UDC 342.738(497.11); 342.738(4-672EU:497.11)
CERIF: S 123
DOI: 10.51204/Anali_PFBU_26203A

Milana PISARIĆ, PhD*

PERSONAL DATA PROCESSING BY THE POLICE IN SERBIA: ASSESSING COMPLIANCE WITH CONSTITUTIONAL, ECHR AND EU LAW STANDARDS

The protection of natural persons regarding the processing of their personal data is a fundamental human right recognised in international and national law. Data protection principles and rules should be respected even when personal data is processed by law enforcement agencies. For the interpretation of this constitutionally guaranteed right, the standards from the case law of the European Court of Human Rights on data protection under Article 8 of the European Convention on Human Rights are relevant. In addition, the harmonisation of national legislation with EU rules on personal data processing for law enforcement purposes also serves to protect this right. The author analyses the domestic legal framework for data processing by the police, in order to establish whether and to what extent the national legal system has achieved compliance with the constitutional guarantee of the right to data protection, ECtHR standards and EU acquis.

Key words: *Human rights. – Data protection. – Police. – Serbia.*

* Assistant Professor, University of Novi Sad Faculty of Law, Serbia, *mpisaric@pf.uns.ac.rs*, ORCID iD: 0000–0001–8344–3349.

1. INTRODUCTION

Data protection, as an increasingly important social, legal and political issue, is not about the adopting a single legal act, but about the integration of the protective principles and rules in all relevant laws and their enforcement in the processing of personal data, in various spheres of life, by various competent entities. Law enforcement, as a 'data-intensive activity', produces significant quantities of data, while processing, inter alia, personal data; therefore, it should not be left out of a comprehensive legal framework on data protection (Aidinlis *et al*. 2024, 4).

The adequate protection of personal data with regard to data processing for law enforcement purposes is a significant indicator that human rights are respected in a country, and this is of the utmost importance for its image and status in international and regional context, especially with regard to law enforcement and judicial cooperation in criminal matters (Funta, Ondria 2021, 150). These requirements necessitate designing and implementing a strategic approach, in order to ensure appropriate legal and factual conditions for the development and operation of capacities for the protection of personal data.

The Constitution of the Republic of Serbia[1] guarantees the protection of personal data, as an inalienable human right, among other human and minority rights and freedoms (Art. 42). The manner of exercising this right is regulated by law – the Law on Personal Data Protection (LPDP) [2]– while provisions on data processing for various purposes are contained in different sectoral laws, which should be in line with the LPDP. In addition, as a member of the Council of Europe (CoE) and a signatory to the European Convention on Human Rights (ECHR), the Serbian state is required to ensure effective protection for guaranteed human rights, among other things, through the creation of a legal framework that respects the principles established in the case law of the European Court of Human Rights (ECtHR). Also, being a candidate for the membership in the European Union (EU), Serbia is required to ensure the harmonisation of its national legislation

[1] *Official Gazette of the RS* 98/2006, 115/2021 (Amendments I–XXIX), and 16/2022.

[2] *Official Gazette of the RS* 87/2018.

with current and future EU law, not only with the General Data Protection Regulation (GDPR),[3] but also with the Law Enforcement Directive (LED),[4] which addresses data processing by police.

With regard to personal data processing by law enforcement authorities (LEA), the author questions whether and to what extent the domestic law has achieved compliance with the constitutional guarantee of the right to personal data protection and other constitutional principles, as well as with ECtHR standards and EU rules.

2. DOMESTIC LAW

The constitutional guarantee of personal data protection, as a human right, has been present in Serbia for more than 30 years,[5] while the manner of exercising this right has been regulated in three laws so far (1998, 2008 and 2018[6]), the LPDP being the most recent of them.

---

[3] 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, *OJ L 119 of 4/5/2016*, 1–88.

[4] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ* L 119 of 4/5/2016, 89–131.

[5] While the 1974 Yugoslav Constitution did not guarantee the right to protection of personal data among the freedoms and rights of men and citizens, which is understandable given the social circumstances of the time, the 1990s constitutions, both of Yugoslavia and Serbia, recognised and explicitly guaranteed this human right.

Constitution of the Socialist Federal Republic of Yugoslavia, *Official Gazette of the SFRY* 9/1974; Constitution of the Federal Republic of Yugoslavia, *Official Gazette of the FRY* 1/1992; Constitution of the Republic of Serbia, *Official Gazette of the RS* 1/1990.

[6] Although the 1992 Yugoslav Constitution (Art. 33) and 1990 Serbian Constitution (Art. 20, guaranteeing the protection of *confidentiality* of personal data) stipulated that data protection/processing is to be regulated by law, such a law was enacted only in 2008 (Law on Personal Data Protection, *Official Gazette of the FRY* 24/1998, and 26/1998 – correction). As this first domestic act was not fully in line with the requirements of EU data protection rules, after the adoption of the Constitution of the Republic of Serbia in 2006, which also required the legal regulation of data processing, the new Law on Personal Data Protection was adopted in 2008, with the

2.1. The Constitution

The Serbian Constitution *explicitly guarantees the right to personal data protection* (Art. 42 para. 1). The constitutional principle of direct application of human rights (Art. 18 para. 1) means that the guarantee alone is sufficient for the realisation of this right, i.e. it is not necessary for the constitutional norm to be specified in a law or any other regulation. Still, even though the Constitution does not provide that the protection of this right is regulated by law, it is necessary to norm the mechanism of its protection, in order to ensure the effective exercise of this right (Simović, Orlović 2023, 307). Additionally, the constitutional protection also covers the guarantee of *procedural rights*: the right to be informed about the collected personal data, in accordance with the law, and the right to judicial protection due to their misuse (Art. 42 para. 4). Therefore, the LPDP, as an 'umbrella' law, prescribes the way of exercising the right to personal data protection in connection with the processing, principles of processing, rights of the data subjects, etc. (Art. 1 LPDP), applying to personal data processing by the police for LEA purposes as well.

The Constitution partially determines the *content of this right*, providing that the collection, storage, processing and use of personal data are regulated by law (Art. 42 para. 2). The relevant provisions are contained in many laws regulating different areas (such as education, employment, etc.). As for data processing by the police for LEA purposes, in addition to in the LPDP, the relevant norms are contained in the Criminal Procedure Code (CPC),[7] the Law on Police (LP),[8] and the Law on Records and Data Processing in the Field of Internal Affairs (LRDP).[9]

---

aim of incorporating the relevant EU standards (Law on Personal Data Protection, *Official Gazette of the RS* 97/2008, 104/2009 – other law, 68/2012 – decision of the Constitutional Court, and 107/2012).

Meanwhile, Serbia gained the status of a candidate for membership in the EU in 2013, thus acquiring the formal legal obligation to harmonise national legislation with the EU acquis on personal data protection. In order to achieve this, a new law was enacted in 2018 (the LPDP).

[7] Criminal Procedure Code, *Official Gazette of the RS* 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – decision of the Constitutional Court, and 62/2021 – decision of the Constitutional Court.

[8] Law on Police*, Official Gazette of the RS* 6/2016, 24/2018 and 87/2018.

[9] Law on Records and Data Processing in the Field of Internal Affairs*, Official Gazette of the RS* 24/2018.

The Constitution contains the *purpose limitation principle*, by declaring that the use of personal data outside the purpose for which it was collected in accordance with the law, is *prohibited and punishable* (Art. 42 para. 3).[10] Nevertheless, the use of personal data beyond the initial purpose is allowed for the purpose of conducting criminal proceedings, or protecting the security of the Republic of Serbia, in the manner provided by law (Art. 42 para. 3). With regard to the purpose of criminal proceedings, the provisions of the CPC, the LP and the LRDP are relevant.

It is especially important to take into consideration that each law containing provisions on personal data processing and/or protection should be in line with the LPDP, accordingly to the *unity of the legal order* principle (Art. 194 para. 1), whereby all laws must be in accordance with the Constitution (Art. 194 para. 3). Nonetheless, with regard to data processing by the police, these constitutional principles *are not consistently respected*, since the relevant laws are not fully in line with the LPDP (see 2.2), while the constitutionality of some of their provisions is questionable.[11]

The right to the protection of personal data should be viewed *more broadly*, since the Constitution expands the guarantees to human rights recognised in the generally accepted rules of international law and

[10] The LPDP sets the basis of misdemeanour liability for processing data for other purposes contrary to the law (Art. 95 para. 1 (2)), while the Criminal Code establishes the criminal offence of unauthorised collection of personal data (Art. 146) (Criminal Code, *Official Gazette of the RS* 85/2005, 88/2005 – correction, 107/2005 – correction, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 and 94/2024). See, Petrović 2022, 474–478.

Additionally, the processing of personal data in violation of and contrary to other LPDP rules and principles may also be a misdemeanour (Art. 95 LPDP), or even constitute the criminal offense against the freedoms and rights of humans and citizens from Chapter XIV of the Criminal Code: e.g. violation of the confidentiality of letters and other parcels (Art.142), unauthorised wiretapping and recording (Art. 143), unauthorised photography (Art. 144), unauthorised publication and display of someone else's document, portrait and recording (Art. 145), unauthorised collection of personal data (Art. 146). Thereby, the commission of the act by an official in the performance of duties is envisaged as a qualifying circumstance, making these criminal offenses more serious, prosecuted ex officio by the public prosecutor. See, Đorđević 2025; Sekulić, Grujić 2020.

[11] For example, there is the issue of whether the CPC provisions on notifying the person whose telephone communication records have been obtained from the operator (Art. 286 para. 5) or who is affected by secret surveillance of communications (Art. 163), are consistent with the constitutionally guaranteed right (Art. 42 para. 4), since the right to notification with respect to police processing operations corresponds to the notification duty of the authorities that process data, and which is not adequately addressed in law. See, Pisarić, Kalaba 2025, 29; ECtHR, *Szabó and Vissy v. Hungary*, Application No. 37138/14, 12 January 2016, §86.

confirmed international treaties (Art. 18 para. 2), as an integral part of the legal order (Art. 194 para. 4) (Prica 2018, 112). Therefore, elements or sub-rights of the right to the protection of personal data, guaranteed by confirmed international treaties, are *directly enforceable,* the same way as the rights explicitly guaranteed in the Constitution (Art. 18 paras. 1 and 2). These rights include those guaranteed in the ECHR, but also those from the CoE's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[12] (Art. 3), and the protocol amending it[13] (Art. 11, entering into force in the future), CoE's Convention on Cybercrime[14] (Art. 15), and its Second Additional Protocol[15] (Arts. 13–14, entering into force in the future). The same applies to the rights in other confirmed international treaties with data protection provisions.

In addition, the Constitution establishes *interpretative rules* for determining the content and scope of constitutional provisions on human rights, providing that they *should be interpreted* in favour of promoting the values of a democratic society, in accordance with valid international human rights standards, as well as the case law of international institutions that supervise their implementation (Art. 18 para. 3).[16] Accordingly, *the ECtHR standards* oblige not only the legislator, but also the courts and other state authorities, especially during the limitation of the right to personal data protection.

[12] CETS No. 108, see Law on Confirmation of the Convention on the Protection of Persons in Relation to Automatic Processing of Personal Data, *Official Gazette of the FRY – International Treaties* 1/1992, *Official Gazette of CS – International Treaties* 11/2005 – other law, *Official Gazette of the RS – International Agreements* 98/2008 – other law, and 12/2010.

[13] CETS No. 223, see Law on Confirmation of the Protocol on Amendments to Convention 108, *Official Gazette of the RS – International Treaties* 4/2020.

[14] See Law on the Ratification of the Convention on Cybercrime, *Official Gazette of the RS – International Agreements* 19/2009.

[15] Law on the Ratification of the Second Additional Protocol to the Convention on Cybercrime, on enhanced cooperation and discovery of electronic evidence, *Official Gazette of the RS – International Treaties* 7/2022.

[16] There are several such institutions at the global and regional level, from the UN Human Rights Committee to CoE bodies, etc.

2.2. Laws

Being a basic law, the LPDP prescribes the *quality and content* of other laws' provisions on personal data processing in various areas (Art. 1). *In order to achieve its main aim*, i.e. to ensure the protection of rights and freedoms of natural persons, especially their right to personal data protection (Art. 2 para. 1), the provisions of these sectoral laws must be in accordance with the LPDP (Art. 2 para. 2). This requirement emerges also from the constitutional principle of the unity of the legal order.

The LPDP establishes two regimes of data processing: the general and the special one. In the *special regime*, the LPDP regulates the right to personal data protection in connection with the processing by competent authorities, *for the purposes* of preventing, investigating and detecting criminal offenses, prosecuting perpetrators of criminal offenses or enforcing criminal sanctions, including preventing and protecting against threats to public and national security, as well as the free flow of such data (Art. 1 para. 2). These purposes are recognised as *special purposes* (Art. 6 para. 3 LPDP): when the competent authorities process the personal data beyond them, the LPDP rules on the general regime apply. Regarding the data processing for special purposes by the police, the prevention, investigation and detection of criminal offenses, including prevention and protection against threats to public security, may be regarded as *LEA purposes.*

Personal data processing by the police is also regulated in the LRDP, both for the general and the special regime in terms of the LPDP. Nevertheless, while this law refers only to processing through records (Art. 1), it should not be overlooked that the generic term *personal data processing* encompasses not only these records, but also collection, recording, classification, grouping or structuring, storage, adaptation or alteration, disclosure, consultation, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4 (3) LPDP). Therefore, besides in the LPDP and the LRDP, the relevant provisions on data processing by the police for LEA purposes are also contained in other laws, primarily in the LP and the CPC.

The LP provides the police with the general *power to process personal data* for the purpose of performing tasks falling within the scope of the Ministry of Interior (Art. 252 para. 1), whereby the LPDP special regime is applied only to data processing for LEA purposes regarding police tasks (Art.

30).[17] In performing these tasks, personal data are collected and otherwise processed through application of police powers, measures and actions, regulated in the LP[18] and the CPC.[19] The LP also provides the police with the *power to keep records of personal data processing*, prescribed by special law (Art. 252 paras. 1 and 2), and by the LRDP.

Sectoral laws, as a rule, refer to the LPDP and should be aligned with it. Such harmonisation is a formal legal requirement, arising from the Constitution and from the aim of the LPDP (Art. 2 para 2). Since many of these laws were adopted before the LPDP (the CPC and the LP, *inter alia*), their provisions were to be harmonised with it by the end of 2020 (Art. 100 LPDP). Still, the relevant amendments or supplements have not been adopted to date. [20]

In addition to the issues of internal legal (dis)harmony, the state is required to harmonise domestic legislation with the requirements of the ECHR and the ECtHR's standards, as well as with the EU rules, which has been lacking so far with regard to personal data processing by the police for LEA purposes. This requirement should be regarded as a precondition for exercising the right to personal data protection, both in terms of the Constitution and the State's international legal obligations.

[17] For example, for crime prevention; detection and elucidation of criminal acts, provision of evidence, their analysis, criminal forensic expertise using modern forensic methods and records, and discovery of property resulting from a criminal act; detection and arrest of perpetrators of criminal acts, etc. (Art. 30 para. 3).

[18] For example, recording in public places; criminal forensic registration, taking other samples and criminal forensic expertise and analysis (Art. 47 para. 2 (5) and (12)), performing security checks (Art. 64 para. 2 (13)), etc.

[19] For example, obtaining records of telephone communications, or used base stations, or locating the place from which the communication is carried out (Art. 283 para. 3).

[20] For example, the LRPD provides that the Ministry of Internal Affairs keeps records, in which it processes the specified data through video-acoustic recording, including biometric data on persons (Art. 47 para. 1). However, since it does not specify which types of biometric data are stored in the records, this article is not in accordance with Arts. 5 and 13 LPDP. For an analysis of compliance of sectoral regulations, see Ružić, Toskić Cvetinović, 2020.

2.3. Domestic law & ECHR

The state signatory of the ECHR has the primary responsibility to ensure to everyone within its jurisdiction the rights and freedoms defined in it (Preamble, recital 7). Therefore, Serbia is responsible for securing the right to protection of personal data, having not only a duty to refrain from unjustified interference with it (negative obligation), but also to ensure its effective realisation and protection (positive obligation), through basic measures needed for full enjoyment of the rights guaranteed, such as the existence of proper rules governing intervention by the police (substantive obligation) and of domestic procedures capable of ensuring the protection of rights holders (procedural obligation).

The right to protection of personal data is *not an autonomous right*, but is derived from the protection of private life under Article 8 ECHR.[21] On the other hand, the 'protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life'.[22] Ever since the issue of the storage of an individual's personal data by a public authority was analysed for the first time in 1987, the Court has developed *rich case law on data protection* under the ECHR.[23] The standards of personal data processing set in CETS No. 108 are also important for comprehending the 'Article 8 rights',[24] as the ECtHR has referred to them in several judgments.[25]

This right is *not an absolute right*, but a qualified one, meaning it may be restricted. However, the interference by a public authority in the exercise of it is allowed only in terms of Art. 8 para 2 ECHR, as a balance between individual and general interests. For collection and processing of personal data by LEA, as *an interference* with the exercise of Article 8 ECHR, to be

[21] The concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity, embracing multiple aspects of a person's identity (gender identification, sexual orientation, name or elements relating to a person's right to their image, etc.) and covering personal information which individuals can legitimately expect should not be published without their consent. See, European Court of Human Rights 2018.

[22] ECtHR, *S. and Marper v. the United Kingdom*, Application Nos. 30562/04 and 30566/04, 4 December 2008, §103.

[23] See, Directorate General Human Rights and Rule of Law 2022.

[24] Key principles include lawfulness, necessity, proportionality, fairness, transparency, purpose limitation, data minimisation, accuracy, data security, accountability, and user control over their information.

[25] See, e.g. ECtHR, *Z. v. Finland*, Application No. 22009/93, 25 February 1997, §95; ECtHR, *Uzun v. Germany*, Application No. 35623/05, 2 September 2010, §46

justified, they must (1) be 'prescribed by law' or 'in accordance with the law', (2) pursue a legitimate aim, and (3) be necessary (in a democratic society) to achieve the legitimate aim pursued. The State has to ensure that any restriction of Article 8 rights satisfies all of these requirements, while the test of necessity requires that the limitation is proportionate to the legitimate aim pursued, responds to a pressing social need, and uses the least restrictive means. Hence, any interference with the right to protection of personal data by the police should have *a clear basis* in domestic law, be *foreseeable* and adequately *accessible*;[26] compatible with the rule of law and *free from arbitrariness*,[27] with proper procedural *safeguards* to ensure fairness and due care, i.e. it must afford appropriate safeguards to prevent any use of personal data that may be inconsistent with the guarantees of Article 8 ECHR.[28]

The Court's standards should to be regarded as guidelines for national legislators when regulating personal data collection and storage by the police, in order for the relevant provisions to comply with the lawfulness requirement.

2.3.1. Personal Data Collection by the Police

Regarding personal data collection for LEA purposes, the stance of ECtHR is that the interference is not 'in accordance with the law' and represents a violation of Article 8 rights, not only in the cases where there is no legal basis, but also in a situation where a legal basis exists but it is not *sufficiently clear and foreseeable,* hence not providing the protection of personal data.

For example, the Court held that the Serbian Criminal Procedure Act used by the police to obtain subscriber information relating to *the dynamic IP address* lacks clarity and does not offer sufficient safeguards against arbitrary interference with Article 8 rights, because at the relevant time there were *no regulations* on retaining the relevant data*, no safeguards against abuse* by state officials in the procedure for accessing and transferring them*, no independent supervision* of the use of the police's powers regarding obtaining information from ISPs.[29] With regard to the installation of a geolocation tracking device on applicant' vehicle for the purpose of GPS surveillance,

[26] ECtHR, *The Sunday Times v. the United Kingdom* (No. 1), Application No. 6538/74, 26 April 1979, §§48–49.

[27] ECtHR, *R.Sz. v. Hungary*, Application No. 41838/11, 2 July 2013, §36.

[28] *S. and Marper v. the United Kingdom*, §103.

[29] ECtHR, *Benedik v. Slovenia*, Application No. 62357/14, 24 April 2018, §130.

the Court held that there had been a violation of Article 8 because, at the relevant time, the national law (neither statute law nor case law) *did not indicate with sufficient clarity to what extent and how* the authorities were entitled to *use their discretionary power*, resulting in non-existence of the minimum protection afforded by the rule of law in a democratic society.[30] Furthermore, the Court held that there had been a violation of Article 8 because the national Code of Criminal Procedure *did not provide reasonable clarity as to the authorities' discretion* in ordering surveillance measures, and in practice it did not provide sufficient *safeguards* against possible *abuse*.[31] As a consequence, when the investigating judge *simply refers to the statutory phrase that the investigation could not be conducted by other less intrusive measures, without clearly indicating why*, the procedure for ordering and supervising the telephone tapping could not be lawful in terms of Article 8.[32] In addition, the ECtHR found *several shortcomings in the national law on secret interception* of mobile telephone communications: the circumstances in which public authorities are empowered to resort to secret surveillance measures, the duration of measures and circumstances in which they should be discontinued, the procedures for authorising interception, the procedure for storing and destroying the intercepted data, the supervision of the interception.[33] Also, the ECtHR insisted that the national legal framework for secret interception of mobile telephone communications *undermines the effectiveness of the remedies* available to challenge this when they are available only to persons who are able to submit proof of interception, since obtaining such proof is impossible due to the absence of a notification system and possibility of access to information about interception.[34]

If the relevant Serbian legal framework regulating collection of personal data by LEA is analysed from the perspective of only these few, exemplary ECtHR's cases, the result would be that the law does not meet the quality of law requirements. Namely, domestic law must indicate 'with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities so as to ensure to individuals the minimum degree of protection to which they are entitled under the rule of law in a democratic society',[35] which Serbian national law fails to do in certain cases.

---

30 ECtHR, *Ben Faiza v. France*, Application No. 31446/12, 8 February 2018, §60.

31 ECtHR, *Dragojević v. Croatia*, Application No. 68955/11, 15 January 2015, §98.

32 ECtHR, *Matanović v. Croatia*, Application No. 2742/12, 4 April 2017, §114.

33 ECtHR, *Roman Zakharov v. Russia*, Application No. 47143/06, 4 December 2015, § 302.

34 *Ibid*.

35 ECtHR, *Piechowicz v. Poland*, Application No. 20071/07, 17 April 2012, §212.

For example, the police are not authorised to lawfully process personal data by using certain modern technologies and technical means, e.g. drones, etc. (Milidragović, Milić 2023, 142). Hence, the eventual use of police spyware, without clear legal basis in the CPC, could not be regarded as interference in accordance with law. Moreover, personal data processing, the basis of which would be derived from some general provisions, would not meet the clarity requirement, such as in the case of video surveillance that enables the police to process biometric data. Certain relevant CPC provisions lack clarity. For example, Article 286 paras. 3–5 CPC (obtaining records of telephone communication and/or used base stations, or locating the place from which the communication is carried out),[36] or Article 163 (dealing with material collected by special evidentiary actions)[37] do not provide the minimum protection as they do not offer sufficient safeguards against arbitrary interference nor provide the effectiveness of the remedies. Thus, the ECtHR would undoubtedly reach conclusions similar to those in the presented cases, whereby, a finding that the measure in question is not 'in accordance with the law' suffices for the Court to hold that there is a violation of Article 8 ECHR, i.e. there would be not need to examine whether the interference in question pursues a 'legitimate aim' or is 'necessary in a democratic society'.

2.3.2. Personal Data Storing by the Police

The ECtHR has found that the mere storing of data related to the private life, by a public authority, amounts to an interference, regardless of how that information was obtained and whether the data is subsequently used.[38] In determining whether the personal information retained by the authorities involves any of the private-life aspects, the Court has due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.[39]

---

[36] See, Pisarić, Kalaba 2025.

[37] Especially because ECtHR has recognised the notification and the right of access to one's data as *an element or sub-right under Article 8* ECHR (Dimitrova, De Hert 2025, 56).

[38] ECtHR, *Amman v. Switzerland*, Application No. 27798/95, 16 February 2000, §69.

[39] *S. and Marper v. the United Kingdom*, § 67.

Although the national authorities *can legitimately set up databases* as an effective means of helping to punish and prevent certain offences, including the most serious types of crime,[40] when police is *collecting criminal record data indiscriminately and open-ended*, that may not meet the Article 8 ECHR requirements 'in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, *inter alia*, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed'.[41]

The ECtHR has in several cases questioned *the broad scope of the data storage system* set up by the authorities. For instance, the Court held that the state oversteps its 'margin of appreciation' when relevant provisions do not provide *a real possibility of seeking the deletion of personal data* from the police database (a system for processing recorded offences, containing information from investigation reports, listing the individuals implicated and the victims) after the discontinuance of criminal proceedings. In addition, 'the length of retention of that data, 20 years, could be assimilated, if not to indefinite retention, at least to a norm rather than to a maximum limit'.[42] The Court also found in several cases that there had been a violation of Article 8 concerning retention of fingerprints and DNA profiles in a police database, being a disproportionate interference with the Article 8 right, unnecessary 'in a democratic society': e.g. when the fingerprints, cellular samples and DNA profiles of those persons are *indefinitely retained*, moreover if the fingerprints of *persons suspected of an offence but not convicted* are retained.[43]

When these findings are applied to the LRDP, it is not difficult to imagine what the conclusion of the ECtHR would be. For example, the Serbian Ministry of the Interior permanently keeps, as secret data, records on access to retained data in telecommunications traffic (among other things, the person's name and surname, personal identification number, IMEI number of the telephone, user number, e-mail address) (Art. 42). In the records on the application of criminal-operational measures and actions and the results of their application, fingerprints, personal identification number, DNA profile, video or audio recording, blood type and other information about the suspect are also kept permanently as secret data, as are fingerprints, personal identification number and DNA profile of the injured party or

40 ECtHR, *Gardel v. France*, Application No. 16428/05, 17 December 2009, §63.

41 ECtHR, *M.M. v. the United Kingdom*, Application No. 24029/07, 13 November 2012, §199.

42 ECtHR, *Brunet v. France*, Application No. 21010/10, 18 September 2014, §43.

43 ECtHR, *M.K. v. France*, Application No. 19522/09, 18 April 2013, §46.

victim of a criminal offense – regardless of whether criminal proceedings have been initiated and the outcome of the proceedings (Art. 43). Namely, the *domestic law* should provide the *appropriate safeguards to prevent any use* of personal data that may be inconsistent with the guarantees of Article 8, especially concerning automatic processing and when data are used for police purposes, ensuring 'that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects *for no longer than is required for the purpose* for which those data are stored'.[44]

3. TOWARDS THE EU

Since the protection of natural persons with regard to the processing of personal data is recognised as a *fundamental right* in EU law,[45] the protective principles and rules should to be applied, ensuring that this right is *legally enforceable*. In the area of freedom, security and justice, this request is *accomplished though the LED*, which aims to *protect personal data* when processed by police or law enforcement and criminal justice authorities, and to *improve cooperation* in the fight against terrorism and cross-border crime. Namely, the LED *sets rules* for protection and free movement of personal data when being processed *for the purposes* of prevention, investigation, detection and prosecution of criminal offences or execution of criminal penalties, including safeguards against and prevention of threats to public security (LED purposes). By requiring member states to transpose the rules into their national law, the LED aims to provide *harmonisation*, in order to ensure the same level of protection throughout the Union, hence increasing trust and facilitating cooperation in the fight against crime in the EU. Nevertheless, the set rules should be regarded *as a minimum*, and the LED itself is not the barrier for states to provide even higher safeguards than those established by it.[46]

The aforementioned requirements are relevant for countries that strive to become a part of the EU, including for Serbia. Although previously Serbia used EU rules on personal data protection as a model, since obtaining *the status of a candidate* for the membership in 2013, when the Stabilisation

[44] *S. and Marper v. the United Kingdom*, § 103, emphasis by author.

[45] This right is guaranteed in Art. 8(1) of the Charter of Fundamental Rights of the European Union and Art. 16(1) of the Treaty on the Functioning of the European Union.

[46] For the LED background, see Leiser, Custers 2019, 369–370.

and Association Agreement (SAA) entered into force,[47] the country became *legally required* not only to *harmonise* the current national framework with EU law in this area, to *continuously follow new EU* rules and amend and supplement the domestic legal framework accordingly, but also to ensure that current and future legislation is *properly implemented and enforced* (Art. 72). Additionally, there is an explicit obligation concerning personal data protection (Art. 81 SAA).

However, there is a question whether Serbia has fulfilled its obligation to ensure full and consistent compliance in accordance with the SAA, i.e. whether harmonisation with the LED and effective implementation of LED-inspired rules have been achieved.

3.1. Harmonisation

The Serbian Law on Personal Data Protection was passed with the aim of *harmonising national legislation* related to the protection of personal data with the EU legislation and other European and international regulations on privacy (Art. 81 SAA[48]), with regard both to the GDPR (the general regime) and the LED (the special regime).

As for the *scope* of the special regime, in defining *special purposes*, the LPDP adds national security, in addition to safeguarding against and the prevention of threats to public security (Art. 6 para. 3). The inclusion of this purpose of data processing is inconsistent with the Preamble (14) and Articles 1 and 2 of the LED, however, 'as Member States are allowed to provide for higher standards of protection beyond the LED, they may extend its applicability to processing activities also in pursuit of national security' (Vogiatzoglou, Marquenie 2022, 24). Although it might appear that the legislator had an even greater protective attitude, this inclusion in the LPDP is just a formal-textual curiosity with no real significance, since the laws regulating the work of security services do not meet the requirements of the

[47] The Law on Confirmation of the Stabilisation and Association Agreement between the European Communities and their Member States, on the one hand, and the Republic of Serbia, on the other hand, *Official Gazette of the RS – International Agreements* 83/2008. On 14 June 2010, the Council of Ministers of Foreign Affairs of the European Union passed a decision to start the ratification of the Stabilisation and Association Agreement with Serbia. The European Parliament ratified the Stabilisation and Association Agreement with Serbia on 19 January 2011, and the ratification process by the EU member states ended on 18 June 2013, after the ratification by Lithuania.

[48] SAA Chapter 7: Justice, freedom and security.

principle of lawfulness of data processing (Art. 5 LPDP), nor the conditions for the legality of processing carried out by competent authorities for special purposes (Art. 13 LPDP). Additionally, by simply rewriting the LED text (Art. 3 (7)), the LPDP defines *competent authorities* as: a) *public authorities* whose responsibility is connected with special purposes;[49] b) *legal entities* that are authorised by law to carry out connected tasks.[50] However, such legal wording is not sufficiently precise and specific. Consequently, it is unclear which competent authorities are required to apply the LPDP provisions on data processing for special purposes, hence, in order for the special regime to have a real impact on ensuring legal certainty, in terms of the competent authorities complying with the rules, and exercising the rights of individuals whose data are processed, it is necessary to specify these definitions.[51] In addition, the tasks of competent authorities are regulated by several other laws, which are left out of any reform aimed at harmonisation with the LED.

3.1.1. Inadequate Legislative Technique

Being a directive, the LED is not directly applicable: it sets objectives, while member states need to incorporate its provisions into domestic legislation using national laws, choosing from various legislative transposition methods and possibilities for implementing LED in accordance with the national law (Hudobnik 2020, 499). The Serbian LPDP was designed in such a manner that the legislator simply took the wording of the GDPR and the LED and mixed them together into one normative act, whereby it did not take into account the different legal force, effect, applicability, scope and meaning of two different sources of EU law (Petrović 2024, 61), nor did it consider the

[49] These *public authorities* are undoubtedly the police, public prosecutor's offices, the Administration for the Enforcement of Penal Sanctions, security agencies, but also a number of other authorities, which process personal data for special purposes in the course of performing their tasks, e.g. the Tax Administration and the Tax Police, the Customs Administration, the Agency for the Prevention of Corruption, etc.

[50] As for *legal entities*, several laws authorise certain legal entities to carry out tasks that include the processing of personal data for special purposes, hence there are many possible cases to which the provisions of the LDPD on special regime would apply (e.g. Private Security Act, *Official Gazette of the RS* 104/2013, 42/2015 and 87/2018; Law on Prevention of Money Laundering and Financing of Terrorism, *Official Gazette of the RS* 113/2017, 91/2019, 153/2020, 92/2023, 94/2024, and 19/2025).

[51] What the legislator may do, and which is not simply a technical issue but would serve the principle of lawfulness, is to exhaustively list the regulations, or at least the areas, in which public authorities and legal entities perform data processing for special purposes.

existing national legal system. Being a directive, the LED only lays down the demands that must be achieved by taking appropriate steps in national legislation in order to achieve the expected results. Although the choice of form and method of transposition is left to the member state, the LPDP provisions on the special regime that literally repeat (translate) the LED text containing a requirement, without taking into account the specificities and requirements of the domestic legal system, cannot be viewed as a proper transposing method nor considered as a manner of fulfilling the LED requirements.[52]

In addition, the LPDP is a cumbersome act, whose text, to the greatest extent, represents mere translation of the LED provisions (inadequate, in some cases). The articles contain an inappropriate number of paragraphs, there are numerous cases of exemption from the set rules, no clear and noticeable distinction was made between the two regimes, etc.,[53] which renders the LPDP wording sloppy, to the point of being illegible. Instead of the transposed provisions of the LED being systematised – perhaps in a separate chapter on data processing for special purposes, or even in a separate law – they are scattered throughout the law, making it difficult to read and understand their aim and purpose. Moreover, the legal wording is very declarative, and does not contribute to legal clarity, nor facilitate the transmission of the LED and the applicability of its provisions – on the contrary, it leaves a wide space for different interpretations and offers

[52] For example, Art. 28 LPDP, which governs the limitation of the right of access, in para. 1 lists the reasons for which this right can be limited (literal translation of Art. 15 LED), and then para. 2 simply states that the law 'can determine' the types of processing that, as a whole or partially, may be covered by some of the cases from para.1. This legal solution cannot be considered as a proper transposition of Art. 15 LED, because such a provision has no place in the LPDP nor any real effect (nor is it a common nomotechnics approach in domestic legal system). Simply repeating the words from the LED does not ensure transposition into national law, or rather does not ensure the satisfaction of the requirements of the LED. Instead, it was necessary to regulate this matter in sectoral laws, as it is done e.g. in Art. 6 LRPD.

[53] From nomotechnics point of view, the regulation of the legal regimes in the LPDP is conducted through two methods: a) the rules for the general regime are set in one or several paragraphs of an article, followed by a paragraph that stipulates that previous rules do not apply to data processing for special purposes – *as an exception to the general rule* (e.g. in Art. 54, which governs the assessment of the impact on the protection of personal data, the rules are set for the general regime, and then in paras. 7 and 10 it is prescribed that the previous paragraphs do not apply to processing carried out by competent authorities for special purposes); b) the rules for the general regime are set in one article, followed by an article that governs the same data processing for special purposes – *as a special rule* (e.g. the processing for other purposes is regulated in Art. 6 for the general regime, and then Art. 7 regulates the processing by competent authorities for other purposes).

a great deal of discretion regarding its enforcement. Due to the difficulty of understanding the provisions, there is a veil of mystery over this law – however, nothing should be mysterious about it, and the rules should be clear and precise and 'its application foreseeable', as required by the case law of the EU Court of Justice (CJEU) and the ECtHR (LED Preamble, 33), especially when it comes to data processing for LEA purposes.

3.1.2. (In)consistence of the Legal Framework with the LED Principles

The wording of the data protection principles established by the LPDP for both data processing regimes (Art. 5), generally corresponds to the LED principles.[54] However, the mere prescribing of principles, even by using the literal translation of the LED provisions, does not represent an appropriate or sufficient transposing measure. Since the rules on data processing for special purposes are contained in numerous other laws, these principles, as guiding rules, *would only make sense if all of these other laws were fully aligned with the LPDP*, which is not the case.

1. For illustration, following Article 8 LED, which defines the *principle of lawfulness* of data processing for special purposes, the LPDP states that a processing is legal only if it is *necessary* for the performance of the tasks of competent authorities and *prescribed by a law* that *should determine*, at the least, the goals of processing, the personal data being processed, and the purposes of the processing (Art.13). In order to speak of a genuine respect of this principle, all sectoral laws, governing data processing for special purposes within the scope of the LED, should meet this requirement (Art. 8(2) LED), i.e. it should specify which authority is competent to process what personal data for which task and purpose, since 'a mere repetition of Article 8 LED in the national transposing law does not constitute a legal basis' (European Commission 2022, 14).

   The LRDP contains an exhaustive list of purposes for which the police may process personal data in general (Art. 3), and then determines the specific goal for each police record, listing data being processed within it (e.g. for records of security checks, identity verification, fingerprinting, photography). Nonetheless, keeping records on data is only one of data processing actions, therefore the LP and the CPC,

[54] These are lawfulness, fairness and transparency; limitation regarding the purpose of processing; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability for action.

as a legal basis for collection and other data processing within the meaning of the LED, should also meet the lawfulness requirement, i.e. they should be clear, precise and specific in determining at least the objectives, the personal data to be processed, and the purposes of the processing. This requirement corresponds to standard of 'in accordance with the law' determined by the ECtHR (see 3.1).

2. The *storage time limit principle* is set in the LPDP in accordance with the LED, requiring that the data be stored in a form that enables the identification of the person only *for the period necessary* to achieve the purpose of the processing, whereby, if it is about personal data processed by competent authorities for special purposes, *a deadline must be set* when that data will be deleted, i.e. a deadline for periodic assessment of the need to keep it (Art. 8 para. 2 LPDP). However, it cannot be deemed that this LED principle is respected in the domestic legislation, *since sectoral laws fail to limit data storage*. For example, the LRPD provides for permanent storage within the operational-criminal collection of many categories of personal data processed by police, such as the case of personal data of a suspect (personal identification number, blood type, fingerprints, and DNA profile) (Art. 41). Such unlimited storage 'is unlikely to be adequate, relevant, and reasonable', nor meets the necessity test (Leiser, Custers 2024, 154). In addition, it does not correspond to ECtHR standards (see, 3.2). In addition, such blanket and indiscriminate nature of the power of retention[55] would not meet the requirement of the *data minimisation principle*, which requires that personal data should be 'not excessive' (Art. 4(1)(c) LED), i.e. not kept longer than necessary for the purpose pursued and only if the purpose of the processing could not reasonably be fulfilled by other means.[56]

There are also several significant omissions in the LPDP, due to which it seems that the legislator did not take into account that the data protection principles are interconnected. For instance, the *purpose limitation principle*, as the cornerstone of data protection law, serves as a guarantee against abuse and arbitrariness (Sunde 2023, 501). Thereby, it is also of importance to other data protection principles, such as storage limitation and lawfulness (Te Molder *et al*. 2023, 516). The LED-set principle requires that the data

[55] CJEU, case C-118/22, Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti, ECLI:EU:C:2024:97, paras. 63–65.

[56] Opinion of AG Pitruzzella to CJEU, C-205/21, Ministerstvo na vatreshnite raboti, ECLI:EU:C:2022:507, paras. 54–55.

needs to be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (Art. 4(1) (b)). The same wording is also used in the LPDP (Art. 5 para. 1 (2)). However, the LPDP approaches the exemption from the purpose limitation principle in a different way.

a. The LPDP allows personal data collected for one purpose to be processed for a different purpose, under the condition that the further processing is prescribed by law (Art. 7 para. 1). *Instead of limiting the purposes for further processing only to special purposes* (which the LED explicitly does[57]), the LPDP permits for data originally collected by police to be processed for any other purpose, by any subject that the law would determine/authorise. This is not in line with the LED purpose limitation principle, and more importantly, it is contrary to Art. 42 of the Constitution, which allows the use of personal data beyond the purpose for which they were collected, exclusively for the purposes of conducting criminal proceedings or protecting the security of the Republic of Serbia. The same applies to the provisions of the LRDP on data exchange with other entities (Art. 9 para. 2, Art. 11 paras. 4, 5, 8).

b. In the following paragraph, the LPDP provides that processing by competent authorities for another special purpose, different from the original one, is permitted if: 1) the controller is authorised to process the personal data for such other purposes, in accordance with the law; and 2) the processing is necessary and proportionate to that other purpose, in accordance with the law (Art. 7 para. 2). From this wording it is clear that for these other purposes *there is no purpose specification requirement*. However, since the LED requires that 'every purpose must be considered as specific and separate', the same applies to that another purpose for further processing, as well (Bonetto 2024, 65). Consequently, even for data processing for the purpose 'other than that for which those data were collected', the assessment of compliance with the requirements for the lawfulness of further processing under Article 4(2) LED 'must be carried out by regarding each of the purposes referred to in Article 1(1) LED as specific and distinct'.[58] Namely, as the essence of this requirement is

[57] The LED allows the processing for other purposes, different from the one for which the personal data are collected in first place, but only *if this other purpose is covered by Art. 1(1)*, and insofar as this further processing is lawful, necessary and proportionate (Art. 4(2)).

[58] CJEU, case C-180/21, Inspektor, ECLI:EU:C:2022:967, para 56.

to offer foreseeability of legislation and thus legal certainty to the data subject, any subsequent use of data within the scope of the LED should be 'coupled with the "compatible use" building block of the purpose limitation principle in Article 4(1) (b)' (De Hert, Sajfert 2021, 12), and allowed only for specified, explicit and legitimate purposes, which is also important for determination of the strict necessity requirement.[59]

3.2. Implementation

Serbia is required by the SAA not only to harmonise its national law with the LED, but also to ensure *effective* implementation of LED-inspired rules (Art. 72 and 81). Achieving this requires the existence of a consistent and harmonised appropriate legal framework. Nonetheless, taking into account the previously presented issues, the enforcement of LED-inspired rules is difficult if not impossible. Therefore, it is necessary to thoroughly review the LED provisions, especially the preamble, but also to take into account the relevant decisions of the CJEU, and to rearrange the relevant LPPD principles and rules accordingly. In addition, the proclamation of the LED-based principles in this law is not enough, since the lack of their acknowledgment in other laws regulating data processing for special purposes leads to the lessening of personal data protection. Such a result is contrary to the LED purpose of providing the *minimum safeguards*, whereby the states are not precluded to seek to ensure a higher level of 'the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities' (Preamble 15). In addition, there is the issue of non-compliance of special laws with this umbrella law. Still, the LPDP should apply to data processing for special purposes even when sectoral laws fail to regulate certain issues or refer to the basic law, and the role of the competent supervisory body is particularly important.

The LED requires states to provide for one or more independent public authorities to be responsible for monitoring its application, while the SAA requires Serbia to *form such a supervisory body* to *effectively supervise and guarantee the implementation* of national legislation on the protection of personal data (Art. 81). Hence a specialised ombudsman was established: the Commissioner for Information of Public Importance and Protection of Personal Data. As for independence and the rules on the establishment

[59] CJEU, case C-205/21, Ministerstvo na vatreshnite raboti, ECLI:EU:C:2023:49, paras. 121–122.

and general conditions for the members of the supervisory authority, the LPDP consistently followed the rules from the LED. Under the LPDP, the Commissioner is responsible for both data processing regimes. As the LED allows states to provide for a supervisory authority established under the GDPR to also supervise this regime, the domestic solution is not disputable, in principle. However, it is questionable whether the Commissioner has at their disposal sufficient organisational, personnel, technical and material conditions and capacities for effective monitoring of the enforcement of the rules not only for these two regimes, but also regarding access to information of public importance.[60]

The LPDP provides the Commissioner with a whole series of *investigative, corrective and other powers*,[61] by consistently following the LED wording, nonetheless it is not clear enough to which extent these powers are used with regard to data processing for special purposes. The publicly available annual and monthly Commissioner's reports jointly represent data on both regimes,[62] probably due to a lack of a reporting mechanism, since the Commissioner's rules do not specify the manner of keeping internal records that would enable a clear distinction between regimes.[63] Although precise data on the data processing for special purposes were requested in a questionnaire sent to the Commissioner (for the 2018–2025 period), the answers do not say much either; moreover, they point to sporadic cases in which the powers related to the special processing regime have been used.

The response to the questionnaire states that the Commissioner has carried out 18 extraordinary inspections, applying all the prescribed powers (except for one power that does not apply to the special regime), whereupon all inspection procedures were carried out at the request of citizens, not *ex*

[60] Law on Free Access to Information of Public Importance*, Official Gazette of the RS* 120/2004, 54/2007, 104/2009, 36/2010, and 105/2021.

[61] In the performance of inspection supervision, the Commissioner might also use the investigative powers from the Law on Inspection Supervision, *Official Gazette of the RS* 36/2015, 44/2018 – other law and 95/2018.

[62] For example, during 2021, the Commissioner initiated 362 supervision proceedings, of which 9 (2.49%) were against judicial authorities and institutions in the field of justice. More precise data on the structure of operators and reasons for the initiation of supervision proceedings does not exist. In the cases in which he determined that the provisions of the LPDP were violated (72), the Commissioner passed 63 corrective measures (Poverenik 2022, 96–97), but there is no clear, publicly available statistical data on the outcome of the supervision. The same remarks on presented data apply to the last reported year (Poverenik 2026, 121–122).

[63] Rulebook on the form and manner of keeping internal records of violations of the Personal Data Protection Act and measures taken in the course of inspection supervision, *Official Gazette of the RS* 40/2019.

officio. However, it is unlikely that the Commissioner was granted access to all data and information by the police, as well as access to all premises, means and equipment, as stated.

Of all the corrective powers, only one was applied: the Commissioner warned the competent authorities by delivering a written opinion that the intended processing operations may violate the LPDP provisions (four times during the reporting period). The Commissioner did not issue any fines regarding data processing for special purposes. Also, although the Commissioner also has the power to bring infringements of the LPDP to the attention of judicial authorities and to commence or otherwise engage in legal proceedings, to date the Commissioner has not submitted any requests for initiation of misdemeanour proceedings for violations of the LPDP, nor criminal complaints. This is unfortunate, because sanctioning public authorities would, at least to some extent, prevent illegal processing and could be an indicator of the genuine readiness of the Commissioner to protect human rights regarding the processing of data for special purposes, as well as a sign of independence.

The Commissioner also has advisory powers in the legislative process (Art. 55 para. 11 LPDP), but since the LPDP entered into force, only a few opinions on regulatory proposals connected to data processing for special purposes have been submitted, at the request of the authorities.[64] Nonetheless, the Commissioner could show more agility in this regard: although the failure to comply with this obligation is not a basis for misdemeanour liability (it is not among the violations listed in Art. 95 LPDP), the Commissioner has other powers at their disposal in performing the task of supervising and ensuring the implementation of the LPDP.[65] Furthermore, since there are

[64] According to the Commissioner's response to the questionnaire, since the beginning of the implementation of the LPDP, a total of 5 opinions have been requested: three on the Draft Law on Amendments to the Law on the National DNA Registry, one on the Draft Rulebook on the method of recording in a public place and the method of communicating the intention of such recording, and the Draft Law on Amendments to the Law on Tax Procedure and Tax Administration.

[65] For example, the Commissioner used such a possibility in 2021 when an initiative was sent to the Public Prosecutor's Office to align the provisions of the Rulebook on Administration in Public Prosecutor's Offices with the provisions of the LPDP regarding the notification of persons for the protection of personal data.

legal provisions that regulate data processing for special purposes, whose compliance with the Constitution could and should be reviewed, some initiative on the part of the Commissioner would be more than welcome.[66]

Acting on express normative powers from the LPDP provisions, the Commissioner has passed several by-laws,[67] which regulate the manner of exercising certain elements of the right to personal data protection (e.g. the right to object), specifying certain obligations of the controller (e.g. the obligation to notify about personal data breaches), but these by-law do not contain any specific rules with regard to data processing for special purposes. However, recognition and insistence on the specificities of the data processing special regime would be a more appropriate manner to norm these issues within the Commissioner's normative power, thus contributing to the protection of the right to personal data protection, in accordance with the ECtHR standard and the LED principle requiring clarity and precision of the law.

Considering the above, the question remaining is to what extent the actions of the Commissioner, as the guardian of the right to the protection of personal data, are truly beneficial to the enforcement of the LED principles and rules, and consequently this right with regard to personal data processing by the police.

3.3. Strategy?

The full and consistent compliance of sectoral laws with the basic one is an essential prerequisite for effective data protection, but ostensibly a *systematic legislative approach* has been lacking. Although a strategy was passed in 2010,[68] the action plan for its implementation was never adopted, nor was a special working group formed, which resulted in this planning

[66] What is commendable, for example, is that in 2018 the Commissioner submitted a proposal for the assessment of the constitutionality of the Law on the DNA Registry (Ružić, Toskić Cvetinović 2020, 34–35).

[67] Based on Art. 52 para. 9 LPDP, the Commissioner adopted the Rulebook on the form of notification of a personal data breach and the method of notifying the Commissioner for Information of Public Importance and Personal Data Protection of a personal data breach (*Official Gazette of the RS* 40/2019); based on Art. 78 para. 4 LPDP, Rulebook on the form and method of keeping internal records of violations of the Law on Personal Data Protection and measures taken during inspection supervision (*Official Gazette of the RS* 40/2019); and based on Art. 78 para. 5 LPDP, Rulebook on the complaint form (*Official Gazette of the RS* 40/2019).

[68] Personal Data Protection Strategy, *Official Gazette of the RS* 58/2010.

document's failure to produce the expected effects. The new Strategy,[69] adopted in 2023, can be commended, since it stresses the *necessity of improving the LPDP*. The improvement of the mechanisms for the protection of personal data is set as the first specific objective of the *measure* for improving the legal framework, through amending and supplementing the LPDP, in order to harmonise it with EU rules, and then harmonising sectoral laws with the amended LPDP. However, while the objective and measure are reasonable and necessary, the Strategy does not specify the direction of the improvement,[70] while the set timeframe is somewhat unrealistic.[71] As for the LED, it receives only rudimentary mention, but neither the shortcomings in the current normative framework nor the directions for improvement are identified/defined. Still, in order to assess the fulfilment of the LED harmonisation obligation (Art. 81 SAA), it is necessary to consider not only the LPDP, but also other laws governing the processing of personal data by the police.

The new Strategy sets respect for the right to the protection of personal data in all areas of life as its general objective, whereas the achievement of this goal is to be measured through the European Commission *adequacy decision*, by which the transfer of personal data from EU countries to Serbia

[69] Personal Data Protection Strategy for the period from 2023 to 2030, *Official Gazette of the RS* 72/2023; Action plan for the period from 2025 to 2027 for the implementation of the Personal Data Protection Strategy for the period from 2023 to 2030, *Official Gazette of the RS* 20/2025.

[70] The Strategy only mentions the regulation of the relationship between digitalisation and technological progress with the protection of personal data, with regard to automated processing of genetic and biometric personal data and the processing of personal data using audio and video surveillance (as a measure for achieving the third specific objective). However, these issues are already regulated in the LPDP.

Some of directions are set out, as to the expected effects, in the Starting basis for the preparation of the Draft Law on the Protection of Personal Data, published by the Ministry of Justice in 2025.

[71] As for sectoral laws, starting from 40% compliance with the LPPD, as the initial value, *the plan* is to reach 60% compliance with the 'improved' LDPD by 2027, and complete harmonisation by 2030. The plan is for: the draft law on amendments and supplements to the LPDP to be prepared by the 2nd quarter of 2026, followed by the legislative procedure for adopting the law; the identification of relevant provisions of sectoral laws that need to be harmonised with the amended LPDP, will be carried out by the 1st quarter of 2027; and the necessary amendments and supplements to at least 20% of these laws to be adopted by the end of 2027. So far, the working group was formed in December 2024, but the text of the draft law has not been presented to the public as of the publication of this paper.

would be enabled without additional administrative obligations. Still, the Strategy *does not differentiate* the adequacy decision in terms of the GDPR and the LED.

The LED sets rules for international personal data transfers (Chapter V), i.e. for 'any action that enables a law enforcement authority in a third country or a relevant international organization to access personal data that originated in the EU' (Drechsler 2021, 184). These rules 'aim at guaranteeing that the level of protection for personal data in a law enforcement context within the EU is not undermined as soon as personal data leaves EU territory' (Drechsler 2020, 49). Regarding the elements that the Commission would evaluate when deciding whether Serbia, as a third country, ensures *an adequate level of protection*,[72] it is clear that even the formal harmonisation of the LPDP, as a fulfilment of the specific objectives of the Strategy, would not be sufficient for an adequacy decision. The set criteria (the rule of law, human rights, effective data subject rights, and an independent supervisory authority) would be assessed not only based on the domestic legislation, but also based on the domestic practice and domestic international commitments (Drechsler 2021, 187). Therefore, the future amendments to the LPDP and sectoral laws, even if they are fully aligned with EU rules, are only an initial prerequisite. It crucial that the relevant provisions are actually implemented in practice, because that is the only way the effective and substantive exercise of the right to personal data protection can be ensured. Furthermore, it is not enough just to establish a Commissioner and to have their powers prescribed in law – it is necessary that they act as a truly independent body in relation to the competent authorities that process personal data for LEA purposes, and ensure and enforce compliance with LED-inspired rules, by applying the prescribed powers to the special regime, too.

After assessing the adequacy of the level of protection, the Commission may at some point decide that Serbia ensures an adequate level of protection. The implementing act may also provide a mechanism for periodic review, at least every four years (Art. 61 (3) LED), whereby the Commission may

[72] During the decision-making process, the Commission takes into account several elements, inter alia: a) the rule of law, respect for human rights and fundamental freedoms, b) relevant legislation, both general and sectoral (including concerning public security, defence, national security and criminal law, and the access of public authorities to personal data) and its implementation, c) data protection rules, case law, effective and enforceable data subject rights, and effective administrative and judicial redress for the data subjects whose personal data are transferred, d) the existence and effective functioning of one or more independent supervisory authorities with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, etc. (Art. 61 (1) and (2)).

monitor developments in Serbia that could affect the functioning of the adequacy decision. In the case that information or a review indicate that the country no longer ensures an adequate level of protection, the adequacy decision may be repealed, amended or suspended (Art. 61 (5) LED). It follows that even after the decision is made, Serbia would be required to continuously ensure an appropriate level of protection.

4. CONCLUSION

The right to the protection of personal data is explicitly guaranteed in the Constitution of the Republic of Serbia, as well as in ratified international conventions that are a part of the domestic legal order. The data protection principles and rules should be a binding framework for the processing of personal data – including when carried out by competent authorities for special purposes – representing a very important segment in the functioning of state mechanisms.

The present incompatibility of sectoral laws with LPDP rules violates the unity of the legal order and complicates their enforcement, rendering the principle of the legality of data processing for special purposes empty wording. Based on the above ECtHR case law, it is clear that the state should ensure that the law regulating data processing by the police meets the requirements of legality, which is a prerequisite for considering whether the data processing is legitimate and justified. In addition, given its status of a candidate for EU membership, Serbia has a formal obligation to harmonise its legislation with the EU acquis and other European rules, ECHR, inter alia. This obligation also includes ensuring the protection of individuals with regard to the processing of personal data by the police.

Although Serbia adopted the LPDP in 2018 as a manner of transposing the LED into national legislation, harmonisation and implementation have not been ensured. The national legislation should provide the proper basis for data processing and comply with the requirements of Article 8 LED; however, merely repeating its wording may not be considered a sufficient legal basis. The principle of lawfulness should be achieved not only through the LPDP, but also through adequate norms in other sectoral laws. This has not been accomplished so far. Furthermore, the LPDP has provided the Commissioner with investigative, corrective and other powers, closely following the wording of the LED. However, these powers have not been used in many cases of data processing for LEA purposes. In this regard, the Commissioner should act upon these powers, because, as an independent

body, their active and effective role is of the utmost importance in ensuring that the data protection rules are implemented in practice when personal data is processed by the police.

Since the current legal framework for data processing for LEA purposes is neither consistent nor harmonised, both internally and externally, overcoming these issues is quite justified and necessary and even clearly articulated as a goal of the new 2023 Personal Data Protection Strategy. However, the previous experiences regarding the application of laws, existing mechanisms for the protection of personal data, and even the text of the Strategy and the accompanying first action plan, do not provide grounds for such expectations.

There is still room and time to integrate improvements into the LPDP and then ensure the harmonisation of sectoral laws governing data processing for special purposes with that version. Some of the observations presented in this paper could also serve as a guideline for of harmonising the domestic legal framework with the ECtHR requirements and the LED provisions, which is, after all, the formal legal obligation of the Republic of Serbia. However, the planned improvement of the LPDP by itself will not suffice, because unless the rules are implemented, the mere guarantee of the right to protection of personal data does not mean much – if anything at all.

REFERENCES

[1] Aidinlis, Stergios, David Barnard-Wills, Leanne Cochrane, Krzysztof Garstka, Agata Gurzawska, Joshua Hughes. 3/2024. Between GDPR and Law Enforcement Directive in Security Research: The Use of Personal Data by Law Enforcement Authorities. *European Journal of Law and Technology* 15: 1–25.

[2] Bonetto, Giacomo. 1/2024. The judgment of the CJEU in *Inspektor (Purposes of the processing of personal data – criminal investigations)* of 8 December 2022 and the concept of further processing under the Law Enforcement Directive. *New Journal of European Criminal Law* 15: 58–71.

[3] De Hert, Paul, Juraj Sajfert. 31/2021. The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680. *Brussels Privacy Hub Working paper* 7: 1–17.

[4] Dimitrova, Diana, Paul de Hert. 1/2025. Real Transparency and Real Oversight of Law Enforcement Data. The ECHR and the Lack of Accountability of Indirect Access Procedures. *Utrecht Law Review* 21: 49–69.

[5] Directorate General Human Rights and Rule of Law. 2022. Case law of the European Court of Human Rights concerning the protection of personal data, T-PD(2023)1. *https://rm.coe.int/caselaw-march-24-april/1680ab0b7*e, last visited February 15, 2026.

[6] Đorđević, Đurđica. 2/2025. Legal framework, criminal and misdemeanor protection of the right to personal data protection in the Republic of Serbia. *Facta Universitatis: Law and Politics* 23: 155–169.

[7] Drechsler, Laura. 2020. The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive. 47–65 in *Cybercrime: New Threats, New Responses,* Proceedings of the XVth International Conference on Internet, Law & Politics, edited by Joan Balcells *et al*. Barcelona: Huygens Editorial.

[8] Drechsler, Laura. 2/2021. Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context. *International Data Privacy Law* 11: 182–195.

[9] European Commission. 2022. Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final.

[10] European Court of Human Rights. 2018. Guide on Article 8 of the European Convention on Human Rights. *https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb*, last visited February 15, 2026.

[11] Funta, Rastislav, Peter Ondria. 2/2021. Data Protection in Law Enforcement and Judicial Cooperation in Criminal Matters. *TalTech Journal of European Studies* 11: 148–166.

[12] Hudobnik, Matthias. 3/2020. Data protection and the law enforcement directive: a procrustean bed across Europe? *ERA Forum* 21: 485–500.

[13] Leiser, Mark R., Bart Custers. 3/2019. The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680. *European Data Protection Law Review* 5: 367–378.

[14] Leiser, M.R., Bart Custers. 2024. Article 5: Time limit for storage and review. 153–163 in *The EU Law Enforcement Directive (LED): A Commentary*, edited by Eleni Kosta, Franziska Boehm. Oxford: Oxford University Press.

[15] Milidragović, Dragan, Nenad Milić. 98/2023. Normiranje novih policijskih ovlašćenja u Zakonu o policiji. *Zbornik radova Pravnog fakulteta u Nišu* 62: 135–153.

[16] Ministry of Justice of the Republic of Serbia. 2025. Starting basis for the preparation of the draft Law on the protection of personal data. *https://ekonsultacije.gov.rs/topicOfDiscussionPage/446/3*, last visited March 26, 2026.

[17] Petrović, Dragana. 4/2022. Privatnost i zaštita podataka o ličnosti – krivično-pravni aspekt. *Strani pravni život* 66: 469–489.

[18] Petrović, Zlatko 1/2024. Video-nadzor i zaštita podataka o ličnosti u Republici Srbiji. *Savremene studije bezbednosti* 57–82.

[19] Pisarić, Milana, Ostoja Kalaba. 1/2025. Data Retention and Criminal Procedure in Serbia. *Annals of the Faculty of Law in Belgrade* 73: 83–121.

[20] Prica, Miloš. 78/2018. Jedinstvo pravnog poretka kao ustavno načelo i zakonsko uređivanje oblasti pravnog poretka – ujedno izlaganje o unutrašnjem pravnom sistemu. *Zbornik radova Pravnog fakulteta u Nišu* 58: 103–125.

[21] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. 2022. Izveštaj o radu za 2021. godinu. *https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2021/Izve%C5%A1taj_LATfinal.pdf*, last visited February 15, 2026.

[22] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. 2026. Izveštaj o radu za 2025. godinu. *https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2024/godisnji_izvestaj_2025.pdf*, last visited March 26, 2026.

[23] Ružić, Nevena, Ana Toskić Cvetinović. 2020. *Analiza propisa koji uređuju sektor bezbednosti iz aspekta zaštite podataka o ličnosti*. Belgrade: OSCE Mission to Serbia. *https://serbia.osce.org/sr/node/473001*, last visited May 29, 2026.

[24] Simović, Darko, Slobodan Orlović. 2023. *Komentar Ustava Republike Srbije sa praksom Ustavnog suda Republike Srbije i Evropskog suda za ljudska prava*. Belgrade: Službeni glasnik.

[25] Sekulić, Miloš, Gordan Grujić. 3/2020. Krivičnopravna zaštita ličnih podataka. *Glasnik Advokatske komore Vojvodine* 92: 347–378.

[26] Sunde, Inger Marie. 4/2023. To have or have not: Limiting the data available for subsequent use by the police. *New Journal of European Criminal Law* 14: 495–511.

[27] Te Molder, Ruben, Masha Fedorova, Marieke Dubelaar, Sjarai Lestrade. 4/2023. The principle of purpose limitation in data-driven policing: A guiding light or an empty shell? *New Journal of European Criminal Law* 14: 512–533.

[28] Vogiatzoglou, Plixavra, Thomas Marquenie. 2022. Assessment of the implementation of the Law Enforcement Directive. Luxembourg: Publication Office of the EU. *https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf*, last visited May 29, 2026.

Article history:
Received: 28. 3. 2026.
Accepted: 27. 5. 2026.