PANORAMIC

DATA PROTECTION & PRIVACY

Serbia

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: July 17, 2024

Contents

Data Protection & Privacy

LAW AND THE REGULATORY AUTHORITY

Legislative framework
Data protection authority
Cooperation with other data protection authorities
Breaches of data protection law
Judicial review of data protection authority orders

SCOPE

Exempt sectors and institutions
Interception of communications and surveillance laws
Other laws
PI formats
Extraterritoriality
Covered uses of PI

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds
Legitimate processing – types of PI

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency
Exemptions from transparency obligations
Data accuracy
Data minimisation
Data retention
Purpose limitation
Automated decision-making

SECURITY

Security obligations
Notification of data breach

INTERNAL CONTROLS

Accountability
Data protection officer
Record-keeping
Risk assessment
Design of PI processing systems

REGISTRATION AND NOTIFICATION

Registration
Other transparency duties

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers
Restrictions on third-party disclosure
Cross-border transfer
Further transfer
Localisation

RIGHTS OF INDIVIDUALS

Access
Other rights
Compensation
Enforcement

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

SPECIFIC DATA PROCESSING

Cookies and similar technology
Electronic communications marketing
Targeted advertising
Sensitive personal information
Profiling
Cloud services

UPDATE AND TRENDS

Key developments of the past year

Contributors

Serbia

BDK Advokati

Bogdan Ivanišević Bogdan.Ivanisevic@bdkadvokati.com
Anja Gligorević Anja.Gligorevic@bdkadvokati.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Data Protection Act 2018 (the DP Act) governs the collection and use of personal information (PI). The DP Act, for the most part, copies the provisions of the EU General Data Protection Regulation (GDPR).

Sectoral laws also apply to PI processing in particular areas.

Law stated - 17 May 2024

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Serbian data protection authority responsible for overseeing the implementation of the DP Act is the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner).

The Commissioner has numerous investigative, corrective, authorisation and advisory powers, which correspond to those exercised by supervisory authorities in EU member states under article 58 of the GDPR.

As a supervisory authority, the Commissioner has the power to supervise PI controllers through inspections. The inspectors act upon information acquired ex officio or received from complainants or third parties.

Law stated - 17 May 2024

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Under the DP Act, the Commissioner has an explicit obligation to cooperate with data protection authorities from other countries. The DP Act refers, by way of example, to the exchange of information and legal assistance in carrying out inspections. The law does not specify mechanisms to resolve different approaches.

Law stated - 17 May 2024

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches of the DP Act may result in the issuance of warnings, reprimands or orders by the Commissioner. When the Commissioner detects a breach, he or she may exercise the corrective powers given by the DP Act, such as issuing orders to controllers or processors to comply with provisions of the DP Act; ordering limitation or a ban on processing; and ordering rectification or erasure of PI, among other things.

Some breaches of the law are set out as misdemeanours for which the DP Act prescribes fines. Where the DP Act prescribes fines within a range, the Commissioner is authorised to initiate misdemeanour proceedings, while misdemeanour courts conduct the proceedings and impose sanctions. Where the DP Act prescribes fines as fixed amounts, the Commissioner itself is authorised to impose sanctions. Also, the DP Act provides for individuals to protect their rights before the courts.

There are also criminal penalties for the unauthorised collection of personal information. The penalties are not prescribed in the DP Act but in article 146 of the Criminal Code, and ordinary courts are in charge of imposing them.

Law stated - 17 May 2024

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

PI owners can initiate proceedings against a decision issued by the Commissioner before an administrative court within 30 days of the receipt of the decision.

Law stated - 17 May 2024

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

In general, the Data Protection Act 2018 (the DP Act) covers all sectors and types of organisations, as well as areas of activity.

However, the DP Act exempts many of its provisions from application to the personal information (PI) processing for the purposes of prevention, investigation and detection of criminal offences, prosecution of offenders or enforcement of criminal sanctions. Also, parts of the DP Act do not apply to processing for journalistic, scientific, artistic or literary expression purposes if such exemptions are necessary for the protection of freedom of expression and information.

Law stated - 17 May 2024

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The DP Act is an umbrella regulation in the field of PI protection in Serbia. Therefore, the general principles set out in the DP Act apply to all forms of PI processing, including interception of communications, electronic marketing, and monitoring and surveillance of individuals.

There are also sectoral laws regulating PI processing in these fields. For example, the Electronic Communications Act 2010 and Electronic Communications Act 2023 regulate the interception of communications, while the E-commerce Act 2009, the Consumer Protection Act 2021 and the Advertising Act 2016 regulate electronic marketing. Comprehensive regulation of the monitoring and surveillance of individuals is still lacking.

Law stated - 17 May 2024

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

The following laws provide for specific data protection rules:

- the Patients' Rights Act 2013 on the obligation of health professionals to keep patients' PI confidential;
- the Labour Act 2005 on PI processing within the employment sector, which provides for the right of employees to access the PI held by their employers and to have specific parts of their PI corrected or erased;
- the Labour Records Act 1996 on collecting and keeping PI in the employment sector;
- the Healthcare Documentation and Healthcare Records Act 2023 on collecting and keeping PI in the healthcare sector;
- the High Education Act 2017 on PI processing within the sector of higher education;
- the Education System Act 2017 on PI processing within the education sector (processing includes collecting and keeping the PI of pupils, parents, teachers and other employees);
- the Pension and Disability Insurance Act 2003 on collecting and keeping PI within the sector of pensions and disability insurance;
- the Health Insurance Act 2019 on collecting and keeping PI within the health insurance sector; and
- the E-commerce Act 2009, the Consumer Protection Act 2021 and the Advertising Act 2016 on obtaining consent for direct marketing that targets the consumer.

Law stated - 17 May 2024

PI formats

What categories and types of PI are covered by the law?

The DP Act covers all forms of PI, without any restriction or exemption.

Law stated - 17 May 2024

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Article 3.3 of the DP Act states that it applies to the processing of PI in the context of the activities of a 'business seat or residence' of a data controller or data processor in Serbia, regardless of whether the processing itself takes place in Serbia or not. The provision employs the concepts of 'business seat' (for legal entities) and 'residence' (for natural persons), instead of the broader concept of 'establishment' from the analogous provision in article 3.1 of the EU General Data Protection Regulation (GDPR). However, the difference in the wording seems to have resulted from the absence of an appropriate translation for 'establishment' in the Serbian language rather than from an intent of the legislature to regulate the jurisdictional issue in a manner different from the GDPR. In the 2024 publication 'Protection of Personal Data: Stances and Opinions of the Commissioner', the Commissioner for Information of Public Importance and Personal Data Protection expressed the stance that the concept of 'business seat or residence' should be interpreted as corresponding to the concept of 'establishment' in the GDPR.

The DP Act also applies to the processing of PI pertaining to individuals residing in Serbia when such processing is carried out by a data controller or a data processor that is located outside Serbia and relates to the offering of goods or services, irrespective of whether a payment of the individual is required, to such individuals in Serbia or the monitoring of individuals' behaviour, provided that their behaviour takes place in Serbia.

Law stated - 17 May 2024

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The DP Act covers all forms of use or other processing of PI. The DP Act defines PI processing as any action or set of actions that is performed on personal data or sets of personal data, whether or not by automated means, such as collecting, recording, classifying, grouping, structuring, storing, adapting, altering, consulting, using, disclosing by transmission or provision, reproducing, disseminating or otherwise making available, comparing, restricting, erasing or destroying such data.

There is a distinction between those who control the processing of PI and those who process PI on behalf of the controllers. The former have the status of 'data controllers'. Under the DP Act, they are entirely responsible for PI. The latter have the status of 'data processors' and are responsible for processing the entrusted PI properly, under law or contract provisions, and also for the implementation of adequate security measures.

Data controllers have a series of obligations under the DP Act, such as providing individuals with information about the processing of their PI, responding to the individuals' requests regarding their PI, implementing appropriate measures to ensure the security of processing, maintaining records of the processing activities, carrying out a data protection impact assessment, appointing a data protection officer, notifying data breaches to the Commissioner and individuals, and enabling such individuals to effectively exercise a broad set of rights that the law grants them.

The DP Act also sets out a scope of obligations on the part of data processors. A processor must maintain records of the processing activities, appoint a data protection officer, notify data breaches to the data controller and abide by the rules of cross-border transfers of PI. Individuals have the right to an effective judicial remedy against the data processor.

Law stated - 17 May 2024

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Under the Data Protection Act 2018 (the DP Act), personal information (PI) processing must be based on one of six grounds to be lawful, namely:

- the individual's consent;
- performance of a contract to which the individual is or intends to be a party;
- compliance with a legal obligation;
- protection of the vital interests of the individual or another natural person;
- performance of a task carried out in the public interest or the exercise of official authority; or
- the legitimate interests pursued by the data controller or by a third party.

Law stated - 17 May 2024

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

In general, the DP Act prohibits the processing of 'special categories of personal data'. These categories of personal data include the PI revealing racial or ethnic origin, political

opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, PI concerning health and PI concerning a natural person's sex life or sexual orientation. However, the law sets out 10 situations or purposes that render the processing lawful.

- The data subject has given explicit consent to the processing of such personal data for one or more specified purposes, except where the law provides that the processing may not be carried out on the basis of consent.
- Processing is necessary for the purposes of carrying out the obligations and exercising statutorily prescribed rights of the controller or of the data subject in the field of employment and social security as well as social protection law, insofar as such processing is authorised by law or a collective agreement providing for appropriate safeguards for the fundamental rights, freedoms and the interests of the data subject.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing is carried out in the course of registered activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. This is also contingent on the processing being related solely to the members or to former members of the body, or to persons who have regular contact with it in connection with its purposes, and that the personal data are not disclosed outside that body without the consent of the data subjects.
- Processing relates to personal data that are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest, on the basis of law, insofar as such processing is proportionate to the aim pursued; respects the essence of the right to data protection; and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
- Processing is necessary for the purposes of preventive or occupational medicine; the assessment of the working capacity of the employee; medical diagnosis; the provision of health or social care or treatment; or the management of health or social care systems and services on the basis of law or pursuant to a contract with a health professional. This is provided that the processing is carried out by, or under the supervision of, a health professional or other person who has an obligation to keep professional secrecy prescribed by law or professional rules.
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care, medicinal products or medical devices, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, provided that the processing is

proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Law stated - 17 May 2024

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The obligation to inform individuals on all relevant aspects of personal information (PI) processing falls on the data controller. The notice must be provided at the time the PI is collected. Under the Data Protection Act 2018 (the DP Act), the notice must contain information about:

- the identity and the contact details of the controller and its representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing as well as the legal basis for the processing;
- the legitimate interests pursued by the controller or by a third party when such interest is the legal basis for the processing;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer PI to a third country or international organisation and the legal basis for the transfer;
- the period for which the PI will be stored or, if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of PI, or restriction of processing concerning the individual or to object to the processing as well as the right to data portability;
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the Commissioner for Information of Public Importance and Personal Data Protection; and
- the existence of automated decision-making, including profiling, information about the logic involved in the automated decision-making, and the significance and the envisaged consequences of such processing for the individual.

Also, a PI controller who collects PI from a third party must inform the individual about it, within a specified time and with the inclusion of elements largely resembling those when PI is collected from the individual.

Law stated - 17 May 2024

Exemptions from transparency obligations
When is notice not required?

Where PI is collected from the individual, notice is not required if the individual already has the information about the relevant aspects of the PI processing.

Where PI has not been obtained from the individual, there are three additional exemptions from the controller's obligation to notify:

- if the provision of information proves impossible or would involve a disproportionate effort;
- if obtaining or disclosure is expressly laid down by law that provides appropriate measures to protect the individual's legitimate interests; or
- where the PI must remain confidential subject to an obligation of professional secrecy regulated by European Union (EU) or EU member state law, including a statutory obligation of secrecy.

Law stated - 17 May 2024

Data accuracy
Does the law impose standards in relation to the quality, currency and accuracy of PI?

The DP Act prescribes that the PI must be adequate and relevant concerning the purposes for which it is processed. Also, the PI must be accurate and, where necessary, kept up to date. Taking into account the purposes of the processing, every reasonable step must be taken to erase or rectify inaccurate PI without delay.

Law stated - 17 May 2024

Data minimisation
Does the law restrict the types or volume of PI that may be collected?

The DP Act restricts the volume and types of PI that may be collected.

The PI must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation principle).

The DP Act generally prohibits the processing of 'special categories of personal data'. These categories include PI revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, PI concerning health and PI concerning a natural person's sex life or sexual orientation. The law sets out 10 situations in which, exceptionally, processing 'special categories of personal data' is permissible.

Processing of PI relating to criminal convictions, offences and security measures may be carried out only under the control of official authority or, when the processing is permitted by law, providing appropriate safeguards for the rights and freedoms of individuals.

Law stated - 17 May 2024

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

PI may be kept in a form that permits the identification of individuals for no longer than is necessary for the purposes for which the personal data are processed.

Law stated - 17 May 2024

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Under the DP Act, the purpose of the processing of PI must be clearly determined and permissible. As a rule, processing for purposes other than those specified is not allowed.

Personal information collected and processed for a particular purpose may also be processed for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

Law stated - 17 May 2024

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The DP Act generally prohibits the use of PI for decision-making based solely on automated processing, including profiling, if the decision produces legal effects concerning the individual or significantly affects him or her.

The law sets out three exceptions in which automated decision-making is lawful:

- the decision is necessary for entering into, or the performance of, a contract between the individual and the PI owner;
- the decision is made based on a law that lays down suitable measures to safeguard the individual's rights, freedoms and legitimate interests; or
- the decision is based on the individual's explicit consent.

Law stated - 17 May 2024

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Data Protection Act 2018 (the DP Act) includes 'integrity and confidentiality' among the principles relating to the processing of personal information (PI). Processing must be performed in a manner that ensures the security of PI, including protection against unauthorised or unlawful processing, or accidental loss, destruction or damage of PI.

The DP Act provides examples of appropriate technical or organisational measures that can be taken to ensure an appropriate level of PI security:

- the pseudonymisation and encryption of PI;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PI promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Law stated - 17 May 2024

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The DP Act defines a 'data breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Data controllers are obliged to notify security breaches both to individuals and to the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner). Data controllers are obliged to notify the Commissioner when a security breach can result in a risk to the rights and freedoms of natural persons. The notification must be submitted without undue delay and, if feasible, not later than 72 hours after becoming aware of the breach. If the breach can result in a high risk to the rights and freedoms of natural persons, the data controller, as a rule, must communicate the breach to affected individuals. The duty to notify the Commissioner and to notify the individuals triggers when the breach 'can result' in the relevant risk. It seems that this departure from the 'likely to' standard in the EU General Data Protection Regulation (GDPR) resulted from poor translation of the relevant GDPR provision and is unlikely to have a bearing in practice.

Additionally, the Information Security Act 2016, as amended, requires operators of essential information and communication systems, such as those used in the banking, health and

transport sectors, to report security incidents to the relevant authority. Depending on the sector in which the operator functions, this authority could be the Ministry of Information and Telecommunications, the National Bank of Serbia, or the Regulatory Agency Authority for Electronic Communications and Postal Services. A security incident is defined as an event having an actual adverse effect on the security of network and information systems.

The Electronic Communications Act 2023 states that a person or entity carrying out electronic communications activities must notify the Regulatory Authority for Electronic Communications and Postal Services of any breach of security and integrity of public communication networks or services that has significantly affected the operations of that person or entity.

Law stated - 17 May 2024

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Personal information (PI) owners are responsible for, and must be able to demonstrate, compliance with the principles relating to data processing set out in the Data Protection Act 2018 (the DP Act). PI owners are obliged to implement appropriate technical, organisational and personnel measures to ensure and to be able to demonstrate that processing is performed in accordance with the DP Act. Where necessary, PI owners should review and update these measures.

Law stated - 17 May 2024

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Under the DP Act, the appointment of a data protection officer is mandatory in the following cases:

- the processing is carried out by a public authority, except for courts acting in a judicial capacity;
- the core activities of the data controller or the data processor consist of processing operations that require regular and systematic monitoring of individuals on a large scale; or
- the core activities of the data controller or the data processor consist of processing on a large scale of special categories of data or PI relating to criminal convictions and offences.

The data protection officer is responsible for performing the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations concerning the protection of personal data;
- to monitor compliance with the DP Act, with other laws and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations and the related audits;
- to provide advice where requested as regards the data protection impact assessment and to monitor its performance; and
- to cooperate with the supervisory authority and to act as the contact point for the supervisory authority on issues relating to processing.

The data protection officer must possess relevant professional qualities and, in particular, expert knowledge of data protection law and practices as well as the ability to fulfil the tasks referred to in the DP Act.

Law stated - 17 May 2024

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

PI controllers are required to establish and maintain PI processing records that contain relevant information on the categories of PI and the individuals involved, and the types of processing activities and the purpose of processing, among others.

A processor is required to maintain a record of all categories of processing activities carried out on behalf of a controller.

These obligations do not apply to companies and organisations with fewer than 250 persons unless the processing:

- can result in a high risk to the rights and freedoms of the individuals;
- is not occasional; or
- includes special categories of PI or PI relating to criminal convictions and offences.

Law stated - 17 May 2024

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

PI owners are required to carry out a data protection impact assessment (DPIA) where a type of processing, in particular using new technologies, and considering the nature, scope,

context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals.

The DP Act specifically identifies three cases in which a PI owner must carry out a DPIA:

- a systematic and extensive evaluation of an individual's personal aspects, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect him or her;
- processing on a large scale of 'special categories of data' or of PI relating to criminal convictions and offences; or
- systematic monitoring of a publicly accessible area on a large scale.

A DPIA must contain at least:

- a description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the PI owner;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of individuals; and
- the measures envisaged to address the risks.

Law stated - 17 May 2024

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

Under the DP Act, a controller must, both at the time of the determination of the means for processing and at the time of the processing itself, do the following:

- implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation; and
- implement appropriate technical and organisational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed – such measures must ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Law stated - 17 May 2024

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

The Data Protection Act 2018 does not require registration with the Commissioner for Information of Public Importance and Personal Data Protection.

Law stated - 17 May 2024

Other transparency duties

Are there any other public transparency duties?

No.

Law stated - 17 May 2024

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

No specific provisions regulate the sharing of personal information (PI) to entities providing processing services to the PI controllers. Under the Data Protection Act 2018 (the DP Act), a 'data processor' is a subject who processes PI on behalf of the PI controller and their relationship must be governed by a contract or other legally binding act. The DP Act specifies the elements that the contract or other legally binding act must contain.

Law stated - 17 May 2024

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Under the DP Act, PI controllers may share the PI with other recipients (PI users) only if there is a legal basis for the sharing as a PI processing operation and, in the case of 'special categories of personal data', an exception from the general prohibition to process the PI applies. The law does not contain restrictions specifically addressing the selling of PI or sharing PI for online targeted advertising purposes.

Law stated - 17 May 2024

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The cross-border transfer of PI from Serbia is not restricted nor subject to any authorisation if the country of import is a party to the Council of Europe Convention for the Protection of Individuals concerning Automatic Processing of Personal Data (Convention 108) or the country ensures an adequate level of protection as determined by the European Union.

For cross-border transfer to other countries or international organisations, specific authorisation from the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner) is not required if the controller or processor may rely on any of the following appropriate safeguards:

- a legally binding and enforceable instrument between public authorities or bodies;
- the PI exporter and importer enter into an agreement containing standard contractual clauses (controller to processor), which the Commissioner adopted in January 2020;
- 'binding corporate rules', approved by the Commissioner;
- a code of conduct, approved by the Commissioner; or
- a certification mechanism, approved by the Commissioner.

Subject to authorisation from the Commissioner, the appropriate safeguards may also be provided by a transfer agreement between the controller or processor and the controller, processor or recipient of the PI in the other country or international organisation, or provisions to be inserted into administrative arrangements between public authorities or bodies that include enforceable and effective rights of the individuals.

Importantly, the DP Act does not vest the Commissioner with the power to create standard contractual clauses for transfers from one controller to another. As a consequence, a transfer from a controller to another controller requires the Commissioner's authorisation, based on a transfer agreement.

Finally, a derogation for specific situations applies, including:

- when the individual has explicitly consented to the proposed transfer;
- the transfer is necessary for the performance of a contract between the individual and the controller or the implementation of pre-contractual measures taken at the individual's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the controller and another natural or legal person; or
- the transfer is necessary for the establishment, exercise or defence of legal claims.

In these instances, authorisation from the Commissioner is not required.

Law stated - 17 May 2024

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

No specific provisions regulate further transfers of PI. Also, the Commissioner has not developed any practice in this regard under the current DP Act. However, it seems plausible that, if the primary transfer requires authorisation, an onward transfer would also have to be encompassed by that authorisation to be lawful.

Law stated - 17 May 2024

Localisation
Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

The law does not require PI or a copy of PI to be retained in Serbia.

Law stated - 17 May 2024

RIGHTS OF INDIVIDUALS

Access
Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have the right to be accurately and fully informed about the processing of their personal information (PI), the right to access the PI and the right to obtain a copy of the PI. To exercise these rights, the individual must submit a request to the PI owner. The right to access can be partly or completely restricted if the restriction is necessary based on the following statutory grounds:

- to avoid obstructing official or statutory collection of information, investigation or proceedings;
- to enable the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties;
- to safeguard public security;
- to safeguard national security and defence; or
- to safeguard the rights and freedoms of other individuals.

Law stated - 17 May 2024

Other rights
Do individuals have other substantive rights?

Upon obtaining access to the PI, individuals have the right to require that the PI owners correct, modify, update or delete the PI. They also may require restriction of the processing. Individuals also have the right to PI portability. This right entitles the individuals to receive their PI, which they have previously provided to a data controller, in a structured, commonly used and machine-readable format. Additionally, the individuals have the right to transmit such PI to another data controller.

Also, the Data Protection Act 2018 (the DP Act) envisages the right of individuals to object to the processing of their PI, including profiling, when the legal basis for the processing is either the data controller's or a third party's legitimate interest or performance of a task carried out in the public interest, or the exercise of official authority vested in the data controller. Individuals may also opt out of the processing for direct marketing purposes, meaning that, where the individual objects to processing for direct marketing purposes, the PI may no longer be processed for such purposes.

Law stated - 17 May 2024

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The DP Act explicitly provides for an individual's right to receive compensation from the controller or processor for both economic and non-economic damage (injury to feelings).

Law stated - 17 May 2024

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

If the PI owner rejects or denies the individual's request to exercise his or her rights, or fails to decide on a request within the specified time limit as well as in other cases prescribed by the DP Act, the individual may lodge a complaint with Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner). The Commissioner issues a ruling, which may be challenged in administrative proceedings before the Administrative Court.

Claims for damages must be brought to a civil court.

Law stated - 17 May 2024

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

The Data Protection Act 2018 (the DP Act) authorises data controllers to restrict the exercise of individual's rights under the law when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure to enable or safeguard:

- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- public security;
- national security;
- defence;
- other important objectives of general public interest, in particular an important economic or financial interest of Serbia, including monetary, budgetary and taxation matters, public health and social security;
- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases further specified in the DP Act;
- the protection of the individual or the rights and freedoms of others; or
- the enforcement of civil law claims.

Law stated - 17 May 2024

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The Electronic Communications Act 2023 states that storing cookies on the end user's terminal equipment is permissible only if the end user has given consent after being provided with clear and comprehensive information about the purpose of collecting and processing PI, and is allowed to refuse such processing.

There have been no authoritative rulings by the Commissioner for Information of Public Importance and Personal Data Protection or the courts as to the adequacy of the specific modes of cookie notification.

Law stated - 17 May 2024

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

The E-commerce Act 2009 states that unsolicited commercial messages may be sent via email to individuals only if individuals have given their prior consent to such types of marketing. The Advertising Act 2016 provides that advertising through sending out electronic messages or by other means of direct electronic communication is prohibited, unless the recipient of the advertising message has given his or her prior consent. The Consumer Protection Act 2021 prohibits direct marketing via devices for distant communication, including but not limited to telephone, fax machine or email, without the consumer's prior consent. Finally, the Electronic Communications Act 2023 provides that making calls, including using automatic calling and communication systems without human intervention, fax machines, email, or other means of electronic messages for direct marketing, is only permitted with the prior consent of the end user.

Law stated - 17 May 2024

Targeted advertising

Are there any rules on targeted online advertising?

No.

Law stated - 17 May 2024

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

Processing of 'sensitive' categories of PI (special categories of personal data) is generally prohibited. However, processing of 'sensitive' PI is lawful if one of the 10 exemptions prescribed by the Data Protection Act 2018 applies. The exemptions include, for example, processing based on an individual's consent and processing related to PI that is manifestly made public by the individual.

Law stated - 17 May 2024

Profiling

Are there any rules regarding individual profiling?

Decision-making based solely on automated processing of PI, including profiling, is generally prohibited if the decision produces legal effects concerning the individual or significantly affects him or her.

The law sets out three exceptions in which such decision-making is lawful:

- the decision is necessary for entering into, or the performance of, a contract between the individual and the PI owner;
- the decision is made based on a law that lays down suitable measures to safeguard the individual's rights, freedoms and legitimate interests; or

- the decision is based on the individual's explicit consent.

Law stated - 17 May 2024

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

No.

Law stated - 17 May 2024

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

There are no updates at this time.

Law stated - 17 May 2024