THE PIVOTAL ROLE OF DPAs IN DIGITAL PRIVACY PROTECTION: ASSESSMENT OF THE SERBIAN PROTECTION MECHANISM

Dušan V. Popović*

ABSTRACT

With the widespread use of the Internet in both personal and professional life, data protection has become a critical aspect of privacy protection. The mechanisms developed in administrative law are the main tools for personal data protection in modern societies. Within the European integration process, the Republic of Serbia has established an independent data protection authority (DPA) that supervises and ensures the implementation of data protection rules, conducts inspections, acts on complaints of persons to whom the data relates, and determines whether there has been a violation of the law. This paper commences with an analysis of international legal instruments imposing a duty to establish an independent data protection supervisory authority. It goes on to further analyze the main characteristics of the national data protection system, the personal, territorial, and material scope of its application, as well as specific rights of data subjects. The efficient protection of digital privacy primarily depends on the investigative powers of the independent supervisory authority, which are also analyzed in detail. Given the global character of the Internet, the protection of personal data also depends on efficient cooperation among DPAs, the extraterritorial application of data protection rules, and adequate regulation of international transfer of personal data.

KEYWORDS

right to privacy
Serbia
Internet
Data Protection Authority (DPA)
personal data
European integrations

* | Full Professor, University of Belgrade Faculty of Law, Serbia, dusan.popovic@ius.bg.ac.rs, ORCID: 0000-0001-8044-1823.

https://doi.org/10.55073/2022.2.131-146

1. Introductory remarks

With the omnipresence of the Internet in both personal and professional life, data protection has become a critical aspect of privacy protection. Nowadays, privacy is often reduced to the privacy of data relating to an identifiable individual. The concept of personal data encompasses not only names and addresses but also all data that can be traced back to an individual, such as browsing history or any other online activity. In Serbian law, the notion of personal data is broadly defined as any information relating to a natural person whose identity is determined or identifiable, directly or indirectly, in particular, by reference to an identifier, such as a name and identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[1] The mechanisms developed in administrative law are the main tools for personal data protection in modern societies. Within the European integration process, the Republic of Serbia has established an independent data protection authority (DPA) that supervises and ensures the implementation of data protection rules, conducts inspections, acts on complaints of persons to whom the data relates, and determines whether there has been a violation of the law. The administrative procedure before the DPA has become the preferred mechanism for personal data protection over civil and criminal law proceedings.

Like other European countries, the Serbian legal framework for personal data protection is determined by specific international obligations stemming from the country's membership in the United Nations[2] and the Council of Europe[3], as well as from the country's European Union candidate status. The paper begins with an analysis of international legal instruments imposing a duty to establish an independent data protection supervisory authority (Section 2). The study then analyzes the main characteristics of the national data protection system: the personal, territorial, and material scope of its application, as well as specific rights of data subjects (Section 3). The efficient protection of digital privacy primarily depends on the investigative powers of the Data Protection Authority, which will be analyzed in more detail (Section 4). Given the global character of the Internet, the protection of personal data also depends on efficient cooperation among DPAs, the extraterritorial application of data protection rules, and adequate regulation of the international transfer of personal data (Section 5).

1 | Law on Protection of Personal Data (hereinafter, the LPPD), Official Journal of the Republic of Serbia 87/2018, Art. 4.

2 | The Federal People's Republic of Yugoslavia was not among the signatories of the Universal Declaration of Human Rights in 1948. In 1971, within the auspices of the United Nations, the Socialist Federal Republic of Yugoslavia ratified the International Covenant on Civil and Political Rights.

3 | The Republic of Serbia became member of the Council of Europe on 3 April 2003 and ratified the European Convention on Human Rights on 3 March 2004.

2. Duty to establish an independent data protection authority

The efficient protection of personal data may be best achieved through the establishment of administrative law mechanisms, rather than through lengthy court proceedings. Indeed, administrative proceedings before an independent data protection authority correspond better with the nature of online interactions and provide a rapid response to various infringements of digital privacy. In the international context, the need for such authorities was recognized quite early. A non-binding but unanimous resolution of the UN General Assembly, adopted in 1991, was the first international data protection text to include the requirement of an independent DPA.[4] The resolution requires that such authority offers guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of a violation of the relevant national provisions, criminal or other penalties should be envisaged together with appropriate individual remedies.[5] The adoption of this UN resolution is seen by many as the moment in which personal data protection has ceased to be exclusively a 'first world problem.'[6]

For the Republic of Serbia, a duty to establish such an independent data protection authority stems from the international instruments adopted by the Council of Europe and the European Union, respectively. As a member of the Council of Europe, the Republic of Serbia ratified the Convention for the Protection of Individuals regarding the Automatic Processing of Personal Data (ETS No. 108)[7] and the Additional Protocol to the Convention for the Protection of Individuals regarding the Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No. 181)[8]. The Convention is the first binding international instrument that protects the individual against abuses that may accompany the collection and processing of personal data and simultaneously seeks to regulate the transfrontier flow of personal data. However, it does not specify any requirements for the establishment of a national data protection authority. The Additional Protocol provides for

4 | Guidelines for the regulation of computerized personal data files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989).
5 | *Ibid*, point 8.
6 | See for example: Greenleaf, 2011, p. 8.
7 | Law on ratification of the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the FR Yugoslavia 1/1992; Official Journal of Serbia and Montenegro 11/2005. Law on amendments of the Law on ratification of the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of the Republic of Serbia 12/2010.
8 | Law on ratification of the Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows (hereinafter, the Additional Protocol), Official Journal of the Republic of Serbia 98/2008.

the setting up of national supervisory authorities responsible for ensuring compliance with laws or regulations adopted in pursuance of the convention concerning personal data protection and transborder data flows. The countries that ratified the Additional Protocol should adhere to six principles when setting up their supervisory authority (authorities).[9] First, the Additional Protocol sets out the principle of institutional autonomy, which states that each country decides whether to establish one or more independent supervisory authorities. Second, the said authority (authorities) should have powers of investigation and intervention, as well as the power to engage in legal proceedings or bring violations of the provisions of domestic law to the attention of the competent judicial authorities. Third, each supervisory authority should be empowered to hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms regarding the processing of personal data within its competence. Fourth, supervisory authorities must exercise their functions in complete independence. Fifth, the national legal framework should allow the decisions of the supervisory authorities, which give rise to complaints, to be appealed against through the courts. Sixth, the supervisory authorities of the countries that ratified the Additional Protocol should cooperate with one another to the extent necessary to perform their duties, that is, by exchanging all useful information. The Republic of Serbia also ratified the Protocol, amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)[10], which has not yet entered into force.[11] The Protocol reinforces the powers and independence of data protection authorities and enhances the legal basis for international cooperation.[12] It requires the parties to establish DPAs that have powers to issue decisions with respect to violations of the provisions of the Convention and that may, in particular, impose administrative sanctions. Furthermore, DPAs should have the power to engage in legal proceedings or to bring to the attention of competent judicial authorities the violations of the provisions of the Convention. DPAs should promote public awareness of the rights of data subjects and the exercise of such rights and should be consulted on proposals for any legislative or administrative measures that provide for the processing of personal data. The Protocol further requires the DPAs to keep data subjects informed of the progress of proceedings initiated by complaints. The acceding parties should ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers. Finally, certain transparency duties have been introduced in the sense that each supervisory authority is required to prepare and publish a periodical report outlining its activities.

9 | The Additional Protocol, Art. 1.
10 | Law on ratification of the Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data (hereinafter, the Protocol), Official Journal of the Republic of Serbia 4/2020.
11 | As of July 2022.
12 | The Protocol, Art. 19.

Within the European integration process, Serbia signed the Stabilization and Association Agreement with the EU (SAA)[13] in 2008.[14] Under Article 81 of the SAA, dedicated entirely to personal data protection, Serbia is required to harmonize its legislation concerning personal data protection with EU law and other European and international legislation on privacy upon the entry into force of the SAA. Serbia is also required to establish one or more independent supervisory bodies with sufficient financial and human resources to efficiently monitor and guarantee the enforcement of national personal data protection legislation. Further, within the statistical cooperation with the EU, Serbia is required to ensure the confidentiality of individual data.[15] The reason for harmonizing the national legal framework with EU rules on personal data protection is to be found in the preamble of the SAA, in which the parties to the agreement reaffirmed their commitment to respect human rights and the rule of law. One of the aims of the SAA is to support Serbia's efforts to develop its economic and international cooperation, including through the approximation of its legislation to that of the EU.[16] The respect for democratic principles and human rights, as proclaimed in the Universal Declaration of Human Rights and as defined, *inter alia*, in the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), form the basis of the domestic and external policies of the parties to the SAA and constitute essential elements of this agreement.[17]

3. Main characteristics of the national personal data protection system

The first attempts to regulate personal data protection in Serbia were made in 1998, when the Law on Personal Data Protection was passed.[18] Unfortunately, that law remained 'dead letter,' since only a few marginal cases of attempted application of the law by the data handlers were recorded over a period of ten years of its application.[19] During this period, the issue of defining an independent data protection authority remained unclear.[20] To comply with the requirements stemming from the international and EU legal instruments[21], Serbia adopted its first modern legislative act regulating personal data protection in 2008[22] and

13 | Stabilization and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Serbia, of the other part, Official Journal of the European Union L 278, 18.10.2013.
14 | The SAA entered into force on 1 September 2013.
15 | SAA, Art. 90.
16 | SAA, Art. 1 para. 2 d).
17 | SAA, Art. 2.
18 | Official Journal of the FR Yugoslavia 24/98 and 26/98.
19 | Resanović, 2019, p. 42.
20 | Ibid.
21 | See Section 2 of this paper.
22 | Official Journal of the Republic of Serbia 97/08, 104/09, 68/12 and 107/12.

adopted the Strategy for personal data protection in 2010[23]. Following the enactment of the 2008 Law on Personal Data Protection, a national DPA was established. The Serbian DPA was established by expanding the competences of the existing independent authority in charge of assuring free access to information of public importance. This authority, entitled the Commissioner for Information on Public Importance, was established in 2004 by the Law on Free Access to Information of Public Importance. On January 1, 2009, following the entry into force of the 2008 Law on Personal Data Protection, the tasks related to the protection of personal data were included in the Commissioner's scope of work. The 2008 Law on Personal Data Protection has been in force for a decade.

The main piece of legislation currently regulating personal data protection in the Republic of Serbia is the Law on Protection of Personal Data (LPPD)[24], adopted in November 2018 and applicable since August 2019.[25] The LPPD is an 'umbrella regulation' in the field of personal data protection in Serbia. Sectoral laws also apply to personal data processing in certain areas. The LPPD lays down general rules on personal data protection, while other laws may prescribe specific legal regimes applicable in certain areas or for certain types of activities. However, the principle *lex specialis derogat legi generali* does not apply because the LPPD explicitly requires that the provisions of other laws regulating the processing of personal data must be in line with the LPPD.[26] The main reason for adopting the 2018 LPPD was the need to harmonize the Serbian legal framework with the European Union's General Data Protection Regulation (GDPR).[27]

3.1. Scope of application of the LPPD

Regarding the personal scope of application, the LPPD applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data, which form part of or are intended to form part of a filing system. Furthermore, the LPPD applies to the processing of personal data performed by a controller or processor who has its business seat/place of residence in the territory of the Republic of Serbia within the framework of activities performed in the territory of the Republic of Serbia, regardless of whether the processing takes place in the territory of the Republic of Serbia. With respect to the territorial scope of application, it has been prescribed that the LPPD also applies to the processing of personal data of data subjects with residence in the territory of the Republic of Serbia by a controller or processor who does not have its business seat/place of residence in the territory of the Republic of Serbia, where the processing activities are related to (1) the offering of goods or services, irrespective

23 | Official Journal of the Republic of Serbia 58/2010.
24 | Official Journal of the Republic of Serbia 87/2018.
25 | The LPPD entered into force on 21 November 2018, but its application started nine months from the date of its entry into force, i.e., on 21 August 2019.
26 | LPPD, Art. 2 para 2.
27 | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L119, 4.5.2016.

of whether a payment of the data subject is required, to data subjects in the territory of the Republic of Serbia; and (2) the monitoring of data subject's behavior as far as their behavior takes place within the territory of the Republic of Serbia.

With respect to the material scope of application, the LPPD does not apply to the processing of personal data by a natural person during purely personal or household activity.[28] By reason of the matter, the LPPD covers all forms of use or other processing of personal data. The LPPD defines personal data processing as any action taken in connection with the information, including collection, recording, transcription, multiplication, copying, transmission, search, classification, storage, separation, adaptation, modification, making available, use, dissemination, recording, storage, disclosure through transmission or otherwise, dislocation, as well as other actions carried out in connection with the personal data, regardless of whether such actions are automated, semi-automated, or carried out otherwise.[29]

3.2. Specific rights of data subjects

Like the GDPR, the LPPD prescribed several specific rights for a data subject. A data controller is required to facilitate the exercise of data subject rights. The former is required to provide information on the action taken on the request of a data subject without undue delay and in any event within 30 days of receipt of the request.[30] The LPPD prescribes additional rules with respect to processing specific categories of personal data. Namely, the LPPD prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.[31] Exceptionally, the said prohibition does not apply in certain cases prescribed by the LPPD, such as when the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, or when processing is necessary to protect the vital interests of the data subject or of another natural person if the data subject is physically or legally incapable of giving consent.

One of the essential rights recognized for a data subject is the right to be informed. The controller is obliged to take appropriate measures to provide the prescribed information to the data subjects, that is, information concerning the exercise of rights, in concise, transparent, intelligible, and easily accessible from, using clear and plain language, if the information is intended for a minor. The requested information may be provided through electronic means. The data subject has the right to obtain the information on (1) whether its personal data is processed or not; (2) the right to access to that data; (3) the categories of personal data that are being processed and the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; (4) the purpose of processing; (5) the

28 | LPPD, Arts. 1–3.
29 | LPPD, Art. 4 para. 3.
30 | LPPD, Art. 21 para. 3.
31 | LPPD, Art. 17.

envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (6) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (7) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; (8) the right to lodge a complaint with a DPA.[32] If personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Further to the right to be informed, the data subject has the right to request personal data from the controller.[33] Third, the data subject has the right to rectify their inaccurate personal data without undue delay.[34] Depending on the purpose of data processing, the data subject has the right to complete their incomplete data, which includes providing a supplementary statement. Fourth, the data subject has the right to have their personal data deleted by the controller when (1) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (2) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing; (3) the data subject objects to the processing and there are no overriding legitimate grounds for the processing; (4) the personal data have been unlawfully processed; (5) the personal data have to be erased for compliance with a legal obligation; or (6) the personal data have been collected in relation to the offer of information society services.[35] If the controller has made the personal data public and is obliged to delete the personal data, the controller, taking account of available technology and the cost of implementation, is required to take reasonable steps, including technical measures, to inform controllers who are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replicate, those personal data.[36] An organization's right to process someone's data might override its right to be forgotten in the following cases: (1) the data is being used to exercise the right of freedom of expression and information; (2) the data is being used to comply with a legal ruling or obligation; (3) the data is being used to perform a task that is being carried out in the public interest or when exercising an organization's official authority; (4) the data being processed is necessary for public health purposes; (5) the data is necessary for archiving purposes in the public interest, or serves for scientific research, historical research, or statistical purposes, and erasure of the data is likely to impair or halt progress towards the achievement that was the goal of the processing; (6) the data is being used for the establishment of a legal defense or in the exercise of other legal claims.[37]

32 | LPPD, Art. 23.
33 | LPPD, Art. 26.
34 | LPPD, Art. 29.
35 | LPPD, Art. 30.
36 | See: Midorović, 2019, pp. 293–296.
37 | LPPD, Art. 30 para. 5.

The LPPD lays down the right of a data subject to an object, on grounds relating to his or her situation, at any time to the processing of personal data concerning him or her, including profiling.[38] If personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Further to the right to object to processing of personal data, a data subject has the right to data portability, that is, the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, if (1) the processing is based on consent or on a contract; and (2) the processing is carried out by automated means.[39]

A data subject has the right not to be subject to a decision based solely on automated processing, including profiling, if such a decision produces legal effects concerning the data subject or in a similar manner significantly affects the data subject.[40] However, the data subject may consent to such automated processing or the latter may be explicitly allowed by law in specific cases. There are at least three possible ways of monitoring and profiling that offer grounds for discrimination: (1) data collection that leads to inferences about the person (e.g., online browsing behavior); (2) profiling at large through linking Internet of Things datasets; and (3) profiling that occurs when data are shared with third parties that combine data with other datasets (e.g., employers, insurers).[41] In real life, automated decision-making supplements human judgment, and these systems appear to escape the prohibition. The LPPD's provision applies only to decisions based solely on automated processing.[42]

Finally, a data subject has the right to lodge a complaint before the DPA if he/she believes that the processing of his/her personal data was performed contrary to the LPPD.[43]

4. Main powers, duties, and responsibilities of the Serbian DPA

The national data protection authority responsible for overseeing the implementation of the LPPD is the Commissioner for Information of Public Importance and Personal Data Protection. The person appointed as Commissioner must act independently in performing its duties and must neither receive nor request instructions from anyone. He or she may not perform any other public or political

38 | LPPD, Art. 37. See also: Mišković, 2020, pp. 134–135.
39 | LPPD, Art. 36.
40 | LPPD, Art. 38.
41 | Wachter, 2018, p. 441.
42 | For an analysis of a similar provision in the GDPR see: Hoofnagle, van der Sloot and Zuiderveen Borgesius, 2019, pp. 65 et seq.
43 | LPPD, Art. 82.

function, nor be employed elsewhere. The Commissioner is chosen among persons with the reputation of an expert specialized in human rights protection. The Commissioner is appointed by the National Assembly for a period of seven years. As reflected in the title of this authority, the Commissioner oversees the enforcement of both the LPPD and the Law on Access to Information of Public Importance[44].

The main powers and responsibilities of the DPA are as follows: (1) ensuring and supervising the implementation of the LPPD; (2) raising public awareness of risks, rules, safeguards, and rights related to processing, especially if it concerns processing data of a minor; (3) giving opinion to the National Assembly, the Government, other authorities and organizations, in accordance with the LPPD, on legal and other measures related to the protection of the rights and freedoms of natural persons in connection with data processing; (4) taking care of the controller's awareness and process in connection with its mandatory regulations on the LPPD; (5) providing, at the request of the data subjects, of information on their rights prescribed by the LPPD; (6) acting on complaints of persons to whom the data relates, determining whether there has been a violation of the law and informing the submitter on the rules on the course and the results of the proceedings being conducted; (7) cooperating with the supervisory authorities of other countries with regard to personal data protection, and by sharing various information and engaging in mutual legal assistance; (8) carrying out inspection on the LPPD enforcement, in accordance with the LPPD and the corresponding law on inspections, and submitting a request for initiating misdemeanor proceedings, in accordance with the law that regulates misdemeanors; (9) monitoring the development of information and communication technologies, as well as business and other practices relevant to the protection of personal data; (10) encouraging the development of codes of conduct and giving opinions and approval to the codes of conduct; (11) encouraging the issuance of a certificate for the protection of personal data and the corresponding trademarks and labels, and setting out the criteria for certification; (12) conducting periodic reviewing of certificates; (13) prescribing and publishing of criteria for accreditation of the certification body; (14) approving binding corporate rules; (15) keeping internal records of violations of the LPPD; (16) performing other tasks in accordance with the LPPD.[45]

The DPA is authorized to take a number of substantially different corrective measures: (1) to warn the controller[46] and the processor[47] by submitting a written opinion that the intended processing operations may violate the provisions of the LPPD; (2) to issue a warning to the controller or processor if the processing

44 | Official Journal of the Republic of Serbia 120/2004, 54/2007, 104/2009, 36/2010 and 105/2021.

45 | LPPD, Art. 78.

46 | Under Art. 4 of the LPPD, a data controller is defined as a natural or legal person, public authority which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by the law, the controller or the specific criteria for its nomination may be provided for by the law.

47 | Under Art. 4 of the LPPD, a data processor is defined as any natural or legal person, i.e., public authority, which processes personal data on behalf of the controller.

violates the provisions of the LPPD; (3) to order the controller and the processor to act upon the request of the data subject in connection with the exercise of their rights, in accordance with the LPPD; (4) to order the controller and the processor to harmonize the processing operations with the provisions of the LPPD, in a specific manner and within a specified time frame; (5) to instruct the controller to inform the person whom the personal data refers to about the violation of his/her personal data; (6) to impose a temporary or permanent restriction on processing operation, including a prohibition on processing; (7) to order the correction or deletion of personal data or restrict the performance of the processing operation, and order the controller to inform the other controller, the data subject and the recipients to whom the personal data have been disclosed or transferred; (8) to revoke the certificate or to order the certification body to revoke the certificate, as well as to order the certification body to refuse to issue the certificate if the conditions for its issuance are not fulfilled; (9) to impose a fine based on a misdemeanor warrant if during inspection it has been established that there was a breach for which the LPPD prescribes a fine in a fixed amount, instead of other measures, depending on the circumstances of the particular case; and (10) to suspend the transfer of personal data to a recipient in another country or international organization.[48] The data subject, data processor, or any other natural or legal person concerned by the DPA's decision may initiate an administrative dispute within 30 days following the receipt of such a decision.[49] Administrative disputes fall under the jurisdiction of the Administrative Court and are conducted pursuant to the Law on administrative disputes[50].

The inspections undertaken by the DPA have proven crucial for efficient enforcement of the LPPD. The inspectors act upon information acquired *ex officio* or received from the complainants. According to a recently published report, the DPA completed 303 inspections in 2021[51] and received 211 complaints for alleged breaches of data protection rules in the same period[52]. Certain breaches of law are set out as misdemeanors, for which the LPPD prescribes fines. The DPA is authorized to initiate misdemeanor proceedings before the competent court. When the legislator prescribes pecuniary fines for misdemeanors in fixed amounts, the DPA may impose the fines directly. However, fines are usually prescribed in range (minimum to maximum amount), which is why the DPA would typically need to initiate the proceedings before the misdemeanor court. The fine imposed may not, in any case, exceed the maximum amounts that can be imposed on the controller or processor for a misdemeanor under the LPPD, that is, up to RSD 2,000,000 (approx. €17,000).[53]

48 | LPPD, Art. 79.
49 | LPPD, Art. 83.
50 | Official Journal of the Republic of Serbia 111/2009.
51 | Report on the activities of the Commissioner for Information of Public Importance and Personal Data Protection for the year 2021 (hereinafter, DPA 2021 Report) [Online]. Available at: https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2021/Izve%C5%A1ta2021CIR.pdf (Accessed: 14 July 2022), p. 96.
52 | Ibid, p. 60.
53 | LPPD, Art. 95.

The LPPD provides for an individual's right to receive compensation from the controller or processor of personal data for the material or non-material damage suffered.[54] Although the breaches of privacy in the digital world may be efficiently terminated in proceedings before the DPA, the compensation cannot be obtained in the same manner but in separate civil law proceedings under the general principles of civil wrongs (torts). If personal data has been controlled and/or processed by several controllers/processors, they shall bear unlimited solidary/joint responsibility.[55]

5. Personal data protection in the context of global online markets

Given the global character of the Internet, the protection of personal data may also depend on the following factors: (1) efficient cooperation among DPAs, (2) extraterritorial application of data protection rules, and (3) adequate regulation of international transfer of personal data. We shall analyze these factors from the point of view of Serbian stakeholders.

The European right to the protection of personal data builds on three main pillars: the obligations of data controllers, the rights of data subjects, and the role of data protection authorities.[56] The GDPR recognizes the importance of international cooperation for the protection of personal data by requiring the European Commission and the national DPAs of the Member States to (1) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; (2) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance, and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (3) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and (4) promote the exchange and documentation of personal data protection legislation and practice, including jurisdictional conflicts with third countries.[57] The Serbian LPPD contains an almost identical provision for international cooperation.[58] From the available public sources, it may be concluded that such international cooperation mainly consists of shared experiences and discussions within different international forums. The Serbian DPA participates in the activities of the Consultative Committee of Convention 108 (Council of Europe), International Conference of Information

54 | LPPD, Art. 86 para 1.
55 | Ibid, Art. 86 para 5.
56 | Giurgiu and Larsen, 2016, p. 342.
57 | GDPR, Art. 50.
58 | LPPD, Art. 72.

Commissioners, Global Privacy Assembly, European Data Protection Board, International Working Group on Data Protection in Technology (IWGDPT), Initiative 2017[59], UNESCO, etc.[60]

There is an inherent conflict between the borderless character of the Internet and the system of legal rules corresponding to state borders. To overcome this problem, data protection rules may be prescribed to have extraterritorial reach. Both Serbian and EU legislators proceeded in this manner. Consequently, the LPPD applies to the processing of personal data of data subjects with residence in the territory of the Republic of Serbia by a controller or processor who does not have its business seat or place of residence in the territory of the Republic of Serbia, where the processing activities are related to: (1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the territory of the Republic of Serbia; and (2) the monitoring of data subject's behavior as far as their behavior takes place within the territory of the Republic of Serbia.[61] Although the Republic of Serbia is not an EU member state, the Union's General Data Protection Regulation may, under specific circumstances, be applicable in the Serbian context. The GDPR applies to the processing of personal data of data subjects who are in the union by a controller or processor not established in the union, where the processing activities are related to (1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the union; or (2) the monitoring of their behavior as far as their behavior takes place within the union.[62] This means that companies that have a connection with the European market must follow the same standard of data protection practiced by European companies.[63]

Given the global character of the Internet, personal data transfers to a foreign country or an international organization occur rather frequently. The generalized acquisition of large amounts of data often appears to be a necessary strategy to maintain the competitiveness of companies and simultaneously introduce innovative products.[64] Therefore, all major jurisdictions regulate such international personal data transfers. The LPPD prescribes two relevant grounds for exceptions based on which personal data may be transferred to third countries or international organizations without approval of the DPA: (1) adequate level of protection or (2) adequate or appropriate safeguards.[65] A transfer of personal data to another country, to a part of its territory, or to one or more sectors of certain activities in that country, or to an international organization, without prior approval, may be performed if it is determined that such other country, part of its territory, or one or more sectors of specific activities in that country or that international organization provides an adequate level of protection of personal data. It is considered

59 | The 'Initiative 2017' group consists of data protection authorities from the countries of former Yugoslavia.
60 | DPA 2021 Report, pp. 132–133.
61 | LPPD, Art. 3 para. 4.
62 | GDPR, Art. 3 para. 2.
63 | Jaeger Junior and Copetti Cravo, 2021, p. 367.
64 | Stazi, 2019, p. 111.
65 | LPPD, Arts. 63–71.

that the appropriate level of protection is provided in countries and international organizations that are members of the Council of Europe's 'Convention 108', or in countries, parts of their territories or in one or more sectors of certain activities in those countries or international organizations for which the European Union established that they provide an adequate level of protection. The Government of Serbia has adopted a Decision on the list of countries, parts of their territories, or one or more sectors of certain activities in those countries and international organizations where it is considered that an adequate level of protection of personal data is ensured.[66] Further to the list of countries adopted by the Government, the LPPD prescribes that an adequate level of protection is deemed to have been provided if an international agreement on the transfer of personal data has been concluded with another country or international organization. If a data transfer is planned for a country that is not on the list of countries providing an adequate level of protection, the transfer can only be carried out with the special consent of the DPA.

6. Concluding remarks

An analysis of the personal data protection mechanism developed in Serbian administrative law has revealed that the procedure before the DPA represents an efficient mechanism for terminating various offline and online breaches of data protection rules. Our comparative analysis also revealed that the provisions of the Serbian LPPD are harmonized with those of the EU's GDPR to a high extent. The main deficiency of the Serbian personal data protection system that our analysis identified was the inadequate articulation of different protection mechanisms. The LPPD asserts that lodging a complaint before the DPA does not affect the data subject's right to initiate other administrative or judicial proceedings. However, the possibility that several state authorities at the same time discuss the same legal matter may lead to contradictory decisions being passed by these authorities. Another remark may be made with respect to the need for better articulation of the activities of different national DPAs. Given the global character of the Internet and the fact that most breaches of personal data protection rules take place in an online environment, that cooperation between national authorities is strengthened and regulated is of the utmost importance.[67] Presently, such cooperation mainly comprises of exchanging experiences within different international forums. Cooperation among DPAs must enter a more advanced phase, in which international mutual assistance in the enforcement of legislation should be provided, including through notification, complaint referral, and investigative assistance.

66 | Official Journal of the Republic of Serbia 55/2019.
67 | On the problem of divergent interpretation of similar GDPR-modeled rules, see: Jori, 2015, p. 133; Daigle and Khan, 2020, pp. 1–38.

Bibliography

Daigle, B., Khan, M. (2020) 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities', *Journal of International Commerce and Economics*, 2020(1), pp. 1–38.

Giurgiu, A., Larsen, T. A. (2016) 'Roles and Powers of National Data Protection Authorities. Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?', *European Data Protection Law Review*, 2(3), pp. 342–352; https://doi.org/10.21552/EDPL/2016/3/9.

Greenleaf, G. (2011) 'Independence of data privacy authorities: International standards and Asia-Pacific experience', *University of Edinburgh School of Law Working Paper Series*, 2011(42), pp. 1–47; https://doi.org/10.2139/ssrn.1971627.

Hoofnagle, C. J., van der Sloot, B., Zuiderveen Borgesius, F. (2019) 'The European Union general data protection regulation: what it is and what it means', *Information & Communications Technology Law*, 28(1), pp. 65–98; https://doi.org/10.1080/13600834.2019.1573501.

Jaeger Junior, A., Copetti Cravo, D. (2021) 'The extraterritoriality of the right to data portability: Cross-border flow between the European Union and Brazil' in Cunha Rodrigues, N. (ed.) *Extraterritoriality of EU Economic Law.* 1st edn. Cham: Springer, pp. 359–370; https://doi.org/10.1007/978-3-030-82291-0_17.

Jóri, A. (2015) 'Shaping vs applying data protection law: two core functions of data protection authorities', *International Data Privacy Law,* 5(2), pp. 133–143; https://doi.org/10.1093/idpl/ipv006.

Mišković, M. (2020) 'Pravo na zaborav – pravni i računarski aspekti' [Right to be forgotten – legal and computational aspects] in Popović, D. V. (ed.) *Intelektualna svojina i internet: 2020 [Intellectual Property and the Internet: 2020].* 1st edn. Belgrade: Pravni fakultet Univerziteta u Beogradu, pp. 123–143.

Presthus, W., Sønslien, K. F. (2020) 'An Analysis of Violations and Sanctions Following the GDPR', *International Journal of Information Systems and Project Management*, 9(1), pp. 38–53; https://doi.org/10.12821/ijispm090102.

Raab, C., Szekely, I. (2017) 'Data protection authorities and information technology', *Computer Law & Security Review,* 33(4), pp. 421–433; https://doi.org/10.1016/j.clsr.2017.05.002.

Resanović, A. (2019) 'Zaštita podataka o ličnosti u Srbiji' [Personal data protection in Serbia] in Ružić, N., Kovačević, R., Pavlović, S., Resanović, A., Zozi Jeković, M. (eds.) *Petnaest godina rada Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti: Zbornik [Fiftheen years of the institution of Commissioner for information of public importance and personal data protection: A monograph].* 1st edn. Belgrade: Commissioner for information of public importance and personal data protection, pp. 39–51.

Stazi, A. (2019) 'Data circulation and legal safeguards: a European perspective', *Comparative Law Review*, 10(1), pp. 89–113.

Wachter, S. (2018) 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR', *Computer Law & Security Review*, 34(3), pp. 436–449; https://doi.org/10.1016/j.clsr.2018.02.002.