) without his authorization or written consent, and then shared these data with all other police officers on the bulletin board of the Jagodina police outpost, thus using the data for an unintended purpose.[4] However, the Higher Court in Jagodina **reversed the judgment and dismissed the charges against the defendant.**[5]

Finally, **in the cases in which court proceedings were suspended**, the duly summoned female[6] and male[7] private prosecutors failed to appear at the trial as scheduled, without justifying their absence. It is noticeable that in both cases the prosecutors did not have attorneys, and one has to wonder if they had understood the importance, i.e., legal consequences of their failure to appear at the trial and the loss of their rights.

***

Based on the presented case law on Article 146 of the Criminal Code, it can be concluded that the criminal law protection of citizens' rights before the courts in this matter is still insufficiently developed, i.e., has not taken root.

First of all, it is evident that the number of cases initiated at Serbian courts is small. There is a stark contrast between the 28 cases of this type initiated between 2015 and July 2020 and the frequency of violation of the right to personal data protection in the Republic of Serbia in the same period, presented in the annual reports of the Commissioner and the recently published Privacy Violations Database.[8]

The statistics show that in 93% of cases citizens who see themselves as victims of violation of the right to privacy assume the role of the prosecutor. Some of the initiated proceedings are terminated as a result of procedural omissions. Private lawsuits (those filed by citizens - victims of violations of rights) often do not contain the elements which are necessary for the case to be initiated at all. The analyzed sample shows that in most cases, private prosecutors without a proxy either miss the three-day deadline imposed by the court or do not know how to supplement or correct the private lawsuit according to the court's instructions in order to enable the court to act on it. In that regard, it is not realistic to expect any significant improvement of the case law when it comes to the protection of citizens' rights in cases of unauthorized personal data processing if the trend of private lawsuits filed by injured parties on their own, without an attorney, continues.

On the basis of just two judgments of conviction issued in this period, one cannot tell whether the courts' sentencing policy for this criminal offense is lenient or strict. The fact that Serbian courts issued only two judgments of conviction for Article 146 of the Criminal Code between 2015 and July 2020, and that, on top of that, they imposed suspended sentences in those cases leads to the conclusion that no major privacy violation case, either in terms of seriousness of consequences for the injured party, or in terms of the number of injured parties, has yet been received by criminal departments at Serbian courts. Reasons for the absence of such cases from courts should certainly be sought outside the courts, bearing in mind the competence for initiating such cases.

One of the reasons may be a small number of cases initiated by public prosecutors, i.e. a small number of indictments filed to courts by public prosecutors' offices. Based on the presented

[4] Basic Court in Jagodina, K. Br. 144/16 od 23.08.2016.
[5] Higher Court in Jagodina, Kž.1 – 254/2016 od 20.12.2016.
[6] Basic Court in Stara Pazova, Court Unit in Inđija K 11/ 17
[7] Basic Court in Novi Sad K.1117/15
[8] The privacy violations database is available at: https://monitoring.mojipodaci.rs/

findings on the relevant case law, in the period covering more than five years competent public prosecutors' offices appeared as prosecutors in two cases alone. We will review the reasons why this number is not higher in the continuation of this analysis, in the part that refers to the analysis of action of public prosecutors' offices on the Commissioner's criminal reports.

Action of public prosecutors' offices on the Commissioner's criminal reports

According to the new LPDP, the Commissioner is entrusted with the authority to conduct inspection supervision of the implementation of the LPDP. Under the previous LPDP, which was in force until 2019, the Commissioner had the competence to conduct supervision (not inspection supervision, though). The competence entrusted to the Commissioner by both the old and the new Law is to submit, following supervision, a criminal report to the competent public prosecutor's office within the scope of the Commissioner's competence, where above-mentioned Article 146 of the CC is the most relevant for this analysis.

This analysis focuses precisely on the action of public prosecutors' offices under Article 146 paragraph 3, in the part that refers to the action on criminal reports submitted by the Commissioner to public prosecutors' offices.

Information on criminal reports were obtained from the Commissioner through official channels, in accordance with the Law on Free Access to Information of Public Importance, and they specified the: date of each report, case number, CC article to which report refers and information on the public prosecutor's office to which the report was submitted.

In the period between January 1, 2015 and July 2020, the Commissioner submitted a total of 17 criminal reports for personal data protection offenses to competent basic public prosecutors' offices, all of them referring to the aforementioned Article 146 of the Criminal Code. The reports were sent to the Basic Prosecutors' Offices in Niš, Kragujevac, the First and the Third Basic Public Prosecutors' Offices in Belgrade, as well as the Cyber Crime Department of the Higher Public Prosecutor's Office in Belgrade.

We reviewed the action of public prosecutors' offices by sending requests for access to information of public importance. In the requests, we asked whether and how the relevant public prosecutor's office acted on the criminal reports submitted by the Commissioner and requested information or explanation on the basis of which we could determine the status of each case established on the basis of relevant criminal reports. We also requested to be sent copies of indictments, if they had been filed and if criminal proceedings had been instituted, along with the information on the stage of proceedings on the date of receipt of the request and the number of cases in each stage of the proceedings.

All five public prosecutors' offices sent their answers within the statutory time frame.

a) What can we learn about the action of public prosecutors' offices on these criminal reports?

The responses of public prosecutors' offices to the requests for access to information of public importance pointed to different ways of applying transparency standards by different public prosecutors' offices. One of the public prosecutors' offices provided detailed explanations for its actions, outlining concrete steps in different stages of the proceedings. By contrast, most public prosecutors' offices to which the requests had been sent decided to restrict the information provided, usually only by quoting the stage in which the proceedings currently were.

Specifically, the First Public Prosecutor's Office in Belgrade was the leader regarding the application of transparency standards, providing records from the SAPO[9] register for each individual case, redacted in appropriate places.

This Prosecutor's Office thus provided detailed information on its action: the overall movement of cases, who had been assigned the case, who the processors were, how many requests for collecting necessary information (PO requests) and when were sent to the police, whether the mechanism of repetitive letters, i.e., requests for urgency, had been used, as well as reports to the Internal Affairs Sector of the Ministry of Internal Affairs of the Republic of Serbia (RS MoI IAS) in case of non-compliance. Evidently, the First Public Prosecutor's Office in Belgrade provided this type of information believing that this was information of public importance, i.e., that there was no other statutory interest that should be protected by denying access to this information.

With the exception of the first answer of the First Public Prosecutor's Office in Belgrade, the submitted answers do not leave much room for analyzing the actions of public prosecutors' offices, since they only note the stage in which the cases are. This type of practice when it comes to responding to requests for free access to information of public importance should certainly be improved, in view of the fact that public prosecutors' offices, like all other public authorities, should be accountable to the public for their work. One of the necessary preconditions for this is for the public to get relevant information about their work, where the grounds for restricting the right of the public to know should be used more rigorously and in a more substantiated manner.

b) How did public prosecutors' offices act on criminal reports?

On the basis of the answers, we can determine that there is a common feature of the actions of public prosecutors' offices on the Commissioner's criminal reports – not a single report had been dismissed, or used for filing an indictment or a motion to indict or for implementing conditionally deferred prosecution.

In order to understand how public prosecutors use mechanisms for collecting facts with the aim of determining grounds for suspicion for a particular criminal offense, we need to start from the most basic one, which is the request for collecting necessary information (PO request) which the prosecution sends to the police. In view of the prosecutor's role in criminal proceedings – to lead the pre-investigative[10] and investigative[11] proceedings – the PO request should contain the most precise possible description of the facts which the public prosecutor needs for determining the elements of the crime, i.e. existence of grounds of suspicion. This also applies to the offenses in the focus of this study, i.e. violations of the rights referred to in Article 146 of the Criminal Code, which are submitted to the public prosecutor's office by the Commissioner.

Furthermore, in the pre-investigative stage of the proceedings, the "threshold" of proof is rather low and facts obtained on the basis of PO requests are used for proving the grounds for suspicion,[12] which upon the completion of the investigation should grow into justified suspicion[13] and an indictment that requires a much higher standard of proof for a particular offense.

If the prosecution fails to get this information from the police within a set period of time, it can use requests for urgency, which are sent in the letter format to the police officer on the case or to his superior.

[9] Standardized software – database of the Administration for the Enforcement of Criminal Sanctions.
[10] Criminal Procedure Code, Article 43 paragraph 2 item 1.
[11] Criminal Procedure Code, Article 43 paragraph 2 item 3.
[12] Criminal Procedure Code, Article 2 paragraph 1 items 17 and 18.
[13] Criminal Procedure Code, Article 2 paragraph 1 item 19.

If, despite requests for urgency to the police officer, i.e., the head of that unit, the public prosecutor's office does not receive a response with necessary information, it can then can only file a disciplinary report to the Serbian MoI Internal Affairs Sector. After that, the Internal Affairs Sector will examine whether the police officer had violated his duties as a result of acting (or omission to act) on the relevant PO.

Specifically, based on the data we received, only the First Basic Public Prosecutor's Office in Belgrade had resorted to the mechanism of reporting to the Serbian MoI Internal Affairs Sector, and this happened just in one case. We see this as the key shortcoming when it comes to the action of public prosecutors' offices on the Commissioner's criminal reports; one gets the impression that public prosecutors' offices are not taking all the measures at their disposal and therefore cases "do not move", i.e., have no outcome.

On the basis of submitted documents, it is evident that neither the prosecution nor the police are proactive in their communication, in view of their legal competences. In other words, in its PO requests the public prosecution should be specific enough regarding the facts it needs for concluding whether the legal standard for further action on the criminal report has been reached. Rather than just quoting the legal provisions pertaining to the crime, the PO request in its legal aspect should, in fact, identify specific operations that the police should take. On the other hand, police should request from the prosecutor to specify the PO if it only contains legal provisions without any reference to the type of information or operations needed for determining whether there are grounds for suspicion or not. Otherwise, shifting responsibility from one authority to another without exhausting all legal mechanisms for proper communication between the public prosecutor's office and the police deprives citizens - victims of violations of rights – of effective pre-criminal and criminal proceedings.

***

Before making any conclusions on the action of public prosecutors' offices under Article 146 of the CC, we should be aware that this analysis fails to include the action of public prosecutors' offices on criminal reports filed by other authorized entities (e.g., victims of rights violations, or other public institutions). In that regard, prosecutors' offices might have completed proceedings when they acted on such reports in certain cases, public, e.g., through conditionally deferred prosecution. However, in view of the Commissioner's competence and authority referred to in the LPDP, a cause for concern is the fact that not a single criminal report filed in 2015 or later by the Commissioner (as probably the most competent body for preparing a substantiated criminal report for the offense referred to in Article 146 of the CC) had an outcome.

In view of the fact that the public prosecution is required to prosecute perpetrators of this crime *ex officio*, it can be expected to demonstrate a much greater level of activity in its work. The job of a prosecutor cannot end once he sends a request for collecting information to the police, without "checking" whether the police are acting on that request. On the contrary, the competent prosecutor must be proactive, duly check whether the police are complying with the request, whether they are taking all actions, collecting necessary information and submitting them regularly and in a timely manner to the competent prosecutor. If the police fail to act in accordance with his request, the prosecutor has different mechanisms at his disposal – from repetitive letters and requests for urgency, to reporting to the MoI Internal Affairs Sector that his request has not been observed. Based on the above, we can conclude that prosecutors do not take any of these actions, which, in turn, only gives police room not to act on PO requests, since they will certainly suffer no consequences for their inaction.

On the other hand, we also have to review the role of the person filing the criminal report in the similar context – which is the Commissioner in this case. On the basis of collected documents, we could not determine whether and how the Commissioner acted after filing criminal complaints to

the public prosecutor's office. We believe that the Commissioner's job should not end after filing criminal reports, but that this should only be the first in a series of consecutive actions ensuring the adequate protection of the injured party from the violation of rights. Regular communication with the injured party - if there are available mechanisms for this purpose, which depends on the case and complaints against the work of the public prosecutor – is just one of the key activities that the Commissioner should undertake alone or, if possible, in cooperation with the injured party. This would be a type of lawful pressure on the public prosecution that would ensure a more effective and more efficient action in the pre-criminal proceedings and speed up this stage, resulting in the issuance of the order and implementation of an investigation.

Since the Commissioner, and not the injured party, was the one who submitted criminal reports in the relevant cases, ways for possible improvement of cooperation between the Commissioner and injured parties should be reviewed. We believe that, whenever the Commissioner informs the public about a filed criminal report, he may also announce that his office is at the disposal of the injured party for further cooperation regarding all important procedural matters related to the report, in order to ensure that competent institutions act in favor of the injured party. Also, the Commissioner should duly inform the injured party about all actions he has undertaken and suggest to the injured party which steps to undertake.

As a result, in communication with the injured party, the Commissioner can inform him about all mechanisms he can use in a situation when the prosecution is doing next to nothing in the proceedings, i.e., when it does not react to the criminal report. This specifically refers to assisting the injured party to draft a complaint to the immediately higher prosecutor's office. Also, if the complaints of the Commissioner and the injured party remain unsuccessful in the pre-criminal stage of the proceedings, the injured party has the *locus standi* to file a constitutional appeal for an ineffective investigation, as a procedural aspect of the violation of rights referred to in Article 8 of the Convention. The Commissioner can assist the injured party in drafting the constitutional appeal. If the constitutional appeal fails, i.e., if the Constitutional Court dismisses or rejects the constitutional appeal, the injured party may file an application to the European Court of Human Rights also for the violation of the right to respect for private and family life.

Activities of Serbian misdemeanor courts in the implementation of the new Law on Personal Data Protection

The implementation of the new LPDP began in August 2019, and in this part of the analysis, we present the case law of misdemeanor courts in the relevant period. We should be aware that there were difficulties in obtaining information on current misdemeanor proceedings related to the implementation of the LPDP, because the registers of misdemeanor courts do not distinguish between proceedings under the old and the new LPDPs. For the purpose of clarification, information collected from misdemeanor courts were cross-referenced with the information obtained from the Commissioner.

Between August 2019, when the implementation of the new Law started, and January 2021, the Commissioner submitted to Serbian misdemeanor courts a total of eight motions for initiating misdemeanor proceedings for violations of the new Law on Personal Data Protection. The Misdemeanor Courts in Sremska Mitrovica, Leskovac, Lazarevac and Niš have one case each, while four proceedings are being held before the Misdemeanor Court in Belgrade. Moreover, two proceedings were completed. The numbers received from misdemeanor courts were larger, but we cannot tell with certainty whether these cases were initiated under the new or the previous Law on Personal Data.

Conclusion

Despite the EU and the Council of Europe focus on the issue of personal data protection in the last decade and despite the adoption of the EU General Data Protection Regulation which focuses on individuals and the protection of their privacy, the practice of Serbian authorities and competent Serbian institutions, regrettably, still lags behind these standards. In view of everything presented above regarding the actions of courts and public prosecutors' offices, we can conclude that Serbia currently does not offer adequate legal protection to injured parties - victims of personal data abuse and misuse.

The criminal law protection of injured parties for the criminal offense referred to in Article 146 of the Criminal Code is neither efficient nor effective. Not a single criminal report filed by the Commissioner in the previous five years has had an outcome. This is also the main reason why the case law on Article 146 of the CC has not been developed.

On the basis of everything presented in this analysis, one gains the impression that competent authorities (MoI and public prosecutors' offices) are not too interested in prosecuting the perpetrators of this crime. If this practice continues, the absence of pre-investigative and investigative actions, failure to undertake legal obligations with the aim of prosecuting perpetrators and the passivity of institutions will doubtless eventually result in systemic violations of the right to protect the private and family life of individuals, because of ineffective and inefficient investigations.

Misdemeanor courts have yet to develop their case law on the implementation of the new Law on Personal Data Protection. The practice of the Commissioner in the first year of implementation of the new LPDP mainly focused on the education of entities that have obligations under the Law, relying on admonitions when irregularities in the implementation of the LPDP are observed during the exercise of competences. We believe that, in general, this approach has been justified, in view of the fact that the culture of personal data protection has still not taken root in Serbia, and that the entities that have obligations under the law had less time for harmonization than their counterparts in the European Union between the adoption and the beginning of implementation of the General Data Protection Regulation. However, since the new LPDP has been implemented for a year and a half, since there is less and less reason to call the law "new", and since the issue regulated by LPDP is not really new in the Serbian legal system, we believe that in the following period, the Commissioner's practice should focus more on initiating misdemeanor proceedings, i.e., imposing punishments in the case of violation of the Law. Despite the low statutory penalties, we believe that if punishments became certain, they might create an additional reason for making improvements in this field, both in the public and private sectors.

Personal data protection in healthcare

Author: Jelena Adamović, Share Foundation

Abstract

The outbreak of the COVID-19 pandemic resulted in a need for collecting and processing data of a large number of citizens, including medical data that have particular importance in this context, because this is exactly the type of data needed by institutions tasked with "fighting" the pandemic. However, from the citizens' point of view, this type of data is particularly sensitive and subjected to a stricter legal protection regime. During the pandemic in Serbia, the possibility of mass electronic processing of such data and creation of unified databases came into the limelight. First of all, the Government of the Republic of Serbia established a special information system, COVID-19 IS, which should contain all data of importance for monitoring the epidemiological situation, including sensitive medical data of all citizens who find themselves in the epidemiological surveillance system in any capacity. In addition to this, the existing e-Zdravlje (e-Health) portal, which, even under regular circumstances, serves different purposes within the healthcare system as the primary online communication system between citizens and healthcare institutions, has been given new purposes (e.g., COVID-19 self-assessment test or the platform for receiving test results). These online platforms are not subjected to exceptions and restrictions that apply within the legality protection and assessment regime under the provisions of the Law on Personal Data Protection. However, obligations referred to in this Law have not been fully respected in their functioning, primarily when it comes to transparency and compliance with the integrity principle.

Description of the issue

Introduction

The personal data protection is regulated by the Law on Personal Data Protection (hereinafter referred to as: the **Law** or **LPDP**),[14] as the general regulation. In that regard, it is important to note that the Law recognizes medical data as sensitive, i.e. defines them as a special type of data, and therefore envisions additional, stricter conditions for their processing. In addition to this, different sectoral regulations in addition to the LPDP, such as the Law on Healthcare or the Law on Patients' Rights, are also relevant for the rules implemented in the healthcare system of Serbia. However, during the pandemic, the provisions of the Law on Protection of the Population from Infectious Diseases[15] are also relevant in addition to this general legal regime. Under Article 6 of this Law, the Government of Serbia adopted a decision on declaring COVID-19, caused by the SARS-CoV-2 virus, an infectious disease[16] and envisaged measures for its suppression, frequently amending this decision depending on the current situation.

Under the September 16, 2020 amendments to this decision, Serbian (and certain foreign) citizens arriving from countries with an unfavorable epidemiological situation, receive a written notice at passport control informing them that they are required to report to competent

[14] Law on Personal Data Protection (Official Gazette of the RS, No. 87/2018)

[15] Law on Protection of the Population from Infectious Diseases (Official Gazette of the RS, No. 105/2016 i 68/2020)

[16] Consolidated text of this decision is available at: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/odluka/2020/23/1/reg, accessed on February 10, 2021; Based on this Article of the Law, the Ministry of Health also issued the order on declaring an epidemic of the COVID-19 infectious disease, published in the Official Gazette No. 37 of March 19, 2020. The Official Gazette of March 15, 2020 included the Serbian Government Decision on declaring a state of emergency, which in fact enabled the restriction of certain constitutional rights, including the right to movement and the right to privacy.

institutions. Under the decision, the Ministry of Health issued guidelines for the implementation of the decision on declaring COVID-19, caused by the SARS-CoV-2 virus, an infectious disease *in the part which restricts the entry of persons in the Republic of Serbia*.[17] Under the guidelines, persons subjected to this epidemiological surveillance regime should use the electronic application form to report to the COVID-19 test center or the Institute of Public Health at: www.e-zdravlje.gov.rs. The guidelines themselves do not offer any other options for meeting this requirement. The Government of Serbia also adopted a conclusion on the establishment of a unified and centralized software solution, the COVID-19 Information System, envisioning the actions of all healthcare institutions with the aim of establishing a unified register of all cases related to the infectious disease caused by the coronavirus.[18]

The eZdravlje Portal – the self-assessment test as an epidemiological measure after a person's return from abroad

Neither the Government decision, nor the Ministry of Health guidelines that refer to Serbian citizens who return from abroad offer any other option for meeting the supervision reporting requirement but the electronic application to the address: www.e-zdravlje.gov.rs.. In practice, this means that such persons must open accounts on the eZdravlje platform in order to comply with the Ministry guidelines. Since practice has shown that a large number of citizens were unable to use this method, they were provided with the option to telephone one of the competent institutions to report. However, since this option has been forced by practice without being regulated, the exact manner in which sensitive personal data are collected in this case has not been regulated anywhere. Therefore, we can say that, inexplicably, this method of collection and processing of health data has remained without a clear legal basis.

As for applications via the eZdravlje portal, it is important to note that under regular circumstances, this portal, as the primary online system of communication between citizens and healthcare institutions, is used for different purposes within the healthcare system. Under the current epidemiological surveillance measures, it has been given an additional purpose, the Covid-19 self-assessment test. However, the first step encountered by any portal user is the login procedure, which can be done in different ways depending on the degree and manner of authentication required, which, in turn, determines the level of access to the system. Thus, the section of the portal where one can take the self-assessment test has the lowest level of protection. The only thing a user has to do in order to log in is to enter his/her LBO and health card numbers - which anyone who has access to the user's health card can have – without the need for any other authentication.

There are also other, safer registration and login systems, but they are used for other purposes. According to the information provided on the eZdravlje portal, there is another type of login that allows access to the section of the portal that contains additional health data, which requires a username and a password. However, even this login method does not let the user access all the data available on the portal. The highest level of authentication, requiring a qualified electronic signature or two-factor authentication, grants users full access to their health records, enabled through links with other systems and databases where these data and documents are held.

Based on the above, we can conclude that the logic applied in the development of the portal has been that not all health data are equally "sensitive" and that some deserve less and others more protection. Such logic has no grounds whatsoever in Serbian regulations governing personal data protection. Data which citizens who take the self-assessment test provide are certainly special personal data, which means that when a system for their processing was designed, the obligation

[17] The Guidelines were published in the Official Gazette No. 108/2020 and 116/2020.
[18] Government conclusion on the establishment of a single, centralized software solution – the COVID-19 information system (Official Gazette of the RS, No. 50/2020, 57/2020).

to apply technical and organizational protection measures suitable for the associated risks, including "privacy by design". and "privacy by default" standards referred to in Article 42 of the LPDP, had to be consistently implemented. Logging in to the eZdravlje portal for the purpose of conducting epidemiological surveillance in the way described above, which enables easy and simple access to such sensitive data, is certainly a sign that the relevant legal obligation has not been observed.

Another omission is that the data processing notice on the eZdravlje portal[19] does not contain any information regarding the use of the portal for self-assessment within epidemiological surveillance. In that regard, the transparency obligation has not been met. Therefore, at this moment, we do not know who the controller[20] of data collected through this test is, who accesses the data and for what purpose, how long the data are stored, whether the services of particular processors are used for processing, etc.

The COVID-19 IS

The COVID-19 Information System (COVID-19 IS), which contains all Serbian citizens' medical data of relevance in the pandemic, experienced a serious security incident in mid-April 2020, when the username and password for the system remained publicly available on the Rakovica health center website for eight days. This was long enough to enable the indexing of this page on Google, and although it was not visible on the website, it could be found by running an internet search.[21] After this incident, the Commissioner for Information of Public Importance and Personal Data Protection initiated the LPDP implementation supervision procedure. As a result of the supervision, the Commissioner issued a warning to the system controller, the Dr Milan Jovanović Batut Institute of Public Health, for omissions, which include the following: (i) absence of appropriate system protection measures, (ii) failure to make a data protection impact assessment, which was mandatory under the LPDP in this case, and (iii) failure to conclude a contract with system processors, primarily the Republic Health Insurance Fund, which is in charge of providing technical support to users.

While the obligations referred to in items (ii) and (iii) may look like the fulfilment of formal requirements referred to in the LPDP, this case shows us how far-reaching the consequences of the failure to observe minimum requirements of lawful processing may be. They are directly related to the omission referred to in item (i) that refers to protection measures, which, under the LPDP must always be directly related to the risks (which are significant in this case in view of the fact that these are sensitive data of all citizens of Serbia). If an appropriate impact assessment had been done before the system was put into operation, this would certainly have been an opportunity to foresee and minimize or eliminate risks.

[19] The notification is available at: https://www.e-zdravlje.gov.rs/helper-page/information/sh.html, accessed on February 10, 2021. Also, after login, the user encounters a link to the portal's Privacy Policy, although the page where the Policy is published cannot be accessed from the public part of the portal. In any case, this Privacy Policy does not apply to medical data themselves.

[20] As regards the data controller of the eZdravlje portal, the privacy information regulating its use under regular circumstances mentions the Dr Milan Jovanović Batut Institute of Public Health of Serbia as the controller. It also says that the Batut Institute collects, processes and manages the data on the portal in accordance with the law, delegated authorizations and obligations - without stating which law and which authorizations. The portal homepage says, however: "Welcome to the *eZdravlje* portal of the Ministry of Health of the Republic of Serbia." This inconsistency certainly creates confusion regarding the real controller and regarding the types of data, which also undermines the principle of transparency.

[21] The Share Foundation wrote about the incident and its detection: https://www.sharefoundation.info/sr/pandemija-jedne-lozinke/ and here: https://www.sharefoundation.info/sr/opomena-batutu-zbog-bezbednosnog-incidenta-sa-licnim-podacima-gradana/, accessed on February 10, 2021.

Recommendation on how to remove identified omissions

Systemic issues

Everything previously mentioned regarding the operation of the eZdravlje portal and the COVID-19 IS during the pandemic indicates that there are systemic issues in the implementation of LPDP rules by Serbian state authorities, including those that process particularly sensitive data. To begin with, whenever multiple bodies participate in the processing, it is not immediately clear which one is the processor and which one the controller, with all the relevant obligations. Bodies that have certain (general) competences under the law frequently start processing personal data for which a relevant legal basis either has not been determined or does not exist in the relevant case - which actually makes the processing illegal. The actions of these bodies leave the impression that compliance with the LPDP obligations is considered to be just an activity to which no attention is paid, and, as a result, the obligation to provide citizens with appropriate information about all circumstances of processing is often missed. Even if publicly available notices are provided, they are frequently incomplete, confusing and insufficiently informative. In addition to this, non-compliance with the data integrity and security principles results from the fact that the use of data processing systems is not planned carefully but "hastily," so that banal incidents occur, the way is paved for serious compromising of sensitive data, or citizens, who have the obligation to submit their personal data in this way, are deprived of safe online communication with authorities.

What should be changed

When it comes to the legal framework that regulates the collection and processing of data by state and health care authorities and institutions during the pandemic, one could say that it is satisfactory in principle. However, this conclusion is primarily based on the fact that the LPDP has transposed all relevant standards and rules referred to in the GDPR.[22] In addition to this, sectoral regulations, such as the Law on Patients' Rights, ensure additional protection in the field of privacy rights. However, since the pandemic dictates the need for the relatively frequent adoption of bylaws, some of which regulate certain personal data protection issues, on the basis of the above-mentioned examples we can conclude that the issuers of these acts do not pay enough attention to this fact. Therefore, whenever regulations are enacted, all circumstances relevant for processing need to be properly regulated, i.e. there must be insistence, prior to the enactment of regulations, on appropriate consultations with relevant experts in order to avoid complications and irregularities in the application of regulations in daily practice.

When it comes to the practical implementation of regulations, there is evidently a complete lack of observation of principles stemming from the "privacy by design" and "privacy by default" concepts. Therefore, one needs to insist on the idea that the observation of privacy and personal data protection do not represent only the fulfillment of legal formalities, but that privacy, as a value, needs to be intrinsic to all actions of competent authorities. Therefore, the above-mentioned situation can certainly be explained, *inter alia,* by the lack of knowledge about this topic of employees in the relevant institutions (both of the issuers of by-laws and employees working on their implementation). Thus, efforts should be made in this area to raise awareness and implement training on specific topics, depending on the type of work that employees perform within the system.

[22] Regulation (EU) 2016/679 (General Data Protection Regulation).

Personal data protection in education

Author: Jelena Adamović, Share Foundation

Abstract

The establishment of the Unified Education Information System (JISP) has been governed by applicable regulations in the area of education since 2017, when the new Law on the Fundamentals of Education System was adopted. This and other relevant laws in this area have since been amended on multiple occasions, while the competent authorities have enacted bylaws that should regulate the operation of the JISP. Given the amount and sensitivity of data that should be stored in this system, the number of persons to whom the data refer, the fact that the data refer to minors, as well as links with other, also sensitive information systems, a source for concern is a lack of publicly available information, both on the establishment and functioning of the JISP, and on its link with the electronic grade book, which, as the main register of students, is mandatory in primary and secondary schools under the law. In addition to this, the integrity of electronic records containing student data was compromised last year. According to information publicly shared by some parents, there is a suspicion that children's data stored in electronic grade books and/or JISP were made available to a private company, which was to offer parents a commercial platform for online communication with schools, which would include some functions that are not available in electronic grade books maintained by schools.

Description of the issue

Introduction

The Law on the Fundamentals of Education System[23] (**ZOSO**) has envisioned the establishment of a Unified Education Information System (**JISP**) as a completely new system in this area, which should primarily serve the purposes of the Ministry of Education, Science and Technological Development (hereinafter referred to as: **the Ministry**). According to the ZOSO, the JISP should consist of several interlinked registers, including a register of children, pupils, adults, attendees, candidates and university students (including data on their parents or guardians),[24] as well as a register of educational institution employees. The JISP should therefore contain a huge number and scope of personal data, including sensitive data (e.g., data on financial status) and special data (e.g., health data) of a large number of persons, from the preschool age to the end of schooling, at the national level. Thus, through the establishment of the JISP, the Ministry of Education, as the controller, will control a huge amount of personal data, unprecedented in its practice. According

[23] Law on the Fundamentals of Education System (Official Gazette of the RS, No. 88/2017, 27/2018 - other law, 10/2019, 27/2018 - other law i 6/2020).

[24] According to Article 177 of the ZOSO, the following is contained in the register of children, pupils, adults and university students: 1) data used for determining the identity of a child, pupil and adult: UEN, sex, date, place and country of birth and residence; 2) data used for determining the educational status of a child, student and adult: previously completed education program, level of education, qualification codes, institution, group, class and department, type and duration of the program, language of education and mother tongue, nationality (declaration of nationality is not mandatory), elective programs, education according to individual curriculum, grades, passed exams, commendations and awards received during education, absence, discipline and issued public documents; 3) data used for determining the social status of a child, pupil and adult: whether they belong to socially vulnerable categories of the population, living conditions and family status; social status of parents, or other legal representative: acquired professional title, occupation and type of employment; 4) data used for determining the functional status of a child, pupil and adult: data obtained on the basis of assessed need for additional educational, health and social support, data on the existence of functional problems concerning vision, hearing, gross or fine motor control, intellectual difficulties, as well as communication, behavior, and socialization difficulties.

to the provisions of the ZOSO, the JISP will be directly linked to a large number of other databases that contain personal data of Serbian and foreign citizens.[25]

Moreover, over the past few years, the Ministry has also been involved in a project of digitalization of mandatory records (popularly known as "grade books") of children, pupils and university students, run by preschool institutions, primary and secondary schools and faculties in Serbia. Although according to the ZOSO and other sectoral regulations,[26] educational institutions have the sole responsibility for maintaining these records, the Ministry launched a project aimed at introducing an electronic grade book, **esDnevnik**, which started in 60 and was completed in more than 500 primary and secondary schools. According to the Ministry website, after the end of the pilot project, the decision was made to include all schools in the central esDnevnik project in the 2018-2019 school year.[27] However, once the transition from hardcopy to electronic grade books started, students' parents did not receive the necessary information regarding the project, which they were entitled to get under data protection regulations. In November 2019, the first concerned parent addressed the Share Foundation, which has since sent several requests for access to information of public importance to the Ministry for the purpose of collecting relevant information. Moreover, in May 2020, a private company (an entity allegedly related to the company that participated in the esDnevnik pilot project) developed a software called eŠkola, which should operate in a similar manner to the esDnevnik, though with additional options for parents, depending on the "package" of services they choose and are willing to pay for.[28] The Share Foundation and the media were informed about this by parents who suspected that the eŠkola service provider had gained unauthorized access to their children's data, which they determined by logging in to the eŠkola portal using the same credentials they use to access the esDnevnik.

The JISP

According to the ZOSO, the Ministry is the data controller in the JISP. To be able to perform the tasks within its competence, the Ministry currently does not have access, even remotely, to the number and type of data that will be in the JISP registers. Referring to the JISP data processing purposes, the ZOSO itself says that these are primarily statistical purposes, monitoring of different indicators in order to perform tasks within the competence of the Ministry or conducting research.[29] In that regard, the first question that must be asked is - why and exactly for which purposes should the Ministry process so massively the personal data of such a large number of persons, i.e., why the Ministry needs personal rather than anonymized data.

In addition to this, in response to Share Foundation's request for free access to information, the Ministry said it believed that the use of JISP did not require an impact assessment in accordance

[25] See Article 181 paragraph 4 of the ZOSO.
[26] Law on Primary Education (Official Gazette of the RS, No. 55/2013, 101/2017, 10/2019 i 27/2018 – other law), Law on Secondary Education (Official Gazette of the RS, No. 55/2013, 101/2017, 27/2018 – other law and 6/2020).
[27] Available at: http://www.mpn.gov.rs/elektronski-dnevnik-esdnevnik/?lng=lat, accessed on February 10, 2021.
[28] Available at: https://eskola.rs/, accessed on February 10, 2021.
[29] Referring to purposes, Article 181 paragraph 2 of the ZOSO quotes **statistical purposes** (i) ensuring the monitoring of indicators for conducting statistical surveys and analyses of quality, efficiency and effectiveness of the education system [...] for the purpose of planning and undertaking measures of education and enrollment policy, (ii) undertaking preventive measures for reducing the number of dropout children, pupils and adults at all levels of education, (iii) monitoring also includes the progress made by students, (iv) monitoring the quality of study programs, as well as measures in accordance with labor market needs and greater employability, (v) conducting national and international research and participation in comparative and evaluation studies in order to create and improve education policy [...], (vi) monitoring the professional status as well as the coordination and organization of professional development of employees, (vii) analyzing the situation regarding the financing of the education and higher education systems; (viii) reporting on educational indicators in accordance with undertaken international commitments and participation in European Union cooperation programs in the field of education and higher education, as well as (ix) efficient performance of other tasks within the competence of the Ministry.

with the Law on the Protection of Data Protection (**LPDP**), explaining that the relevant information system was protected by the appropriate technical and organizational protection measures. According to the LPDP, such an assessment is mandatory whenever it is likely that some type of processing, and in particular the use of new technologies, will **result in high risk to the rights and freedoms of natural persons**, in view of the nature, scope, circumstances and purpose of processing. In view of all the above, it seems obvious that the establishment of a system such as the JISP and the Ministry's direct access to personal data of Serbia's entire population represents an extremely high risk to the rights and freedoms of all Serbian citizens who will in future, due to the mandatory nature of primary education, will have to be in this system.

The esDnevnik

Although, according to the ZOSO and relevant laws, educational institutions should have the right to decide on the way in which electronic grade books will be maintained, in practice this decision was made for them by the Ministry. Although the ZOSO and other sectoral laws are confusing when it comes to regulation of the link between the JISP and the electronic grade book, practice has already provided some answers. According to available information, all public primary and secondary schools in Serbia are already using esDnevnik for electronic record-keeping,[30] within a project for which all contracts with service providers (processors) have been concluded only by the Ministry. Although this solution can partly be understood from the aspect of efficiency, it raises the issue of how much **schools, as the controllers of data** processed within esDnevnik, can in practice fulfill their obligations towards data subjects, i.e., exercise their rights towards data processors. According to information obtained within the Share Foundation research, parents who addressed schools in an attempt to obtain information to which they are entitled under the LPDP were referred by the school staff to the Ministry for answers. The esDnevnik platform itself does not contain the privacy policy or a notice on personal data processing that is available to parents. Also, since all schools currently use the same platform for electronic record-keeping, the issue is raised of integrity and security of such a software solution.

The eŠkola

Trying to register to the esDnevnik portal, a number of parents received a notification in May 2020 that they could register at https://moja.eskola.rs/ using **the same access data** they use for logging in to the esDnevnik. When they registered to the new eŠkola platform, they received an offer for the commercial use of this platform through certain packages (family and standard) and were also shown the complete data of their children contained in the electronic grade book.[31] Asked about this, the Ministry said that the esDnevnik software for improved services, which is offered for a fee, is not intended for state educational institutions, but for all other schools accredited for education, which have been founded by another legal or natural person. However, no clear explanation has been provided for the fact that a private company has been given the opportunity to use the access credentials of parents of state-run school students and personal data contained in the esDnevnik. At the Share Foundation's request for free access to information, the Commissioner for Information of Public Importance and Personal Data Protection replied that the procedure of supervision of the Ministry had been initiated in this case, and that the public would be notified about its results, which has not happened so far.

[30] Available at: https://esdnevnik.rs/, accessed on February 10, 2021.

[31] Media information is available at: https://www.danas.rs/drustvo/ko-je-privatnoj-firmi-dao-podatke-djaka/; https://www.danas.rs/drustvo/moguce-sprovodjenje-nadzora-u-ministarstvu-prosvete/?fbclid=IwAR0kW5Gt047vZuy0QHuLWXYUsZptiaB-gDX3jc36Sr0o6WXsrgH-sPkABxU, accessed on February 10, 2021.

Recommendations on how to remove the identified omissions

Systemic issues

The establishment of the JISP in accordance with provisions of the applicable ZOSO violates several principles that are mandatory under the LPDP. First of all, it appears that there is a violation of the principle of **restriction in relation to the purpose of processing**, in conjunction with the **principle of minimization**, because the Ministry has been awarded the management of a huge amount of personal data pertaining to all children throughout the education process as well as their parents (i.e., which is virtually the entire population), although only anonymized data that could be provided by schools should be enough for the Ministry to perform its tasks.

Also, according to the ZOSO, data in the register of children, pupils, adults and students are stored permanently (with the exception of data on social and functional status), which is an obvious violation of the **principle of restricted safekeeping**, again taking into account the purposes of data processing conducted by the Ministry and regulated by the ZOSO.

Another source for concern is the Ministry's position in the implementation of ZOSO provisions and throughout the esDnevnik establishment project, which has been reactive and defensive in the face of pressure by parents, requests for free access to information and media inquiries, and completely deprived of proactivity that would be needed under the described circumstances in accordance with the principle of **fairness and transparency**.

The case of the eŠkola platform is just an indication that the Ministry is not guided by the best interests of parents and children and directly brings into question the security and safety of data over which the Ministry, owing to its role in the esDnevnik project, already has control. The incident in which a private company was allowed to access the esDnevnik login credentials and children's data referred to therein also violates the **principle of integrity and confidentiality**.

Finally, the Ministry's position that the development of an **impact assessment on the personal data protection** is unnecessary is more than dangerous. Furthermore, it could be said that JISP is a "textbook example" of a situation in which this assessment would have to be mandatory according to the LPDP rules.

What would need to be changed

The establishment of JISP has had great importance for all citizens of Serbia, because this is an unprecedented information system when it comes to the type and amount of data which it should contain according to current regulations, which means that the intrusion into privacy by a state body such as the Ministry is huge. In view of the Ministry's legal competences, it would be necessary thoroughly to review and revise the need for its direct access to personal data, i.e., to make an assessment of the types of data that the Ministry needs to have in order to be able to achieve the, primarily statistical, purposes of processing entrusted to it under the ZOSO and other relevant regulations.

Also, the entire process of JISP introduction should be accompanied by an adequate public debate among the professional public as well as citizens, because of the far-reaching consequences to privacy that such an information system might have.

Personal data processing through the video surveillance of public areas

Author: Kristina Kalajdžić, Partners Serbia

Facial recognition technology threatens to replace traditional methods which states, and primarily law enforcement agencies, apply with the aim of improving the safety of citizens. Moreover, this technology affects our daily lives and the subjective experience of freedom we have as individuals within our community. When someone observes us, we feel psychological pressure, which, in turn, makes us feel less free. In an age when many believe that privacy is outdated, international and domestic regulations should yet provide appropriate responses to the challenges of technological development.

For the last ten years, facial recognition cameras have been used globally, from China, through the UK to America. Although they have been developed as an additional tool for the protection of persons and property and more efficient capture of crime perpetrators, the issue has been raised of the real effectiveness of such video surveillance systems, as well as of potential abuse as a result of these technologies.[32] Although much attention is being paid to the improvement of these technologies in terms of hardware and software, it seems that less has been done for the development of rules and procedures ensuring the legal and ethical use of video surveillance systems. Negative international examples, primarily those from China, show that these technologies can be used as a tool for mass surveillance and control of citizens. Also, reports on the efficiency of video surveillance systems show that these technologies are insufficiently reliable and that they cannot replace the traditional methods of detection of crime perpetrators.

A study, which the *Big Brother Watch* organization conducted in 2018 by sending requests for free access to information of public importance to UK police departments, revealed that cameras with facial recognition software proved not to be an effective tool for detecting perpetrators. According to this study, on average (depending on the relevant police administration), as many as 95% of "matches" generated by facial recognition technology wrongly identified the perpetrator of the criminal offense. [33]

In addition to the efficiency issue, these technologies have a potentially negative impact on our rights and freedoms, primarily the right to privacy of individuals and other rights such as freedom of assembly, freedom of speech, etc.

Over the last two years, the Republic of Serbia has also initiated procurement procedures for video surveillance technologies using facial recognition programs. Examples of Serbian public authorities' activities aimed at planning and setting up surveillance systems demonstrate a lack of awareness of the importance of personal data protection, insufficient knowledge about regulations and obligations of authorities regarding personal data protection in the establishment of surveillance systems, as well as a lack of accountability of competent authorities in case of violations of the Law on Personal Data Protection.

[32] Partners Serbia, „Video nadzor: sredstvo za unapređenje bezbednosti ili kršenje privatnosti građana?" (Video surveillance: a means for improving security or for violating citizens' privacy), Belgrade 2020 https://www.partners-serbia.org//public/news/Studija-slucaja-Video-nadzor-Partneri-Srbija(2).pdf

[33] More about this in the analysis: "Face Off The lawless growth of facial recognition in UK policing" https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

Legal framework in the video surveillance area and practice of bodies of public authority in the Republic of Serbia

The video surveillance area has not been regulated systematically in the Republic of Serbia. Individual provisions concerning video surveillance are scattered in the laws regulating the operation of police and other security services, while the introduction of video surveillance systems has been allowed only to the police and entities providing private security services, where the work of the latter is regulated by the Law on Private Security. In addition to this, there is also a disputed authorization for the surveillance of public areas and processing of biometric data, provided to the communal police under bylaws[34].

From the aspect of protection of human rights and freedoms, primarily the right to privacy and personal data protection, public authorities that set up video surveillance systems should harmonize their actions with the new Law on Personal Data Protection.

Although the Law on Personal Data Protection does not specifically define the obligations of controllers regarding video surveillance systems, this, of course, does not mean that public authorities do not have any obligations regarding citizens' personal data protection. The use of video surveillance systems belongs to high-risk personal data processing activities because of the amount and types of personal data collected through these technologies. Thus, under the Law on Personal Data Protection, "If it is likely that some type of processing, especially through the use of new technologies and taking into account the nature, scope, circumstances and purpose of processing, will put the rights and freedoms of individuals under high risk, the controller shall, before starting with the processing, assess the impact of planned processing activities on personal data protection",[35] and if it turns out during the preparation of the impact assessment that the planned processing operations could put the right to personal data protection under high risk, the controller is required to request the opinion of the Commissioner before starting with the relevant processing actions[36] ("commissioning" of the video surveillance system). Also, during the establishment of a video surveillance system, the body of public authority (controller) is required to implement appropriate technical, organizational and staffing measures in order to ensure the appropriate level of security against the potential risks to personal data that may be caused by data processing activities.

However, the practice of public authorities has shown that once a video surveillance system is established, little attention is paid to assessment of risk to the right to personal data protection, as well as measures to eliminate/reduce these risks.

The Ministry of the Interior "Secure City" or "Safe City" project, under which the introduction is planned of a video surveillance system with facial recognition software, is the first such attempt in the Republic of Serbia. It refers to the introduction of more than 1,000 cameras throughout the capital. The public was informed about the project in January 2019 by the then Minister of Interior Nebojša Stefanović and Police Director Vladimir Rebić, who in several statements in early 2019 announced that almost 1,000 video surveillance cameras would be installed in Belgrade in 800 locations in the coming period, and that these devices would contain the facial and license plate recognition software.[37] According to subsequent 2019 statements by Minister Nebojša Stefanović,

[34] This refers to the Rulebook on the manner of recording in public places and the manner of announcing the intention to record, to which the communal police refers when recording public areas, i.e., processing of personal data of citizens, which violates the Law on Personal Data Protection, under which personal data processing activities may be conducted and authorizations for processing by state authorities may be given only on the basis of laws.

[35] Law on Personal Data Protection (Official Gazette of the RS, No. 87/2018) Art. 54. para 1, https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

[36] Ibid, Article 55.

[37] N1. Direktor policije: Ne postoji mogućnost zloupotrebe kamera (Police Director: There is no way that cameras might be abused): http://rs.n1info.com/Vesti/a458949/Direktorpolicije-Ne-postoji-mogucnost-zloupotrebe-kamera.html

"2,000 cameras will be installed in Belgrade by the end of next year."[38] Since this technology has a major impact on the citizens' right to privacy and other human rights, the public observed the implementation of this project with great attention. The public learned the most about the "Safe City" project through a case study conducted by Huawei, Serbia's strategic partner in this project. For promotional purposes, Huawei shared on its website some details regarding the chronology of this project – actually, the broader "Safe Society" projects, the negotiations on which began in 2011. In the case study, Huawei said that the project should include the eLTE technology, smart video surveillance, smart transportation system, construction of data centers, etc. Shortly after its parts appeared in the public, the study was removed from the company website."[39] The Ministry of Interior, which manages this project, however, revealed little and thus violated one of the main principles of the Law on Personal Data Protection - the principle of transparency of personal data processing. In 2019, it became known that before the implementation of the Project, the Ministry of Interior had not made the impact assessment of personal data processing on personal data protection. This document was subsequently drafted and sent to the Commissioner to provide an opinion (as one of the obligations envisioned in Articles 54 and 55 of the Law on Personal Data Protection). According to the publicly available data, the Commissioner's opinion on the impact assessment developed by the Ministry of the Interior was not positive. This document was jointly analyzed by the Share Foundation, the Belgrade Center for Security Policy and Partners Serbia, and the results were presented in the document "Analysis of the Impact Assessment of Processing on Personal Data Protection Using the Ministry of Interior Video Surveillance System."[40] The common conclusion of the Analysis is that the Ministry of Interior impact assessment meets neither formal nor substantive requirements referred to in the Law on Personal Data Protection, and that the Ministry of Interior should suspend the introduction of smart video surveillance systems until further notice.[41] In addition to this, the Analysis says that: "The central question that is raised in the case of smart video surveillance is its necessity, proportionality and efficiency, in view of the intrusiveness of this measure. Therefore, the data controller, i.e., the Ministry of Interior, has an additional obligation to prove the necessity of introduction of such a measure, its proportionality in relation to the desired purpose and the efficiency in achieving the objectives of data processing."[42] The public has not received these answers to date, and the installation and use of these systems by the Ministry of the Interior has meanwhile started.

On that occasion, the Share Foundation launched the „Hiljade kamera" (Thousands of Cameras) campaign in May 2020, inviting citizens to report the mounting of video surveillance cameras in the territory of Belgrade, as well as to sign the online petition requesting the abolishment of this system.[43] The aim of the campaign is to point out that the public still has no information about the real purpose of introduction of such mass video surveillance, measures for protecting the security of thus collected data, the price of the entire project, and the exact number and locations of mounted cameras. Between November 2020 and February 2021, over 14,000 citizens, 6,000 of them from Serbia, signed the petition, and with their help more than 1,000 cameras were detected at about 500 locations throughout Belgrade. All this shows that citizens recognize the dangers

[38] Mondo Portal, 30.07.2019: https://mondo.rs/Info/Beograd/a1208322/Nebojsa-Stefanovic-o-javnim-kamerama-u-Beogradu.html

[39] Partners Serbia analysis, „Video nadzor: sredstvo za unapređenje bezbednosti ili kršenje privatnosti građana?" (Video surveillance: a means for improving safety or for violating citizens' privacy), Belgrade 2020, page: 14, https://www.partners-serbia.org//public/news/Studija-slucaja-Video-nadzor-Partneri-Srbija(2).pdf

[40] Share, Partners Serbia and Belgrade Center for Security Policy, Analiza Procene uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora Ministarstva unutrašnjih poslova (An Analysis of the Impact Assessment of Processing on Personal Data Protection Using the Ministry of Interior Video Surveillance System):https://bezbednost.org/wp-content/uploads/2020/06/analiza_procene_uticaja_obrade_na_zastitu_podataka.pdf

[41] Ibid.

[42] Ibid.

[43] Website of the „Thousands of cameras" campaign: https://hiljade.kamera.rs/sr/pocetna/

from the misuse of such systems, that they want to play an active part in decision-making processes, as well as that they value their privacy.

Unfortunately, the case of the City of Belgrade is not the only one that points to the unlawful actions of public authorities within plans for introducing video surveillance systems. For example, the Sombor-based SOinfo.org portal in May 2020 announced that the introduction of a system for video surveillance of public areas had started in the city of Sombor, that one bidder had applied and was awarded a contract worth 105,392,325.00 RSD (excluding VAT). Partners Serbia requested from the Sombor City Administration information and documents justifying the public procurement of video surveillance systems, which were to be mounted in a large number of public areas, including squares, parks, roads, schools and kindergartens, as well as information on whether within preparations for the introduction of video surveillance, an impact assessment of such data processing on the personal data of the citizens of Sombor had been conducted. In its first response, the City Administration said that it had not made an impact assessment before initiating activities on the setting up of the video surveillance system, which represents a violation of the Law on Personal Data Protection. Answering our other questions regarding the justification of the introduction of the video surveillance system, the City Administration responded that "these systems do not raise the risk to the rights and freedoms of individuals in any way, and their only purpose is to improve citizens' safety."[44] However, the City Administration failed to submit documents corroborating claims that the introduction of video surveillance was necessary or a study or another document that could serve as the basis for a conclusion that the introduction of video surveillance would significantly improve citizens' security.

After that, Partners Serbia asked the Commissioner to supervise the implementation of the Law on Personal Data Protection in the City of Sombor and determine the legality of actions of local governance authorities in relation to all aspects of processing and personal data protection within the planned video surveillance system.

Following the Partners Serbia initiative, the Commissioner sent a letter to the City Administration requesting their position on the planned personal data processing activities, and asking whether the City planned to make an impact assessment of such data processing on citizens' privacy. The City Administration responded to the Commissioner's letter, stating, *inter alia*, that the planned introduction of video surveillance had been temporarily suspended due to the epidemiological situation, and that before beginning to *process data obtained through video surveillance, it would implement an impact assessment on personal data protection in accordance with applicable legal regulations and other documents regulating the relevant area.* In view of everything above, the Commissioner concluded in his communication to Partners Serbia that he would continue to monitor the Sombor City Administration's activities on the establishment of video surveillance, and that, if necessary, he would initiate inspection supervision in this case.

This example shows that local governments are still insufficiently familiar with personal data protection regulations, as well as obligations they have during different types of personal data processing. At the same time, the presented example is an indicator that a timely public reaction can help to improve the practice of public authorities in dealing with citizens' personal data.

Final remarks

Everything stated above illustrates that public authorities are not aware of the obligations imposed on them by the Law on Personal Data Protection when it comes to personal data processing of citizens on a massive scale. In addition to violating the Law on Personal Data Protection, public authorities apparently do not really intend to adapt massive personal data

[44] Response of the Sombor City Administration to the request for free access to information of public importance sent by Partners Serbia.

processing (such as the introduction of video surveillance systems in public areas) in such a way as to reduce risks to personal data protection of citizens and even when they implement the legally prescribed obligations, they do so only in order to formally harmonize their actions.

In view of the identified problems concerning video surveillance and other sectoral areas that we present in this publication, Serbia needs a synchronized and systemic national solution or harmonization of regulations in all fields with the Law on Personal Data Protection, and where necessary, also the adoption of bylaws or other acts that would regulate certain types of data processing in greater detail.

Previously, rumors could be heard in the public about the adoption of a special law that would refer to the establishment and use of video surveillance, but it has remained unknown whether the legislator plans to really draft such a regulation. Although this law would systematize the area of video surveillance, there is fear that bodies of public authority, primarily those that look after the safety of citizens, would thus be given broader powers in the establishment and use of such systems. In any case, such a regulation should, above all, guarantee at least the same standards of personal data protection as the umbrella law.

During a consultative meeting which representatives of the organizations participating in the Preserve Privacy - Resist Pressure project had with the Commissioner, we learned that there were plans to amend the Law on Personal Data Protection, and that one of the modifications could be the introduction of provisions regulating the mounting and use of video surveillance, as a special type of personal data processing.

Regardless of whether a special law is adopted, and whether the Law on Personal Data Protection is amended so as to include provisions regulating in more detail the area of video surveillance, it is important to emphasize that the existing legal framework ensures the protection of citizens' rights and prescribes standards and procedures that public authorities are required to apply in the planning and use of video surveillance systems, especially large-scale ones (such as in the examples described above), and even more so when those systems involve the use of facial recognition technology.

An analysis of the Law on Social Card in the context of personal data protection

Author: Danilo Ćurčić, Initiative A 11

Introductory remarks on the reform of the welfare system and adoption of the Law on Social Card

The reform of the welfare system, especially in the part that refers to financial social benefits (financial social assistance, increased financial social assistance, etc.), belongs to topics that have been discussed for years. In view of this, amendments to the Law on Social Protection[45], as well as the Law on Financial Support to Families with Children[46], have long been awaited. On the other hand, in the previous years, plans were made for adopting the Strategy for the Development of Social Protection for the period between 2019 and 2025. However, this process was slowed down after a May 2019 public debate, and the proposed public policy was not adopted.

Finally, the adoption of the Law on Social Card was mentioned as the key welfare system reform measure, enabling faster exchange of data between competent state authorities that maintain records on situations of importance for the exercise of social protection rights. As stated in the new Serbian Government exposé: "The reform priority aimed at better targeting of social benefits refers to the work on social cards that represent a unified insight into data on current and potential users." It was also stressed that "[social] cards [will] ensure greater visibility of citizens in the most difficult economic position in the system, enabling them to realize the right to necessary support in a timely and effective manner."[47] A public debate was held on the Draft Law on Social Card in the summer of 2019, when, after the presentation and collection of comments from the interested professional and other public, work on its preparation continued, after which in late January 2021 the Draft Law on Social Card was sent to Parliament, without a report on the public debate and without answering why some of the issues remained unresolved. The Law was adopted by the National Assembly on February 11, 2021. No amendments to the Draft Law on Social Card were filed, which means that the National Assembly adopted the text submitted by the Serbian Government.

This analysis provides a preliminary view on the provisions of the Law on Social Card and some issues that its adoption will raise in the domestic legal order. Due to time constraints and unavailability of all data of importance for the analysis of the Law, it is not comprehensive and subsequent analyses and communication with competent state authorities might raise new issues regarding the implementation of this Law and its compliance with the Constitution, personal data protection standards and other human rights standards.

Key issues regulated by the Law on Social Card

The social card is established by law as a single register of data on individuals and related persons, data on the socio-economic status of individuals and related persons, data on the type of social protection rights and services that the person uses or has used, as well as data on official persons who handled or decided on individual rights.

Under Article 3 of the Law on Social Card, the goal of this regulation is to establish a unified and centralized register of the socio-economic status of individuals and related persons. This goal

[45] Official Gazette of the RS, No.24/2011.
[46] Official Gazette of the RS, No.113/2017 i 50/2018.
[47] Serbian Government Program presented by Prime Minister-Elect Ana Brnabić, October 28, 2020.

should enable administrative bodies responsible for deciding in the welfare system *better to process data* in order to determine facts that are necessary for exercising rights and services in the welfare system. All this is undertaken for the purpose of achieving greater efficiency, *fairer distribution of social benefits and ensuring proactivity of administrative bodies* that decide on rights and services in the welfare system.

Following the main obligations referred to in the Law on Personal Data Protection, the Law on Social Card defines the purpose of data processing in the Social Card Register. It regulates the following five questions that determine the *purpose of data processing*:

1) determination of the socio-economic status of individuals and related persons;
2) automatization of procedures and processes pertaining to welfare actions;
3) development of social policies through the determination of the socio-economic status of individuals, related persons and wider community;
4) prevention of poverty and removal of consequences of social exclusion, and
5) implementation of statistical and other research in welfare.

Under Article 5 of the Law, the unified register is established and maintained by the ministry responsible for welfare issues. Within the meaning of the Law on Personal Data Protection, the Ministry of Labor, Employment, Veterans and Social Affairs represents the data controller, while the Office of Information Technology and Electronic Administration performs technical support tasks in establishing, maintaining and ensuring data security and safety.

According to Article 11 of the Law on Social Card, Social Card *data users*[48] are centers for social work, local self-government units that perform entrusted tasks in the field of welfare, the ministry in charge of social affairs, the provincial secretariat in charge of social affairs and other state administration bodies and institutions. Article 11, paragraph 2 of the Law says clearly that when it comes to data processing, Social Card data users act in accordance with the umbrella law - the Law on Personal Data Protection.

Lack of harmonization between the Law on Social Card and the Law on Personal Data Protection

Inappropriate data protection impact assessment

The Law on Social Card was prepared and sent to the Parliament without an appropriate public debate, which means that a chance was omitted for improving the text of the law presented as the Draft Law on Social Card in summer 2019. Moreover, some provisions of the Draft Law depart from the main principles of the Law on Personal Data Protection, primarily because of the scope and purpose of data processing and disregard of Serbia's legal tradition in the definition of certain legal issues. According to the information obtained from the expert service of the Commissioner for Information of Public Importance and Personal Data Protection, the impact assessment of the adoption of this law on personal data protection did not meet the requirements imposed by the Law on Personal Data Protection. Thus, the opportunity was missed to improve the draft from the aspect of personal data protection. As a result, further engagement and communication with the Commissioner for Information of Public Importance and Personal Data Protection are deemed necessary in order to find the appropriate legal remedy for responding to the lack of harmonization between the Law and personal data protection standards.

[48] Law on Personal Data Protection does not recognize the term „user "of data, but only data processor, who processes personal data on behalf of the data controller.

Scope of personal data processing

The Law on Social Card envisions the processing of a large number of personal data. According to the most moderate assessments, at least 135 different data can be found in the Social Card. In that regard, the *issue of the scope of data processing* is raised, i.e., whether the same purpose could have been achieved with a smaller scope of processing of personal data of beneficiaries and potential beneficiaries of the welfare system. The processed data are grouped in several sections. General data on individuals are defined in Article 7 of the Law, which provides for the *processing of general data* used for the identification of beneficiaries or potential beneficiaries of the welfare system. These data range from the name, citizenship, residence, occupation, data on the level of education and type of qualifications, all the way to data on the property status, movable property, payment of financial assistance according to other grounds, etc. Article 8 of the Law provides for the *processing of special data* on individuals, which primarily include the data on the beneficiary's application to the welfare system, decisions issued at the request of beneficiaries, period of validity of the decision, financial assistance, as well as special statuses, primarily medical condition, data on disability, data on independence in functioning, guardianship, foster care, etc. Finally, the next article prescribes *common and individual data of persons related* to the individual, which are collected and processed for the purpose of determining whether the conditions for exercising the welfare rights have been met. Particularly sensitive data are those related to domestic violence and measures taken against the perpetrator, data on child support and enforcement procedures in cases of when support is not paid, as well as data on related persons, income of these persons, real estate they own, disability or welfare rights in which the related person is the right holder.

The unified Social Card Register is established on the basis of data taken from the records in the field of social welfare kept by the relevant ministry, as well as registers kept by other state authorities.
These include:

1) data contained in the Central Population Register;
2) registers of the organization for mandatory pension and disability insurance;
3) Ministry of Interior registers of vehicles, arms, readmission;
4) National Employment Service registers on the payment of unemployment benefit and temporary and special benefits;
5) data contained in the Tax Administration registers;
6) Republic Geodetic Authority data.

At a glance, it seems that from the aspect of the Law on Personal Data Protection, the quoted provisions violate the principles of data minimization and restrictions pertaining to the purpose of processing. Namely, although Art. 4 of the Law on Social Card lists data processing purposes, subsequent provisions do not specify which data or data sets are processed for each specified purpose of processing. Rather than that, data and processing operations are listed "collectively", which means that the legislator should have specified these provisions, i.e., prescribed which specific data are necessary for the realization of each purpose of processing referred to in Article 4. It is quite certain that some of the processed data are not necessary for the welfare system, and especially not for the purpose of approving financial social assistance.

Groups of persons whose data are processed are defined imprecisely

Another controversial legal issue in the Law on Social Card that we should stress is that the Law envisions the collection and processing of *data of persons related to the beneficiary* or potential beneficiary of the welfare system. With regard to this, however, the problem lies in the fact that the circle of related persons is too wide, including even former extramarital partners as related persons. In addition to the fact that the Law does not precisely define whether this applies only

to former extramarital partners who live in the same household as applicants or to former extramarital partners who have the obligation to participate in child support, or to some other situation, the question is also how the administrative authorities will act in cases where there are multiple former extramarital partners - whether they will all be deemed related persons and when this relation relevant for the Law on Social Card ceases. Another question is whether these data will also be taken into account in the case of domestic violence, failure to provide child support or other cases in which social work centers might reject the request or revoke the right that had been recognized to the applicant as a result of a former extramarital partner's higher income or property of higher value.

In addition to this, Article 6 paragraph 4 of the Law stipulates that *by way of exception,* personal data of individuals belonging to vulnerable groups whose rights are determined by the Government may be processed in the Social Card, whenever assistance is provided in accordance with conditions defined in each individual case. This provision is vague and leaves room for flexible interpretations, including even the expansion of the originally defined circle of persons to whom the Social Card refers and whose data are collected and processed in this register.

Lack of harmonization of mechanisms for ensuring the right to insight

Moreover, an individual whose data are processed in the Social Card, according to Article 11 paragraph 3 of the Law, has the right to insight and the right on the basis of the insight, *through the eUprava Portal*, in accordance with the law governing personal data protection. It should be noted here that the Law on Personal Data Protection, as the umbrella law, defines the right of access to personal data much more widely than Article 11 paragraph 3 of the Law on Social Card. This primarily refers to the part that regulates the manner for exercising the "right to insight" and the "right based on the insight." Thus, *according to the umbrella law*, this right, defined under the term "access to data", can be exercised *regardless* of whether it is implemented through the eUprava Portal or in any other way. Since persons whose data are processed under the Law on Social Card are the beneficiaries of rights and services of the welfare system and potential beneficiaries of this system, we can rightly assume that poverty, lack of technological training, lack of access to computers, internet or smartphones mostly prevents them from using the eGovernment Portal. Therefore, the right to insight and rights based on the insight referred to in Article 11 paragraph 3 should be interpreted as an additional, special right regulated by the Law on the Social Card, in addition to the rights provided by the Law on Personal Data Protection. Any other interpretation would be in contravention with the Law on Personal Data Protection and would open a discussion on whether this is in accordance with the constitutional principle of unity of legal order.[49] In the absence of a clearer legal provision, it is yet to be seen how this provision of the Law will be interpreted in practice.

Data exchange as a data processing activity

In addition to this, the Law on Social Card is insufficiently precise in defining the exchange of data that occurs as a result of the application of this Law. Thus, the Law envisions *the exchange of data* contained in the previously mentioned records and registers for the purpose of maintaining and updating the Social Card. However, the question here is to what extent this exchange goes both

[49] See the Constitutional Court of Serbia decision in the case: IUz-231/2009 of 22 July 2010 "Starting from the provision of Article 4 paragraph 1 of the Constitution which establishes the principle of unity of legal order, as one of the main principles on which the constitutional system of the Republic of Serbia is based, the Constitutional Court points out that although the applicable legal system in the Republic does not distinguish between the so-called organic, fundamental or other laws that have stronger legal force than other, 'ordinary' laws, where, consequentially, in accordance with the provisions of Article 167 of the Constitution, the Constitutional Court is not competent to assess harmonization among laws, the constitutional principle of unity of legal order imposes the obligation of ensuring that main principles and legal instruments provided by laws which systematically regulate an area of social relations are respected in special laws, unless the systemic law explicitly prescribes the possibility of different regulation of these issues."

ways, i.e., how it is ensured that the data contained in the Social Card can be exchanged and disclosed through the transfer or submission to the operators of records and registers that exchange data with the Social Card. The Law on Social Card does not provide (adequate) answers to these questions.

The procedure of drafting and submission of notifications – the real purpose of the Law on Social Card?

Under the title "Procedure of drafting and submission of notifications," Article 17 of the Law on Social Card probably explains the purpose of the Law and previously described wide data processing established under it. This article prescribes the procedure in cases where inconsistency of data on the user or related persons is determined. In this case, a notification on data inconsistency is drafted, instructing the data user that it is necessary to check data by making an insight and downloading them from official records, documentation and public documents, that it is necessary to make a decision at the request of the party or that it is necessary to initiate *ex officio* proceedings after learning about facts of major importance for the exercise, change or termination of welfare rights.

Why should the process of drafting and submission of notifications be considered key to understanding the purpose of the Social Card?

To answer this question, we must go back to the main concepts defined in the Law on Social Card. The Law states that an individual is a beneficiary of welfare rights and services and a person in the process of realization of welfare rights. In short, the Social Card processes personal data of individuals who have gained the right to social assistance or a person who is trying to get the right to social assistance. These persons and these persons alone are in the Social Card Register.

To present the purpose of the Law on Social Card in simpler terms, we will imagine two persons in similar life circumstances.

Person A lives with his extramarital partner and a child, he has been unemployed for a long time, although he regularly reports to the National Employment Service, he has a dilapidated house in which he lives and does not own property of greater value. Person A became a beneficiary of the welfare system in 2009, when he fell into poverty, after which he failed to get back on his feet. According to the Law on Social Card, *Person A* is a beneficiary of welfare rights and services, i.e., an *individual whose personal data are collected and processed*.

Person B, on the other hand, has a wife and two children, lives in the basement of an abandoned building, he is unemployed, poorly educated, has no regular income, he is ill and due to a lack of information has not yet applied for welfare. According to the Law on Social Protection, *the Law will not apply to Person B before he applies for social assistance*.

Ex officio proceedings, provided for in Article 17 paragraph 2 item 3 of the Law on Social Card cannot be initiated in the case of Person B. The Social Card does not contain information about Person B, he is neither a beneficiary nor a person in the process of getting welfare rights. He is just an indigent individual in need of welfare.

On the other hand, when Person A's extramarital partner gets a job in a shop, when he goes to Germany "to seek asylum", or when he receives a gift of greater value, inconsistency of beneficiary data will be identified and Article 17 paragraph 2 item 3 will be activated through a notification of inconsistency, which cautions that Person A has been receiving welfare for a longer time or in an amount higher than the one he is entitled to under the Law on Social Protection.

Due to the above-mentioned provision of the Law, we can only conclude that the Law on Social Card is not adopted in order to improve the visibility in the system of citizens who are in the worst economic and social position and enable them to exercise the right to needed support in a timely and efficient manner, but in order to abolish or suspend assistance in cases in which a life situation makes a beneficiary "go over" the threshold for exercising the right to financial social assistance.

It is important to note that, potentially, better targeting may also be achieved in the case of beneficiaries whose application for social assistance has previously been denied and whose life circumstances change, as a result of which they meet the requirements for getting welfare rights. The percentage of such cases is unknown. In such cases, the centers for social work will act in accordance with Article 17 paragraph 2 item 3 of the Law on Social Card and "initiate the *ex officio* procedure". It remains to be seen whether this will really happen in practice, since the centers for social work in most cases do not initiate other procedures within their competence *ex officio*.

In addition to this, Article 17 of the Law on Social Card will additionally reaffirm the obligation of beneficiaries to report changes that might affect the right they enjoy referred to in Article 97 of the Law on Social Protection. This article of the Law on Social Protection says, *inter alia*, that the beneficiary of the right to social assistance is required to address the Center for Social Work *and report any change affecting a recognized right within 15 days from the date of the change*.

The reasoning of the Law says that the adoption of the Law on Social Card will enable "a fairer distribution and less abuse, greater efficiency in work and proactivity of public administration bodies." It also says that the Law prevents abuse in the part that refers to the exclusion from the system of all those "who have been 'mistakenly' awarded rights".

When we add to this provision a new view on the Law on Social Protection, which in Article 96 prescribes that "the Center for Social Work shall review conditions for exercising the right to financial social assistance in May, based on the income of beneficiaries realized in the previous three months," except for the beneficiaries who are capable of working and who have been receiving welfare in Serbia for nine months during a calendar year, it is clear that the *automatic review*, i.e., drafting and submission of notifications referred to in Article 17 of the Law on Social Card largely "tightens" the requirements provided by the Law on Social Protection. This takes us back to the observation of the constitutional principle of unity of legal order, because the law that regulates special personal data processing within the social protection system affects the rights from the welfare system itself, which are regulated by the Law on Social Protection.

Conclusion

The lack of harmonization between the Law on Social Card and the umbrella law in the field of welfare - the Law on Social Protection - is obvious, especially in Article 17 of the Law on Social Card, and further steps need to be made for the purpose of determining whether the legal solution is unconstitutional as a result of violation of the unity of legal order and restriction of rights and requirements under which financial social assistance is granted within the welfare system.

In addition to this, the scope of personal data processing introduced through Social Cards is in evident disproportion with the purpose and aim of the Law. Therefore, the question of equal treatment of beneficiaries and potential beneficiaries of the welfare system is raised, i.e. the observation of the principle of equality of all citizens. The processing of at least 135 data established under this law is of such scope and is so poorly regulated that the issue is raised of whether there is systemic discrimination against beneficiaries of the welfare system in this respect.

Discriminatory provisions of the Serbian Ministry of Health Rulebook on more detailed requirements, criteria and method of selection, testing and evaluation of donors of reproductive cells and embryos and their consequences for the privacy of LGB persons

Author: Miloš Kovaćević, Da se zna!

Pursuant to Article 21 paragraph 4 of the Law on Biomedically Assisted Fertilization (Official Gazette of the RS, No. 40/17 and 113/17 - other law), the minister of health has adopted a rulebook on detailed conditions, criteria and method of selection, testing and evaluation of donors of reproductive cells and embryos (Official Gazette of RS, No. 27/2019, hereinafter: the Rulebook). The Rulebook entered into force on April 20, 2019.

As its name indicates, the Rulebook prescribes the conditions, criteria and method of selection, testing and evaluation of donors of reproductive cells and embryos, which the centers for biomedically assisted fertilization, i.e., reproductive cell banks, are required to apply before obtaining reproductive cells and embryos.

However, once the Rulebook was adopted, the interested public raised the issue of inconsistency between certain provisions of the Rulebook and anti-discrimination regulations, especially from the aspect of LGB rights, on the occasion of which an independent state authority, the Commissioner for the Protection of Equality, has provided an opinion. These provisions can also be debatable from the aspect of personal data protection regulations.

Namely, under Article 2 paragraph 2 of the Rulebook[50] the main criterion for the selection of reproductive cells and embryos is that potential reproductive cell donors, i.e., both partners whose reproductive cells are used for creating the embryo, meet all the criteria of anamnestic data and complete clinical examination, including psychological evaluation, which is conducted through questionnaires and interviews by a qualified and professionally trained medical worker, and that potential donors, *inter alia*, **do not have anal sex** and anal warts.

---

[50] *Article 2 paragraph 2 of the Rulebook on more detailed conditions, criteria and method of selection, testing and evaluation of donors of reproductive cells and embryos*

The main criterion for the selection of reproductive cells and embryos is that potential reproductive cell donors, i.e., both partners whose reproductive cells were used for creating the embryo, meet all the criteria of anamnestic data and complete clinical examination, including psychological evaluation, on which data are collected through questionnaires and interviews conducted by a qualified and professionally trained medical worker and that they:

1) are in the optimum reproductive age (up to 40 years of age for men, and between 21 and 34 for women);
2) are in good physical and mental health, according to a psychological evaluation;
3) do not belong to the risk group of drug addicts;
4) do not have anal sex and do not have anal warts;
5) do not have needle marks on their skin;
6) did not have tattoos or piercings in the past 12 months and lymphadenopathy has not been detected during physical examination;
7) do not have jaundice of unknown origin or hepatomegaly;
8) do not take alcohol and do not smoke;
9) have normal sperm analysis results according to the World Health Organization criteria, i.e., the ovarial reserve has been preserved in the case of women;
10) their weight and height are more or less average for their age, sex and race.

Moreover, Article 4 of the Rulebook[51] specifies candidates who are disregarded in the process of selection of donors of reproductive cells, and paragraph 2 item 3 of this Article stipulates, *inter alia,* that a **donor of reproductive cells or embryos may not be a person who had homosexual relationships in the past five years.**

The analysis of the above-mentioned provisions of the Rulebook leads to the conclusion that homosexuals have been placed in an unequal position to heterosexuals, as well as that the application of these provisions will result in the violation of their right to privacy, as a result of reasons presented in the text below.

First of all, it needs to be said that Article 4 paragraph 2 item 3 of the Rulebook defines anamnesis as a procedure for collecting all data of importance for diagnosing and determining the nature of a disease through interviews, i.e., that anamnesis represents a part of the disease identification process. It also needs to be stressed that this provision is part of the article which in other points lists diseases/diagnoses that exclude persons suffering from these diseases/diagnoses from potentially becoming donors of reproductive cells or embryos.

In view of the above, it turns out that homosexual relationships are placed in the context of diseases, even though the World Health Organization removed homosexuality from the list of diseases as early as in 1990.[52]

In addition to this, since anamnesis is a product of interviews held for the purpose of gathering relevant information from patients, it is indisputable that in order to establish the right diagnosis in each individual case, the medical professional will ask potential donors of reproductive cells or embryos if they had homosexual relationships in the past five years, which means that they will thus be indirectly asked to disclose their sexual orientation. However, this would be a direct violation of Article 21 of the Anti-Discrimination Act, under which sexual orientation is a private matter and no one may be asked to disclose their sexual orientation.

In addition to this, whenever during interviews with medical professionals potential reproductive cell or embryo donors say that they currently have or that they had homosexual relationships in the past five years, they will be denied the right to be the donors of reproductive cells or embryos under Article 4 paragraph 2 item 3 of the Rulebook. In other words, the Rulebook denies the right to donate reproductive cells or embryos to an entire group due to their personal trait – sexual orientation – although the only justified thing to do would be to exclude just high-risk behavior.

---

[51] Article *4 paragraph 2 of the Rulebook on more detailed conditions, criteria and method of selection, testing and evaluation of donors of reproductive cells and embryos*

In addition to reasons referred to in paragraph 1 of this Article, a donor of reproductive cells or embryos may not be a person:

1) who has been diagnosed with dementia or any other degenerative or demyelinating disease of the central nervous system (CNS) or another neurological disease of unclear etiology;
2) who has been diagnosed with lymphadenopathy, genital ulcerous lesions, chancroid, herpes simplex or urethral discharge following a physical examination;
3) with the anamnesis of homosexual relationships in the past five years;
4) with hemophilia and any other similar coagulation disorder, and who has received humane derivatives of concentrated coagulation factors in the past five years;
5) who has received a cell, tissue or organ transplant and who has received other humane material for therapeutical purposes (transfusion).

[52] World Health Organization. (1992). The **ICD**-10 classification of mental and behavioral disorders: Clinical descriptions and diagnostic guidelines. Geneva: World Health Organization (internet) Available at: https://icd.who.int/browse10/2019/en#/F60-F69 (accessed on: 14 December 2020)

Article 2 paragraph 2 item 4 of the Rulebook has similar a effect. Namely, it may be assumed that the above-mentioned provision was included because, from the aspect of the medical profession, anal sex may be regarded as a risk for sexually transmitted diseases (STDs). However, even if anal sex represents a high risk for STDs from the aspect of the medical profession, the exclusion of an entire group of potential donors cannot be regarded as justified, that is, the only justified thing would be to exclude high risk behavior. More precisely, the Rulebook could have said only that potential donors must not have had **unprotected** anal sex. However, the language used in Article 2 paragraph 2 item 4 of the Rulebook affects homosexuals more than heterosexuals and is discriminatory, particularly against gay and bisexual men.

Therefore, Article 4 paragraph 2 item 3 obviously and directly places LGB persons in a less favorable position than heterosexuals, because it places homosexuality in the context of diseases. Moreover, this is an insult to the dignity of LGB persons. In addition to this, the implementation of this provision would quite certainly result in the disclosure of the sexual orientation of the potential donor and, therefore, the denial of the LGB persons' right to donate reproductive cells or embryos.

On the other hand, Article 2 paragraph 2 item 4 would be an example of indirect discrimination.

Indirect discrimination exists if, as a result of a personal trait, a person or a group of persons is placed in a less favorable position by an act, action or omission that is apparently based on the principle of equality and prohibition of discrimination. Since Article 2 paragraph 2 item 4 makes no mention of either homosexual relationships or homosexual orientation, at the first glance it could be concluded that this provision is based on the principle of equality and that it affects all persons equally. However, since anal sex is more common among homosexual or bisexual men than among heterosexuals, it is clear that this provision affects and discriminates against gay and bisexual men more.

Therefore, the above-mentioned provisions violate Article 21 of the Anti-Discrimination Act, under which, as we have already mentioned, sexual orientation is a private matter and no one may be asked to disclose it. Also, the disputed provisions of the Rulebook obviously violate Articles 6 and 7 of the Anti-Discrimination Act, which prohibit direct or indirect discrimination against persons or groups of persons for their personal traits, which is in this case their sexual orientation.

Acting on complaints from the *Da se zna!* Association, *Izađi* Group and Regional Info Center, the Commissioner for the Protection of Equality reached the same conclusion and recommended to the Ministry of Health to harmonize the disputed provisions with the Anti-Discrimination Act.[53] Due to the failure of the Ministry of Health to comply with the recommendation, the Commissioner for the Protection of Equality reprimanded it.[54]

Also, from the aspect of regulations on personal data protection, we may wonder whether the collection of data referred to in Article 4 paragraph 2 item 3 and Article 2 paragraph 2 item 4 is in accordance with the principles of the Law on Personal Data Protection.

All personal data processing cases must have a legal basis. In this particular case, one could assume that the legal basis for data processing is provided in Article 45 paragraph 2 item 3 of the Law on Biomedically Assisted Fertilization, under which data on the personal and family

[53] Opinion with recommendation of the Commissioner for the Protection of Equality, No. 07-00-343/2019-02 of 12.08.2019.

[54] Decision on reprimand issued by the Commissioner for the Protection of Equality, No. 07-00-343/2019-02 of 28.12.2020.

anamnesis are stored in a unified register of biomedically assisted fertilization procedures in the territory of the Republic of Serbia. However, the fact that the Rulebook mentions the collection of data related to homosexuality under personal anamnesis is disputable and unjustifiably places homosexuality in the context of diseases. Whether somebody has had homosexual relationships or not says nothing about the state of their health, which means that the collection of this type of data is obviously pointless and excessive.

In other words, provisions of the Rulebook have not been harmonized with the restriction on the purpose of processing or with the principle of data minimization referred to in the Law on Personal Data Protection.[55] Under this law, whenever there is data processing, in addition to the appropriate legal basis, there must be a specific, explicit, justified and legitimate purpose of processing, and the processed data must be appropriate, important and restricted to what is necessary in relation to the purpose of processing. In other words, only data necessary for achieving the purpose of processing may be collected.

To this end, the Rulebook provisions on the processing of data on the sexual orientation of potential donors of reproductive cells or embryos must be placed in the context of the desired purpose. On the basis of provisions of the Rulebook, one may conclude that (from a medical point of view) the collection of personal data of a potential donor of reproductive cells or embryos is aimed at protecting the health of future embryos and participants in the procedure of biomedically assisted fertilization.

However, since everything stated above shows that personal data of potential donors of reproductive cells or embryos that pertain to their sexual orientation or anal sex have nothing to do with high-risk behaviors or other risks that need to be ruled out from the aspect of medical profession in the biomedically assisted fertilization procedure, one can conclude that the collection of such data is not justified and that it violates Article 5 items 2 and 3 of the Law on Personal Data Protection.

It should also be stressed that data on a person's sexual activity or sexual orientation represent a special type of data, the processing of which is allowed only if special requirements provided by the Law on Personal Data Protection have been met. Since the application of the disputed provisions of the Rulebook would quite certainly result in the disclosure of a potential donor's sexual orientation and sexual activity, it would be particularly important to harmonize the disputed provisions of the Rulebook and the principles of the Law on Personal Data Protection.

Although the implementation of the above-mentioned principles of the Law on Personal Data Protection contributes to the protection of the right to privacy, a consistent implementation of these principles in this specific case would also prevent the described discrimination against LGB persons. Based on this example, we may conclude that **personal data protection represents a powerful anti-discrimination tool**.

Bearing all this in mind, it is necessary:

1. That the Ministry of Health act on the recommendation of the Commissioner for the Protection of Equality, and amend and harmonize the Rulebook with anti-discrimination regulations by:

- completely deleting Article 4 paragraph 2 item 3 of the Rulebook
- amending Article 2 paragraph 2 item 4 of the Rulebook by prescribing that a donor must not have unprotected anal sex.

[55] Article 5 of the Law on Personal Data Protection (Official Gazette of the RS, No. 87/2018)

2. If the Ministry of Health fails to act on the recommendation of the Commissioner for the Protection of Equality, the Constitutional Court should examine the legality of Article 4 paragraph 2 item 3 and Article 2 paragraph 2 item 4 of the Rulebook, i.e., their compliance with higher legal documents in the field of personal data protection.

International personal data transfers from Serbia

Author: Dunja Tasić, Share Foundation

Introduction

The right to personal data protection is one of the fundamental human rights guaranteed by the Constitution of the Republic of Serbia. It does not exist in a vacuum, but is interconnected with other constitutionally guaranteed rights, such as the right to secrecy of letters and other means of communication, the right to dignity, etc. Whenever personal data are handled unlawfully in any way, different consequences can ensue - from possible identity theft, through financial consequences, to damage to one's reputation, etc. This is especially true in situations in which special types of personal data, such as data on one's racial or ethnic origin, religious beliefs, health status, biometric data, sexual orientation, etc., are unlawfully processed. Since international personal data transfers also represent acts of processing, unlawful data transfers may injur the person whose data are transferred in many different ways. Depending on the country to which the data are transferred, a person could potentially lose control of his data, and therefore also the rights guaranteed by the *Law on Personal Data Protection*.

The Serbian Law on Personal Data Protection[56], adopted in 2018 on the model of the *EU General Data Protection Regulation*[57] (GDRP) regulates, *inter alia*, the issue of personal data transfers from Serbia to third countries or international organizations.

Here, we will focus on the international transfers of Serbian citizens' personal data, because a Serbian company may process personal data of EU citizens, planning to transfer them to a third country, in which case certain additional rules referred to in the GDPR may apply (extraterritorial application).[58]

Since the LPDP envisions a large number of legal bases for personal data transfers, a significant number of which are applied very rarely or are not applied at all at the moment (e.g., issuance of certificates, approved codes of conduct, etc.), here we will focus on the most frequent basic aspects of transfer.

Also, the subject-matter of this analysis is not the transfer of data by competent authorities for the purpose of preventing, investigating, detecting and prosecuting perpetrators of crimes or enforcing criminal sanctions. Rather than that, the focus of the analysis is on the international transfers of personal data of Serbian citizens by Serbian and foreign companies.

Different legal bases for the transfer

Free transfer based on the adequate level of protection

The LPDP envisions several different legal bases for international personal data transfers from Serbia. The transfer of Serbian citizens' personal data from Serbia to some countries is completely free, i.e., no approvals or fulfillment of conditions are needed, because these countries are believed to have the so-called *adequate level of personal data protection*. Observed most broadly, the *adequate level of protection* implies that the relevant country has the appropriate legislation

[56] Law on Personal Data Protection (Official Gazette of the RS, No. 87/2018)
[57] The text of the GDPR is available here.
[58] GDPR is implemented extraterritorially on Serbian companies which process personal data of EU citizens by offering them goods and services or by monitoring the behavior of EU citizens (Article 3 of the GDPR).

and the rule of law that ensures an efficient implementation of personal data protection regulations.

The list of countries to which Serbia can freely transfer personal data without the fulfilment of any prior conditions is not negligible - it currently includes more than fifty countries, which are made up of 1) signatories to the *Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*[59] (hereinafter referred to as: Council of Europe Convention), and 2) countries which, according to the EU Commission, have the adequate level of protection[60] (so-called EU Commission adequacy decision countries).

These are also countries that have the *adequate level of protection* according to a Serbian Government decision. Our Government has adopted a decision[61] which lists countries and international organizations regarded by Serbia as those that have the adequate level of personal data protection (54 countries in total), but the list is made up only the signatories to the Council of Europe Convention and those listed by the EU Commission – right now, the Serbian Government has not established a free international transfer regime with any other country except the above-mentioned ones.

We should also note that, until recently, US companies certified within the *Privacy Shield* mechanism[62] were regarded as entities with the *adequate level of protection*, i.e., those that were allowed free transfer of data from the Republic of Serbia, since such US companies were on the list of EU Commission adequacy decision countries. Under the July 2020 judgment[63] of the EU Court of Justice[64], *Privacy Shield* is no longer applicable as a transfer mechanism, which will be discussed in greater detail in the text below.

Therefore, if a third country is on any of the above-mentioned lists, transfers of our citizens' personal data from Serbia should not be a problem, since they are permitted and free.

There is currently a special issue concerning personal data transfers from the EU to the United Kingdom after this country has left the EU and, from the EU point of view, now represents a third country. In order to address the issue of data transfers from the EU to the UK at a systemic level, the UK Government has asked the European Commission for an adequacy decision that will ensure free data transfers. The adequacy decision has not been issued yet, and the EU has meanwhile approved the postponement (of up to six months) of transfer restrictions under the GDPR in favor of the United Kingdom. If no adequacy decision is made in favor of the United Kingdom within this period, the transfer restriction under the GDPR will apply on the United Kingdom, like it does on all other countries outside the list of adequacy decision countries.

Data transfers from Serbia to the United Kingdom are completely free, however, since the United Kingdom is a signatory to the Council of Europe Convention and is, therefore, regarded as a country that has the *adequate level of personal data protection*.

Transfers with the application of adequate protection measures

[59] List of signatories to the Convention is available here.
[60] List of countries for which the EU Commission has determined that they have the adequate level of data protection for the export of data outside the EU is available here.
[61] Decision on the list of states, parts of their territories or one or multiple sectors of certain industries in these states and international organizations which are regarded to have the adequate level of personal data protection (Official Gazette of the RS, br. 55/19)
[62] Official website of the *Privacy Shield* mechanism is available here.
[63] The CJEU judgment is available here.
[64] Court of Justice of the European Union (CJEU)

If a third country to which we plan to transfer data from Serbia fails to provide the *adequate level of protection* (i.e., is not on any of the above-mentioned lists), the LPDP permits transfers if the controller or processor who plans to transfer data has adequate measures for the protection of these data. The LPDP lists multiple adequate protection measures, which, *inter alia*, include the so-called *standard contractual clauses* prepared by the Commissioner for Information of Public Importance and Personal Data Protection of the Republic of Serbia (hereinafter referred to as: Commissioner), approved codes of conduct, certificates issued by the Commissioner or certification bodies, binding business rules, etc.

Since we currently do not have any known practice of the Commissioner or other relevant bodies concerning the use of many of the above-mentioned safeguards, we will focus on the *standard contractual clauses* as the most frequent basis for transfers in this group.

Standard contractual clauses actually represent a standardized contract signed between the entity that "exports" personal data from Serbia and the entity that "imports" the data to a third country, guaranteeing mutual protection of personal data which represent the subject of export or import. This legal basis is the most frequent since it is the simplest – in order for a transfer to be lawful it is enough to sign the integral version of the Standard Contractual Clauses which our Commissioner adopted in January 2020[65] on the model of standard contractual clauses adopted by the EU Commission[66].

However, there are numerous practical issues concerning compliance with standard contractual clauses, i.e., in a large number of cases they end up as a "dead letter", since the "exporters" from Serbia do not have the capacity to check whether the "importer" from a third country has really fulfilled the obligations envisioned in the signed standard contractual clauses.

Data transfers in special situations

It should be noted that the LPDP also envisions the possibility of international data transfers from Serbia even if the importing country does not have the *adequate level of protection* or any of the prescribed protection measures.

For example, a transfer is possible if the data subject has expressly agreed to it, or if the transfer is necessary for the conclusion and enforcement of a contract between the data subject and the controller, or if it is necessary for pursuing an important public interest prescribed by the law of the Republic of Serbia, as well as in other cases prescribed by law.

The fall of *Privacy Shield*

Until recently, US companies could volunteer to be certified within the *Privacy Shield* mechanism and could thus join the EU Commission's adequacy list, which meant that they were regarded as entities that had the *adequate level of protection* from the aspect of our LPDP – which, in turn, meant that data transfers from Serbia to the US by domestic and US companies under the auspices of *Privacy Shield* were free.

However, in July 2020, the EU Court of Justice passed a judgment declaring the *Privacy Shield* mechanism invalid and thus "deleting" US companies from the list of those that have the adequate level of data protection. This decision has a practical impact on Serbia, and primarily on Serbian companies to which the GDPR applies extraterritorially and which outsource personal data

[65] Decision on the determination of standard contractual clauses (Official Gazette of the RS, No. 5/20)
[66] Current standard contractual clauses of the EC Commission are available here, although there are announcements that they will be revised soon.

processing to US IT giants such as Amazon, Digital Ocean, etc. Now the issue is how Serbian companies will respond to the above-mentioned judgment of the EU Court of Justice.

Under the judgment, a free transfer of personal data from Serbia to US companies on the basis of *Privacy Shield* is no longer possible. However, the issue is what will happen to other legal bases for data transfer (standard contractual clauses, for example).

Although the EU Court of Justice judgment regards standard contractual clauses as a legal basis for data transfers, these legal restrictions primarily apply on situations in which EU citizens' data are transferred to the US. When it comes to Serbian companies to which the GDPR does not apply extraterritorially (which do not process and transfer EU citizens' personal data), they can still use standard contractual clauses as the legal basis for data transfers to the US.

Moreover, the judgment still allows the "necessary" transfers of personal data to the United States - for example, data transfers necessary for fulfilling a contract (e.g., an online shopping contract), consensual transfer, etc.

Practical issues and recommendations

Serbian companies that transfer data to the US face numerous practical problems as a result of the "fall" of *Privacy Shield*, and this especially applies on Serbian companies that have entrusted personal data processing to IT companies that store personal data on their infrastructure (Amazon, Digital Ocean, etc.) and have relied on the fact that the US companies were on the list of entities that had the *adequate level of protection* owing to *Privacy Shield*. In this case, Serbian companies must find another basis for data transfers to the United States, or they can be penalized for the misdemeanor of unauthorized transfer under the LPDP.

In addition to this, if the GDPR applies extraterritorially on a Serbian company which transfers EU citizens' data to the United States, the company may face astronomical fines under the GDPR.

However, Serbian companies to which the GDPR does not apply extraterritorially can continue to use standard contractual clauses for data transfers to the United States, without special restrictions.

What appears to be a problem in case of standard contractual clauses is the fact that our Commissioner has so far approved only the clauses that regulate relationships between controllers and processors in situations in which controllers transfer data to processors. Therefore, we do not have standard contractual clauses that regulate transfers between two controllers, or transfers between the processor and the sub-processor, which means that they cannot be used as a legal basis for such transfers before they are adopted by the Commissioner. Our recommendation is that in the coming period the Commissioner adopt standard contractual clauses that will enable transfers between two controllers, and those that will allow transfers between the processor and the sub-processor. We should also take into account the announcements[67] that the EU Commission will revise its own standard contractual clauses by the end of 2020. Although this did not happen by the time when this text was published, once it does, one can reasonably expect that the new EU standard contractual clauses will affect the standard contractual clauses of our Commissioner.

In a situation where a US giant such as Facebook transfers Serbian citizens' data to the US, our standard contractual clauses cannot be the legal basis for the transfers, because Facebook cannot

[67] One of such announcements is available here.

sign them with itself – for the signing of standard contractual clauses, there must be two contracting parties – the personal data exporter and the personal data importer.

The next issue is also related - when foreign companies transfer Serbian citizens' data to other countries in violation of the LPDP, the question arises: how to punish such companies under the Serbian law? Situations in which foreign companies transfer Serbian citizens' data to other countries (very frequently the US) happen every day - Facebook, Google, Netflix and similar companies do this regularly.

For misdemeanors, the LPDP envisions fines between 50,000 and 2,000,000 RSD for a controller or a processor – the legal entity that transfers personal data to other countries in violation of the LPDP. On the other hand, under the Serbian Law on Misdemeanors[68] a foreign legal entity may be punished for a misdemeanor committed in the territory of Serbia only if it has a business unit or a representative office in the Republic of Serbia. This makes us wonder how a foreign entity without a business unit or a representative office in Serbia will be punished for a misdemeanor in connection with data transfers under the LPDP? This is a serious legal gap because, judging by the current situation, the punishment of foreign legal entities for violations of our law seems to be impossible.

Since the LPDP is applied extraterritorially on foreign companies that process our citizens' data by offering goods and services and monitoring our citizens' behavior, the LPDP requires from such companies to appoint their representatives in the Republic of Serbia. Above all, this refers to companies such as Facebook, Google, Amazon, Netflix, Viber, etc.[69] If foreign companies to which the LPDP applies extraterritorially appoint their representatives in Serbia, the Commissioner and other persons may address their representatives regarding all personal data processing issues for the purpose of ensuring compliance with the LPDP. Thus, the appointment of foreign company representatives will potentially facilitate the punishment of such companies for violations of the LPDP. Therefore, we also recommend that the Law on Misdemeanors be amended in the part that allows the punishment of foreign legal entities, so as to reflect the possibility of punishing legal entities that do not have business units or representative offices in Serbia for the violation of the LPDP. As for the appointment of representatives of foreign companies to which the LPDP applies, our recommendation is to impose the mandatory public registration of representatives with the Commissioner, since this type of information is not always public and the very purpose of representatives is to be easily accessible to stakeholders who can address them in connection with personal data processing conducted by the company that has appointed them.

Finally, Serbian citizens need systematic education and raising of awareness concerning who processes their data and why they are exported from the country. Only citizens who are aware of these issues can regain control of their own data by exercising their rights guaranteed by the LPDP.

[68] Law on Misdemeanors (Official Gazette of the RS, No. 65/2013, 13/2016, 98/2016 – CC decision, 91/2019 and 91/2019 -other law)

[69] At the moment of writing of this analysis, as far as we know, out of the multinational companies that operate on the internet – Google, Viber, Netflix and Booking.com have appointed their representatives in Serbia.