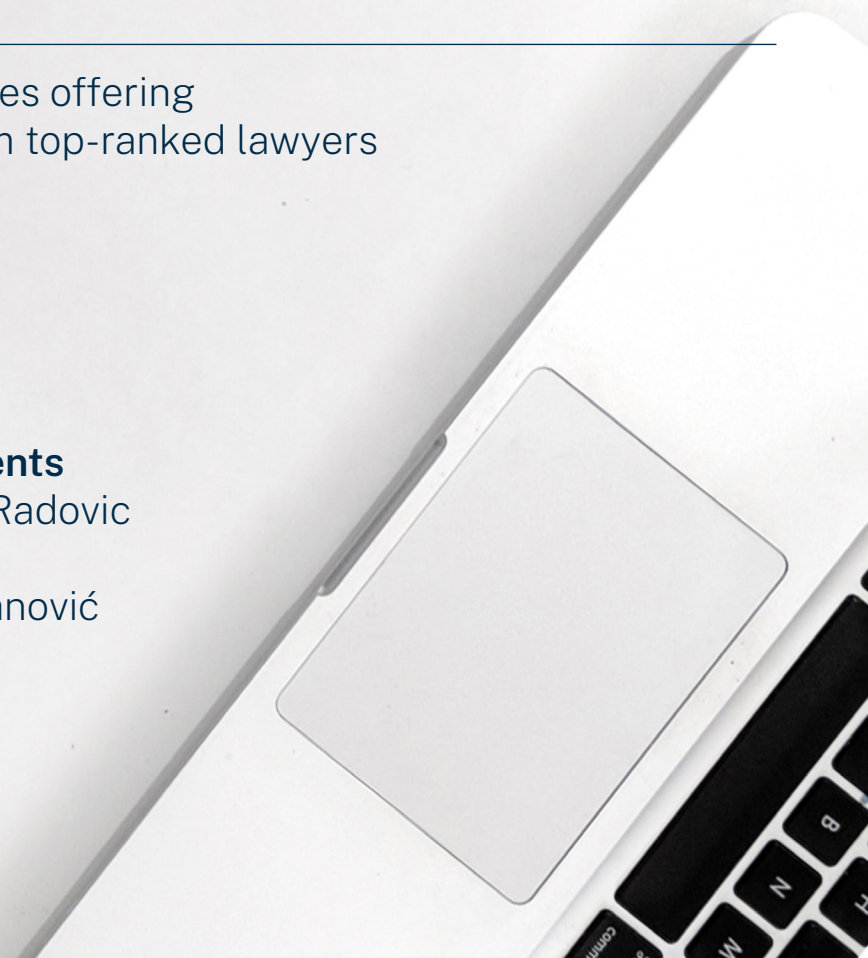
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers



Serbia: Law & Practice and Trends & Developments

Vladimir Djeric, Katarina Radovic and Lena Petrovic
Mikijelj, Janković & Bogdanović

SERBIA

Law and Practice

Contributed by:
Vladimir Djeric, Katarina Radovic and Lena Petrovic
Mikijelj, Janković & Bogdanović

Contents

Mikijelj, Janković & Bogdanović was established in 1985 in Belgrade, Serbia, and has been continuously recognised as one of the leading law firms in the field of dispute resolution and IP law. The firm's data protection team comprises three members, two partners and one senior associate. The team has advised clients in matters of data protection and privacy, particularly in telecommunications, pharmaceuticals, online trade, advertising, gambling and media. Mikijelj, Janković & Bogdanović also has an extensive practice in the areas of advertising, media, employment, and corporate and commercial law.

Authors

Vladimir Djeric is a partner at Mikijelj, Janković & Bogdanović. He advises clients on data protection, dispute resolution, advertising law and media law.

Lena Petrovic is a senior associate at Mikijelj, Janković & Bogdanović. Lena practices in the areas of data protection, advertising law, dispute resolution and intellectual property.

Katarina Radovic is a partner at Mikijelj, Janković & Bogdanović. She specialises in matters relating to employment law, data protection, dispute resolution and intellectual property.

Mikijelj, Janković & Bogdanović

Vlajkoviceva 28
Belgrade
Serbia

Tel: +381 113 231 970
Fax: +381 113 245 065
Email: office@mjb.rs
Web: www.mjb.rs

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Constitution of the Republic of Serbia contains several provisions relating to the protection of privacy, including the confidentiality of letters and other means of communication (Article 41 of the Constitution) and the protection of personal data (Article 42 of the Constitution).

Under the Constitution, the confidentiality of letters and other means of communication may only be derogated from for a specified period of time and on the basis of a court decision for the purpose of conducting criminal proceedings or protecting the safety of Serbia, in a manner stipulated by the law (Article 41 of the Constitution).

The Constitutional guarantee of protection of personal data (Article 42 of the Constitution) provides that use of personal data for any purpose other than that for which it was collected is prohibited and punishable in accordance with the law, unless it is necessary to conduct criminal proceedings or protect the safety of Serbia, in a manner stipulated by the law.

The Constitution also guarantees that everyone shall have the right to be informed of the collection of personal data relating to them, in accordance with the law, as well as the right to court protection in the case of abuse of their personal data.

The Personal Data Protection Act

In August 2019, application of the new Personal Data Protection Act (PDPA) came into effect. The solutions provided by the PDPA are in line with the GDPR. The PDPA defines personal data, the different types of personal data and the manner of their collection, processing and transfer outside of the territory of Serbia. In Avgust 2023 Serbia adopted the Personal Data Protection Strategy for the period from 2023 to 2030. The main goal of this Strategy is "[r]especting the right to protection of personal data in all areas of life".

Provisions that are of relevance to the protection of personal data may also be found in the Electronic Communications Act (ECA), as well as in sector-specific legislation, such as the Act on Health Documents and Records, the Act on Records and Data Processing in Interior Affairs, the National DNA Registry Act and the Law on Social Card.

Also, the provisions of the Information Security Act (ISA) regarding data breach reporting and notification are relevant to the protection of personal data and privacy. The ISA regulates (i) measures for protection against security risks in ICT systems, (ii) the liability of legal entities in relation to management, and (iii) the use of ICT systems and competent authorities in charge of the implementation of protective measures (Article 1 of the ISA).

Thus, the operators of the ICT systems for essential services are obliged to notify the Regulatory Authority for Electronic Communications and Postal Services (RATEL), as the national Computer Emergency Response Team (CERT), of incidents and attacks related to the ICT system that may have a significant impact on informational security. An incident has to be reported in writing to the national CERT within one day of its occurrence and, if it relates to the secret data, the operator of the ICT system of special importance is also obliged to follow the rules related to data secrecy (Article 11 of the ISA).

If the reported incident is of a public interest, RATEL may order its public disclosure. If the incident is related to crimes prosecuted ex officio, RATEL shall inform the competent Public Prosecutor's Office and/or the Ministry of the Interior. If the incident involves a violation of personal data, RATEL will report the incident to the Commissioner for Protection of Personal Data (Article 11 of the ISA).

According to the Constitution of Serbia, ratified international treaties and generally accepted rules of international law are part of the legal system of Serbia, and laws and other general acts enacted in Serbia have to comply with ratified international treaties and generally accepted rules of international law (Article 194 of the Constitution).

In the context of personal data protection, Serbia has ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows (ETS No 108, Strasbourg, 28 January 1981) (the "Convention"). The Convention serves as a legal ground for transfer of data from Serbia to the UK after Brexit, since the UK is party to it and signatories of the Convention are considered to be countries that ensure an adequate level of data protection.

Serbia is also a signatory to various international agreements that contain provisions that could be relevant for accessing or obtaining data processed in the territory of Serbia, mostly in the context of international co-operation in civil and criminal matters.

Because Serbia is in the process of accession to the EU, much Serbian legislation focuses on the implementation of the standards and provisions provided by EU legislation.

Moreover, the PDPA contains solutions provided by the GDPR and Directive (EU) 2016/680 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 (the "Police Directive").

1.2 Regulators

Under Serbian legislation, the main regulator in the area of data protection is the Commissioner for Information of Public Importance and Protection of Personal Data ("the Commissioner"), whose prerogatives are defined by the PDPA. Under the PDPA, the Commissioner is a supervisory body that:

- monitors and enforces the application of the PDPA;
- advises the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
- provides information to any data subject concerning the exercise of their rights under the PDPA; and
- co-operates with the supervisory authorities of other states.

The Commissioner also:

- handles complaints lodged by a data subject;
- prepares standard contractual clauses and authorises contractual clauses that would serve as an adequate safeguard for the transfer of data to a country or international

organisation that does not ensure adequate levels of protection of personal data;
- establishes and maintains a list in relation to the requirements for a data protection impact assessment when required by law; and
- accredits certification bodies, issues certifications and approves criteria of certification (Article 78 of the PDPA).

Data Protection Commissioner Powers

The Commissioner is vested with a set of investigative powers, corrective powers and advisory powers that are identical to the powers of the supervisory body prescribed by the GDPR. The Commissioner is authorised, inter alia, to:

- order the data controller or data processor to provide information it requires for the performance of its tasks;
- monitor the application of the provisions of the PDPA by exercising its inspection powers;
- carry out a review on certifications issued in accordance with the PDPA;
- obtain access to any premises of a controller or processor, including to any data-processing equipment and means;
- issue reprimands to a controller or processor where processing operations have infringed provisions of the PDPA;
- order the controller or the processor to comply with the data subject's requests to exercise their rights pursuant to the PDPA;
- order the controller or processor to bring processing operations into compliance with the provisions of the PDPA, where appropriate, in a specified manner and within a specified period;
- order the controller to communicate a personal data breach to the data subject;
- impose a temporary or definitive limitation, including a ban on processing;
- order the rectification or erasure of personal data or restriction of processing;
- withdraw a certification or order the certification body to withdraw an already-issued certification;
- impose an administrative fine – in addition to, or instead of, other corrective measures – depending on the circumstances of each individual case; and
- order the suspension of data flows to a recipient in a third country or to an international organisation (Article 79 of the PDPA).

1.3 Enforcement Proceedings and Fines

Under the PDPA, the Commissioner is authorised to exercise its powers in accordance with the Administrative Procedure Act and Inspection Act (Article 77 of the PDPA) as well as to initiate proceedings before the courts and other competent bodies in accordance with the law (Article 79 of the PDPA).

The Commissioner is obliged to act upon the complaints of a data subject and initiate the inspection procedure, as well as to inform the data subject about the outcome of the inspection and their right to initiate administrative court proceedings against the decision of the Commissioner. If the data subject is not satisfied with the decision of the Commissioner, or if the Commissioner fails to act upon the complaint within 60 days from its receipt, the data subject is authorised to initiate court proceedings against the Commissioner in accordance with the Administrative Court Proceedings Act (Articles 82 and 83 of the PDPA).

The enforcement of personal data protection is the remit of the Commissioner, which is authorised to investigate whether data processing is lawful, including the right to request access to the premises of the data controller and means

of data processing, as well as to order rectification of identified irregularities in data processing within a specified period of time, or to render a temporary ban on any processing carried out contrary to the provisions of the PDPA (Article 79 of the PDPA).

Data processing contrary to the provisions of the PDPA represents a misdemeanour punishable with a fine between RSD50,000 and RSD2 million for a legal entity, RSD20,000 and RSD500,000 for an entrepreneur, and RSD5,000 and RSD150,000 for both a natural person and the responsible person in a legal entity (Article 95 of the PDPA).

1.4 Data Protection Fines in Practice

According to the Commissioner's annual report for 2023 (the report for 2024 is not available at the moment of submission of this article) the Commissioner carried out a total of 731 inspections (549 regular inspections and 182 extraordinary inspections). 689 cases were closed after confirming compliance with previous inspection findings, 24 cases were closed with an official note or response to the complainant, as no violations of the PDPA were found. 18 cases were pursued further as misdemeanours.

Violations Identified

66 cases were found to involve violations of the PDPA, leading to the following enforcement actions:

- ten misdemeanour proceedings were initiated;
- five misdemeanour orders were issued; and
- 51 corrective measures (warnings) were imposed on data controllers.

Initiation of New Supervision Procedures

The Commissioner initiated 771 new supervision procedures:

- 566 regular inspections; and
- 205 extraordinary inspections;
  (a) 138 based on complaints;
  (b) 29 due to data breach notifications; and
  (c) 38 for other reasons.

Court Proceedings Related to Commissioner's Activities

Administrative Court Cases

72 lawsuits were filed against the Commissioner before the Administrative Court.

16 lawsuits were filed by the Ministry of Internal Affairs due to orders to delete personal data from their records.

The Administrative Court resolved 12 lawsuits, rejecting all as unfounded.

The Constitutional Court received 30 constitutional complaints related to the Commissioner's decisions, but due to classification methods, it is unclear how many were about personal data protection.

The Constitutional Court issued 12 rulings, rejecting all complaints.

Misdemeanour responsibility

The Commissioner filed ten misdemeanour requests due to violations of the PDPA, targeting:

- four cases of processing personal data contrary to fundamental principles;
- one case of processing personal data without consent; and

- five cases of failure to appoint a Data Protection Officer (DPO).

These requests were filed against three responsible persons, six legal entities and one entrepreneur.

Since 2010, 238 misdemeanour requests have been filed:

- 216 under the old PDPA, with common violations including failure to update records, unlawful processing and failure to comply with the Commissioner's orders; and
- 24 under the new PDPA, mainly related to unlawful processing and lack of adequate security measures.

In 2023, five misdemeanour orders were issued for:

- three cases of failure to maintain processing records; and
- two cases of failing to publish or submit DPO contact information.

Criminal Complaints and Prosecutor's Actions

Since 2010, the Commissioner has filed 49 criminal complaints, covering offences such as unauthorised wiretapping, unauthorised data collection and abuse of official position.

Only two indictments were filed, leading to:

- one conditional conviction (six months' probation); and
- one acquittal.

23 complaints were dismissed due to:

- 15 cases of prosecution being deferred;
- three cases where the offence was not considered a criminal act; and
- five cases of expired statutes of limitations. In 2023, misdemeanour courts issued five first-instance decisions:
- three convictions with warnings;
- one dismissal due to expired statutes of limitations; and
- one rejection due to the statute of limitations.

SHARE Foundation has reported 76 cases of violations of privacy and data protection, out of which 22 perpetrators are persons from the public sector, 16 natural persons and 16 persons from media outlets. In 42 cases, the violation affected a large number of people, 32 cases relate to individual data subjects and one relates to a political data subject.

Serbia has an active but relatively mild enforcement of data protection laws. While there are administrative and legal actions against violators, the lack of significant fines or major criminal convictions suggests that data protection compliance may not yet be a top enforcement priority. The relatively low penalties (compared to GDPR) may contribute to the limited motivation for full compliance among organisations.

1.5 AI Regulation

AI is still not regulated in Serbian legislation. In 2019, Serbia adopted "Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025." The strategy established "goals and measures for the development of artificial intelligence, the implementation of which should result in economic growth, improvement of public services, improvement of scientific staff and development of skills for the jobs of the future". Also, "implementation of the measures of the Strategy should ensure that artificial intelligence in the Republic of Serbia is

developed and applied in a safe manner and in accordance with internationally recognised ethical principles in order to use the potential of this technology to improve the quality of life of each individual and society as a whole, as well as for achieving the Sustainable Development Goals".

In 2022, Serbia became a member of Global Partnership on Artificial Intelligence and, in 2023, Serbia became a member of the AI Governance Alliance at the AI Governance Summit of the World Economic Forum in San Francisco.

In January 2025, Serbia adopted the new "Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2025-2030". The new Strategy acknowledged that Serbia had adopted UNICEF's Recommendation on the Ethics of Artificial Intelligence and that it had implemented the application of AI in the educational and health sector. The new Strategy advocates support for start-ups and small- and medium-sized enterprises in the AI sector and measures for increasing investment in the development of AI. It also establishes a National Artificial Intelligence Platform, an infrastructure platform which would facilitate innovation. The Strategy also focuses on introducing and implementing AI solutions in the public sector. One of the most important goals prescribed by the Strategy is the creation of a legislative framework for AI. The adoption and full implementation of the AI legislation are planned by the end of 2027.

1.6 Interplay Between AI and Data Protection Regulations

As mentioned in **1.5 AI Regulation**, AI is not regulated in Serbian legislation.

2. Privacy Litigation

2.1 General Overview

Two main pieces of legislation relevant for privacy litigation in Serbia are the PDPA and the Law on Public Information and Media. The PDPA defines data subjects' rights and mechanisms for their protection, with the Commissioner as the main authority for the protection of personal data. As mentioned in **1.4 Data Protection Fines in Practice**, Serbia has a modest number of cases related to the protection of personal data. However, there are numerous defamation cases governed primarily by the provisions of the Law on Public Information and Media.

In recent years, there have been many SLAPPs (strategic lawsuits against public participation) against independent media and investigative journalists, filed by government officials, public servants, politicians, celebrity figures, and business owners whose business activities have been associated with corrupt practices.

Since Serbia is not a member of the EU, EU case law does not directly affect Serbian courts. However, decisions of the ECHR are relevant for domestic court cases and are considered, particularly concerning the interpretation and application of the provisions of the European Convention on Human Rights.

2.2 Recent Case Law

As discussed in **1.4 Data Protection Fines in Practice**, there is not much case law relating to the application of the PDPA. Recent examples of SLAPPs relate to the investigative journalist's portal KRIK (the Crime and Corruption Reporting Network), which has been sued by a judge and her husband for a violation of privacy rights (criminal charges were also brought) by publishing profiles in the "Judge Who Judges"

database, which aims to increase transparency within the judiciary. Monetary compensation was requested in the lawsuit. Similarly, Nenad Milanović, chief of staff to the mayor of Belgrade, filed a lawsuit against the Balkan Investigative Reporting Network (BIRN) Serbia, alleging defamation.

2.3 Collective Redress Mechanisms

Serbian legislation does not support collective redress mechanisms in relation to privacy and data protection. Serbian Consumer Protection Law is a single piece of legislation which provides a collective redress mechanism but only for consumer-related matters. Registered consumer associations and the Ministry of Trade may initiate proceedings for the protection of the consumer's collective interest. However, this possibility is not available for privacy litigations.

Since Serbia is in the process of accession to the EU, it should take into account the EU's Representative Actions Directive (EU) 2020/1828 and introduce collective redress mechanisms into other areas of law apart from the consumer protection law; there is no indication that such legislation will be adopted in the near future.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

IoT is not regulated by Serbian law.

3.2 Interaction of Data Regulation and Data Protection

IoT is not regulated by Serbian law. The processing of personal data is subject to the general rules of the PDPA.

3.3 Rights and Obligations Under Applicable Data Regulation

See **3.1 Objectives and Scope of Data Regulation**.

3.4 Regulators and Enforcement

See **3.1 Objectives and Scope of Data Regulation**.

4. Sectoral Issues

4.1 Use of Cookies

Serbian legislation does not have special rules governing the application of cookies, beacons, the use of tracking technologies or behavioural advertising so the general rules of the PDPA also apply to these topics.

4.2 Personalised Advertising and Other Online Marketing Practices

The PDPA does not contain special provisions regarding online marketing. However, it does regulate processing for direct marketing purposes and entitles the data subject to object at any time to the processing of personal data concerning them for such marketing, which also includes profiling (Article 37 of the PDPA). Regarding other aspects of online marketing, general rules on data processing apply.

The Advertising Act (AA) also contains a provision that allows direct advertising only upon obtaining prior consent from the person to whom the advertising is sent (Articles 62 and 63 of the AA). Behavioural advertising and targeted advertising are not regulated explicitly by Serbian law.

4.3 Employment Privacy Law

Under the PDPA, the processing of employees' personal data is carried out in accordance with the provisions of employment law and collec-

tive agreements based on the principles set out by the PDPA. The PDPA also recognises that employment regulations and collective agreements may contain provisions related to the protection of personal data of employees, in which case they also need to specify suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights (Article 91 of the PDPA).

Under the Employment Act of the Republic of Serbia, employers are allowed to collect data regarding their employees where this is prescribed by that law and other laws related to employment matters. The Employment Act also authorises employers to monitor the work of their employees, a provision that is frequently used in practice as a ground for accessing employees' computers and email communications. In this respect, the Commissioner has taken the position that such access is allowed if the computer and email account were provided by the employer for the purpose of work performance and if it does not invade the employees' privacy. If an employee is using a private email account or private computer, the employer may access the data contained therein only in the presence of that employee, who will then be able to prevent the employer's access to private communication and files. In a recent ruling the Commissioner took the position that an employer must not continue to use its former employee's email account upon termination of employment, as it contains the employee's name: a piece of personal data whose processing is no longer justifiable, legal and necessary.

4.4 Transfer of Personal Data in Asset Deals

In Serbia, the transfer of personal data in asset deals is regulated by the PDPA. When an asset deal involves personal data (eg, customer or employee databases), the transfer must have a valid legal basis under the LPDP:

- legitimate interest (Article 12 of the PDPA);
- consent if the transaction involves sensitive data or when no other legal basis is available (Article 15); and
- legal obligation (Article 17) (eg, employment records).

During the due diligence procedure, the seller should minimise data exposure and use anonymised or pseudonymised data where possible. NDAs must also be signed.

Once the transaction is closed, the buyer becomes a new data controller and must inform data subjects (customers, employees) about the change. If the transfer changes the purpose of data processing, additional consent may be required. If the buyer is outside Serbia, data transfers must comply with PDPA rules on international transfers (transfers to countries without an adequate level of protection require standard contractual clauses (SCCs) or other safeguards). The buyer must provide information on how their data will be used post-transfer.

5. International Considerations

5.1 Restrictions on International Data Transfers

Under the PDPA, international transfers of data to a country, a territory or one or more specified sectors within that country, or an international organisation that ensures an adequate level of protection do not require any prior authorisation (Articles 63 and 64 of the PDPA).

It is assumed that an adequate level of protection exists in:

- countries and international organisations that are parties to the Convention;
- countries and international organisations that are considered by the EU to ensure adequate levels of protection of personal data; and
- countries with which the Republic of Serbia has concluded international treaties regarding the transfer of personal data (Article 64 of the PDPA).

The Serbian government has rendered a decision on the list of countries, parts of their territory or one or more specified sectors within those countries or international organisations which are considered to ensure the adequate level of personal data protection, which specifies the countries to which the transfer of data is free.

Furthermore, under the PDPA, the transfer of personal data is also allowed to a country, a territory of, or one or more specified sectors within, that country, or an international organisation that does not have an adequate level of protection if the controller or processor provides appropriate safeguards, and if enforceable data subject rights and effective legal remedies for data subjects are available in that country, a territory of, or one or more specified sectors within, that country, or the relevant international organisation (Article 65 of the PDPA).

The appropriate safeguards may be provided by a controller without requiring any specific authorisation from the Data Protection Commissioner by:

- a legally binding instrument between public authorities or bodies;
- standard data protection clauses prepared by the Data Protection Commissioner that regulate the legal relationship between the controller and processor;
- binding corporate rules that regulate processing of personal data by a controller and the group of companies to which the controller belongs;
- an approved code of conduct, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certificate issued in accordance with the PDPA, together with binding and enforceable commitments on the part of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

The appropriate safeguards may also be provided through contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation, or through provisions inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights, but only with the specific authorisation of the Commissioner, which is obliged to give such authorisation within 60 days from the day of receipt of the request for authorisation (Article 65 of the PDPA).

Further, under the PDPA, the data controller may introduce binding corporate rules that are adhered to by a controller or processor established in the territory of the Republic of Serbia for the purpose of a transfer, or a set of transfers, of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. If the Data Protection Commissioner approves the binding corporate rules, it is considered that a controller has provided adequate safeguards and that data

may be transferred outside of the territory of the Republic of Serbia (Article 67 of the PDPA).

Nonetheless, each international transfer of data has to be lawful – ie, it must be based on one of the legal grounds prescribed by the law, namely:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- it is necessary for compliance with a legal obligation to which the controller is subject;
- it is necessary in order to protect the vital interests of the data subject or of another natural person;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller; or
- it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by those interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child.

5.2 Government Notifications and Approvals

Under the PDPA, prior approval of the Data Protection Commissioner may be required if data is to be transferred to a country that does not ensure an adequate level of protection (Article 65 of the PDPA). For more details see **5.1 Restrictions on International Data Transfers**.

5.3 Data Localisation Requirements

Under the current Serbian legislation, there is no requirement for data localisation. However, each instance of data processing, including the transfer of data, has to be made on one of the grounds for data processing stipulated by the PDPA and must ensure adequate levels of data protection (Articles 12 and 65 of the PDPA).

5.4 Blocking Statutes

As stated in **5.1 Restrictions on International Data Transfers**, the transfer of personal data to a country that is not a party to the Convention is subject to prior approval of the Commissioner. If that approval is denied, the data cannot be transferred.

As regards requests for transfer of personal data to a foreign country for the purpose of conducting criminal or civil proceedings, all such requests are governed by the rules of the international treaties and bilateral agreements regulating the co-operation of Serbia with foreign countries in criminal and civil law matters.

5.5 Recent Developments

There is no applicable information in this jurisdiction.

Trends and Developments

Contributed by:
Vladimir Djeric, Katarina Radovic and Lena Petrovic
Mikijelj, Janković & Bogdanović

Mikijelj, Janković & Bogdanović was established in 1985 in Belgrade, Serbia, and has been continuously recognised as one of the leading law firms in the field of dispute resolution and IP law. The firm's data protection team comprises three members, two partners and one senior associate. The team has advised clients in matters of data protection and privacy, particularly in telecommunications, pharmaceuticals, online trade, advertising, gambling and media. Mikijelj, Janković & Bogdanović also has an extensive practice in the areas of advertising, media, employment, and corporate and commercial law.

Authors

Vladimir Djeric is a partner at Mikijelj, Janković & Bogdanović. He advises clients on data protection, dispute resolution, advertising law and media law.

Katarina Radovic is a partner at Mikijelj, Janković & Bogdanović. She specialises in matters relating to employment law, data protection, dispute resolution and intellectual property.

Lena Petrovic is a senior associate at Mikijelj, Janković & Bogdanović. Lena practices in the areas of data protection, advertising law, dispute resolution and intellectual property.

Mikijelj, Janković & Bogdanović

Vlajkoviceva 28
Belgrade
Serbia

Tel: +381 113 231 970
Fax: +381 113 245 065
Email: office@mjb.rs
Web: www.mjb.rs

Software for Monitoring the Physical Development and Motor Development of Students

The Ministry of Education of the Republic of Serbia planned to implement software for monitoring the physical development and motor skills of students in primary and secondary schools. It was called project ZDRAVITAS. The idea was to use ZDRAVITAS as a tool for the collection of such data in a digital form. Previously this data was collected by the teachers of physical and health education classes in paper form.

The Ministry of Education announced that the project would start at the beginning of December 2024, however due to the harsh objections from the public and particularly parents, the project was postponed.

Project ZDRAVITAS raised concerns about the security of the collected data and the benefits of the digitalisation of this data. The security measures for the protection of the collected data were questioned, the possibility of data leakage was raised, the necessity of the collection of such data in a digital form was also put before the Ministry of Education. There were rumours that the software would collect the students' health data.

In response to strong public objection to the project, the Commissioner for Information of Public Importance and Personal Data Protection conducted an extraordinary inspection which confirmed that the project was in line with the applicable data protection legislation.

The Commissioner explained that the Ministry of Education established a legal basis for data processing and had implemented measures to protect personal data. The legal basis is the Law on the Fundamentals of the Education and Upbringing System. The type of data that is to be collected is prescribed by this Law ie, name, date of birth and unique identification numbers, as well as physical measurements and performance metrics like height, weight and various fitness test results. Access to the data would be given to parents as registered users of the portal and designated personnel in schools.

Before launching the portal, the Ministry conducted a data protection impact assessment to evaluate the impact of the planned data processing activities on personal data protection. They implemented technical, organisational and personnel measures to ensure an appropriate level of data security relative to the associated risks. Also, the Ministry of Education was cooperating with the Office for IT and eGovernment in order to ensure technical support for the smooth operation of the software. Their cooperation was regulated by the agreement on personal data processing.

The Commissioner's overall conclusion was that features of the ZDRAVITAS project did not represent a threat to the protection of personal data of students who would be involved in it. Nonetheless, the project had to be postponed because of the lack of trust and scepticism of the general public who were very suspicious about the processing and protection of health data.

Spy Software Surveillance

In December 2024, Amnesty International published a report "A Digital Prison: Surveillance and the Suppression of Civil Society in Serbia," stating that the Serbian authorities were using advanced surveillance technologies against political activists, journalists and members of civil society.

According to the report, Serbian police and the Security Information Agency (BIA) were using a domestically developed spyware known as "NoviSpy". The spyware was secretly installed on individuals' devices while they were in detention or being interviewed by the police, in situations when their devices were temporarily seized. The use of spyware is completely illegal and politically driven, as the data extracted in such manner cannot be used in any legal proceedings. The spyware could capture sensitive personal data and remotely activate a device's microphone or camera. Also, the report states that the authorities were using mobile forensic tools from the Israeli company Cellebrite to extract data from mobile devices. Devices would be unlocked by the Cellebrite's tools and spyware would then be installed onto the device.

The report also recalled previous attempts of the Serbian authorities to use surveillance tools that disregarded the limits of legal provisions on the lawfulness of surveillance measures and procedures for their implementation, eg, Pegasus and Predator spyware which had been used in previous years. Surveillance measures are exceptional measures which may be imposed only in accordance with a strictly defined procedure and under strict conditions. They should be narrow and focused on a specific target and not abused for mass unauthorised surveillance.

The Serbian Ministry of Internal Affairs and the Security Information Agency rejected these claims, stating that the forensic tools they deploy are in line with the police practice worldwide and entirely within the legal framework provided by the Serbian legislation.

Political and environmental activists, journalists and members of civil society who experienced unlawful surveillance were seriously concerned about their safety and the confidentiality of their communications. Human rights organisations and civil society groups defined this practice as a serious violation of privacy, freedom of expression and freedom of assembly and requested the authorities to conduct serious investigations and punish those involved in this practice. State authorities did not comment further on this topic.

Violation of Privacy of Political Activists

In 2024, during the student-led anti-corruption protests in Serbia, certain pro-government media outlets published personal data, including passport photographs, of student protesters.

This action represents a pure violation of privacy and personal data protection laws in Serbia.

First, the Constitution of the Republic of Serbia explicitly prohibits the use of personal data beyond the purpose for which it was collected, stating that such misuse is both prohibited and punishable.

Secondly, the Personal Data Protection Act defines personal data as any information relating to an identified or identifiable natural person. It mandates that personal data must be processed lawfully and collected for specified, explicit and legitimate purposes.

Thirdly, the Law on Public Information and Media prohibits the publication of information from an individual's private life or personal records without the consent of the individual concerned (personal documents and images included).

The publication of students' passport photos by media outlets represents unauthorised use of personal data contravening both the Constitution and the Personal Data Protection Act. It is also an invasion of privacy because disclosing

personal documents and images without consent breaches the Law on Public Information and Media, which safeguards individuals' private lives from unwarranted public exposure.

Additionally, these actions also breached journalistic ethical standards. The Code of Journalists Ethics of Serbia emphasises respect for individuals' privacy and mandates that personal data should not be published without consent. It also advises against discrimination based on personal characteristics and insists on the use of honourable means in data collection.

The Commissioner for the Protection of Information of Public Importance, Milan Marinović, announced that measures would be taken to identify the source of the leaked passport data. However, he noted that his office lacks authority over media outlets concerning content published for public information purposes. He suggested that the affected students could request information from the Ministry of Internal Affairs regarding the data leak and, if unsatisfied with the response, file a complaint with the Commissioner's office.

Personal Data Protection Strategy 2023-2030

In August 2023, the government of the Republic of Serbia adopted the Personal Data Protection Strategy for the period from 2023 to 2030. The three specific goals defined in the new Strategy are set out below.

Improvement of functional mechanisms for personal data protection

The fulfilment of this goal, among other things, implies the amendment of the legislative framework, and above all the (long overdue) amendment of the Personal Data Protection Act in order to clarify insufficiently clear provisions and mechanisms that do not exist in the domestic legal system. The Strategy raises the possibility that the Commissioner be vested with competence to impose administrative measures, including penalties, similar to those already available to the Serbian Competition Commission (and already exercised by the data protection authorities in the EU). Further, it is considered that the amounts could be higher than the maximum RSD2 million prescribed at the moment (around EUR17,000) and should go in the direction of the fines prescribed by the GDPR (EUR20 million or 4% of realised revenues).

Other planned measures include the establishment of regional offices of the Commissioner, an increase in the number of specialised persons dealing with data protection and in the number of operators who have adopted internal acts in this area, as well as the appointment of new representatives of foreign operators in Serbia.

Further raising of awareness of the importance of personal data protection and ways of exercising rights

This goal includes the education of controllers and decision-makers, and the training of public administration employees in the field of personal data protection, as well as the education of judges and prosecutors. On the other hand, the importance of the public's awareness of their rights is also recognised, and the introduction of subjects in this field at different levels of formal education, as well as the education of teachers and professors.

Improvement of the personal data protection system during the development and application of information and communication technologies in the digitisation processes

The strategy recognises the impact of new technologies on personal data protection. The devel-

opment of guidelines for assessing the impact of processing on the protection of personal data when it comes to new technologies is foreseen, as well as the number of software solutions that have been developed on the basis of this impact assessment. Further measures envisage the regulation of automated processing of genetic and biometric data, as well as audio and video monitoring, special training for those who supervise such automated processing, as well as an increase in the number of employees at the Commissioner's office who deal with the protection of personal data in the field of information and communication technologies in the digitisation processes.

The government of the Republic of Serbia adopted the Action Plan for implementing the Strategy and its goals in January 2025. In mid-January 2025, the working group responsible for preparing a draft of amendments of the personal data protection act held its first meeting. They announced that their work is to be focused on the introduction of legislation which is omitted from the current law but urgently needed such as the legal regulation of cookies, video surveillance, AI and the like.

Serbia Adopted a Second Artificial Intelligence Strategy 2025-2030

In 2019m Serbia adopted the "Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025." The strategy established "goals and measures for the development of artificial intelligence, the implementation of which should result in economic growth, improvement of public services, improvement of scientific staff and development of skills for the jobs of the future". Also, "implementation of the measures of the Strategy should ensure that artificial intelligence in the Republic of Serbia is developed and applied in a safe manner and in accordance with internationally recognised ethical principles in order to use the potential of this technology to improve the quality of life of each individual and society as a whole, as well as for achieving the Sustainable Development Goals".

In 2022, Serbia became a member of Global Partnership on Artificial Intelligence and, in 2023, Serbia became a member of the AI Governance Alliance at the AI Governance Summit of the World Economic Forum in San Francisco.

In January 2025, Serbia adopted the new "Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2025-2030". The new Strategy acknowledged that Serbia had adopted UNICEF's Recommendation on the Ethics of Artificial Intelligence and that it has implemented the application of AI in the educational and health sectors. The new Strategy advocates support for start-ups and small- and medium-sized enterprises in the AI sector and measures for increasing investment in the development of AI. It also establishes a National Artificial Intelligence Platform, an infrastructure platform which would facilitate innovation. The Strategy also focuses on introducing and implementing AI solutions in the public sector. One of the most important goals prescribed by the Strategy is the creation of a legislative framework for AI. The adoption and full implementation of the AI legislation are planned by the end of 2027.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com