LAW ON PERSONAL DATA PROTECTION

1.22

WHITE BOOK BALANCE SCORE CARD

Recommendations:	Introduced in the WB:	Significant progress	Certain progress	No progress
Provide the Commissioner with improved working conditions, equipment, and staff to ensure the effective implementation of the DP Act.	2009			√
Harmonise the provisions of other laws related to the processing of personal data with the DP Act.	2022			√
Regulate special types of personal data processing, such as video surveillance, processing employees' personal data, and processing for scientific and historical research and statistical purposes.	2019			√
Amend the DP Act to create conditions for easier transfer of personal data outside of Serbia.	2022			√
Intensify the activities of the Commissioner in issuing guidelines to facilitate the implementation and interpretation of the DP Act, specifically guidelines on the implementation of appropriate data protection measures, and the obligation of the controller to inform individuals about data breaches.	2020		√	
Prescribe conditions for issuing permits to certification bodies.	2020			√
Prescribe the competencies and procedures for accrediting legal entities to conduct compliance control of codes of conduct.	2021			√
Update the 2019 Decision on the List of Countries, Territories, or Sectors of Activities and International Organizations Where an Adequate Level of Data Protection is Considered to be Ensured, in accordance with the European Commission's Adequacy decision for the EU-US Data Privacy Framework.	2020			√
Adopt an action plan for the implementation of the Strategy for Personal Data Protection for the Period 2023–2030 and establish a working group to oversee the implementation of the Strategy and action plan.	2023		√	

CURRENT SITUATION

The Personal Data Protection Act ("Official Gazette of the Republic of Serbia" no. 87/2018) (hereinafter: DP Act) has been in effect since 21 August 2019. The DP Act is, to a considerable extent, a translation of the EU General Data Protection Regulation 2016/679 (GDPR), excluding its recitals and with certain specificities reflecting the characteristics of the legal system of the Republic of Serbia.

The DP Act is based on seven data processing principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability of the controller for data processing. In order for processing to be lawful, it must be based on one of the six legal bases for processing: consent; contract; legal obligation; vital interests; public interest; or legitimate interests. The DP Act imposes stricter conditions for the lawful processing of special categories of data, which include, for example, health data. The DP Act grants data subjects broad rights. Data subjects have, inter alia, the right of access to data, the right to rectification, the right to have incomplete personal data completed, the right to erasure, restriction, and data portability, the right to object, and the right to withdraw consent.

The DP Act imposes a number of obligations on controllers and/or processors. Controllers and processors must implement appropriate technical, organisational, and personnel measures to ensure a level of security appropriate to the risk to the rights and freedoms of individuals. Controllers are required to report data breaches to the supervisory authority, and in certain cases, to inform the data subjects. The DP Act allows for the free transfer of data outside of Serbia to countries that are members of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and to countries for which the European Union has determined

provide an adequate level of protection (by adopting an "adequacy decision"). The transfer of data to other countries is permitted on the condition that the data exporter implements one of the prescribed safeguards (for example, the conclusion of standard contractual clauses, prepared by the Commissioner, with the data importer), or if one of the specific situations set out in the DP Act applies (for example, transfer based on the explicit and informed consent of the data subject).

Controllers and/or processors have a number of additional obligations under the DP Act, such as: appointing a data protection officer; keeping records of processing activities; contractually regulating relationships with processors and joint controllers; conducting data protection impact assessments if it is likely that a certain type of processing will result in a high risk to the rights and freedoms of individuals, and more.

The DP Act has extraterritorial application. The DP Act applies to controllers and processors in Serbia, and, under certain conditions, to those outside of Serbia as well, if they process data about individuals who have residence or domicile in Serbia.

Compared to the GDPR, the fines prescribed for violations of the DP Act are low. While the GDPR allows for fines of up to 20,000,000 euros, or in the case of a legal entity, up to 4% of the total worldwide annual turnover of the preceding financial year (whichever amount is higher), the fines under the DP Act range up to a maximum of 2,000,000 dinars, i.e. approximately 17,000 euros. In this regard, it is proposed to adopt the recommendations contained in the adopted Strategy for the Protection of Personal Data for the Period 2023-2030, which the Government of the Republic of Serbia approved in August 2023. Among other measures, the strategy calls for an increase in penalties in line with the GDPR; and these recommendations have also been corroborated by various legal analyses.

POSITIVE DEVELOPMENTS

The Commissioner has continued to actively participate in expert meetings related to the enforcement of the DP Act and make public appearances to highlight the importance of data protection. The Commissioner has published its tenth publication "Protection of Personal Data: Opinions and Stances of the Commissioner" includes examples from the Commissioner's practice. The Commissioner has published a "Brief Guide to Free Access to Information and Personal Data Protection" in collabouration with the OSCE Mission in Serbia, aimed at better understanding the key concepts and rights of citizens. Additionally, on the Commissioner's website, manuals, opinions, and positions are available to help clarify the unclear areas of the Law. It is noteworthy that the Commissioner, after opening an office outside the Commissioner's headquarters in Novi Sad in 2022, opened another office in Niš, and invested in administrative equipment for the Commissioner's work. In December 2024, the third office in Kragujevac began with it's operations.

The Commissioner is involved in the implementation of a short study program "Training of Managers for Personal Data Protection" conducted by the Faculty of Security studies at the University of Belgrade, as well as the short program "Legal Protection of Data and Access to Information" conducted by the Faculty of Law at the University of Kragujevac. Furthermore, members of the Commissioner's office participate in training sessions for individuals involved in personal data protection organised by the Serbian Chamber of Commerce. Finally, in the 2024/2025 academic year, the Faculty of Law at the University of Belgrade implemented for the first time a new programme, "Studies for Innovation of Knowledge – Data Protection Law". Members of the Commissioner's office have participated in the implementation of specialist studies. The implementation of the study programmes contributes to the education and training of individuals for personal data protection within the higher education system of the Republic of Serbia. Since the second quarter of 2024, accredited lecturers from the Commissioner's Office have started conducting training sessions for three target groups – the healthcare sector, higher education institutions, and internal affairs sector.

The most significant development is the adoption of the Action Plan for the Period 2025–2027 for the Implementation of the Strategy for Personal Data Protection for the Period 2023–2030 in which the Government of the Republic of Serbia has outlined objectives and measures to align the legal framework of the Republic of Serbia with the rules and standards of the European Union. The Action Plan stipulates that the implementation of the Strategy will be regulated through two action plans, each with a duration of three years, whereby the first will cover the period from 2025 to 2027, and the second will cover the period from 2028 to 2030.

The Action Plan envisages, among other things, concrete steps for the adoption of amendments to the DP Act, har-

monisation of other laws with the DP Act, development of the Commissioner's digital platform for online submission of complaints, improvement of the institutional framework, professional training of employees in public administration, and education of judges and holders of public prosecutorial functions.

The Commissioner regularly submits reports to the National Assembly, and on 24 March 2025, submitted the Report on the Implementation of the Free Access to Information of Public Importance Act and the Data Protection Act in 2024 to the National Assembly of the Republic of Serbia. This actively utilizes the institutional process for monitoring the situation and reporting systemic issues.

REMAINING ISSUES

The capacities of the Commissioner's office have not seen significant development. Staffing and financial conditions remain at a similar level to previous years.

The relevant ministries have not yet taken steps to align the provisions of sectoral laws with the DP Act, despite the DP Act stipulating that the provisions of other laws relating to the processing of personal data must be harmonised with the DP Act by the end of 2020.

Certain specific types of personal data processing, such as video surveillance, processing of employees' personal data, and processing for the purpose of scientific and historical research and statistical purposes, are not systematically regulated.

The DP Act needs to be amended to create conditions for easier transfer of personal data outside of Serbia. Firstly, the Commissioner's authority to adopt standard contractual clauses needs to be expanded. In comparison to the EU, where standard contractual clauses for four different transfer models exist, the standard contractual clauses for the transfer of data from Serbia only apply to the transfer of data from a controller to a processor. Standard contractual clauses for other transfer models (such as from controller to controller) do not exist because the DP Act does not empower the Commissioner to adopt them. Recognising EU standard contractual clauses and binding corporate rules approved by the relevant EU bodies as adequate mechanisms for data transfer in the DP Act, in addition to the domestic ones, would further facilitate data transfer.

The Commissioner should intensify activities in issuing guidelines that will help with the implementation and interpretation of the DP Act. For instance, guidelines for implementing appropriate technical, personnel, and organisational measures to protect personal data, as well as guidelines on the controller's obligation to inform data subjects about a data breach that may pose a high risk to individuals' rights and freedoms, would be particularly beneficial for controllers and processors.

The Commissioner has not used its power to set conditions for issuing permits to certification bodies, which, according to the DP Act, would be authorised to issue certificates to controllers and processors as proof of compliance with the DP Act. In addition, neither the DP Act nor any other regulation establishes the competencies and procedures for accrediting legal entities to conduct compliance control of codes of conduct.

The Council expects the Government of the Republic of Serbia to state its position on the impact of the European Commission's Adequacy decision for the EU-US Data Privacy Framework of 10 July 2023 on companies operating in Serbia and to update the 2019 Decision on the List of Countries, Territories, or Sectors of Activities and International Organizations Where an Adequate Level of Data Protection is Considered to be Ensured.

The role of the data protection officer (DPO) in Serbia is still not sufficiently affirmed. Although the DP Act foresees this function, many organisations formally appoint a DPO without ensuring real autonomy or resources. The Commissioner should develop a programme for periodic trainings and certifications of data protection officers.

FIC RECOMMENDATIONS

- Provide the Commissioner with improved working conditions, equipment, and staff to ensure the effective implementation of the DP Act.

- Harmonise the provisions of other laws related to the processing of personal data with the DP Act.
- Regulate special types of personal data processing, such as video surveillance, processing employees' personal data, and processing for scientific and historical research and statistical purposes.
- Amend the DP Act to create conditions for easier transfer of personal data outside of Serbia.
- Intensify the activities of the Commissioner in issuing guidelines to facilitate the implementation and interpretation of the DP Act, specifically guidelines on the implementation of appropriate data protection measures, and the obligation of the controller to inform individuals about data breaches.
- Prescribe conditions for issuing permits to certification bodies.
- Prescribe the competencies and procedures for accrediting legal entities to conduct compliance control of codes of conduct.
- Update the 2019 Decision on the List of Countries, Territories, or Sectors of Activities and International Organizations Where an Adequate Level of Data Protection is Considered to be Ensured, in accordance with the European Commission's Adequacy decision for the EU-US Data Privacy Framework.
- Develop a national register of personal data breaches, accessible to the Commissioner and relevant authorities, to ensure transparency and analysis of security incident trends.
- Introduce mandatory training for all employees processing personal data in the public sector (mandatory modules within public administration).
- Create institutional conditions to better integrate data protection into sectoral laws (healthcare, telecommunications, communications, security).
- Encourage the certification of organizations based on international data protection standards (ISO 27001/27701) through tax incentives or public subsidies. The introduction of certification and accreditation mechanisms could facilitate demonstrating compliance and increase trust among citizens and EU partners.
- Develop the Commissioner's digital platform for e-reporting of violations, requests, and complaints – to enable faster communication between citizens and the supervisory authority.
- The Commissioner should develop a programme for trainings and certification of data protection officers.