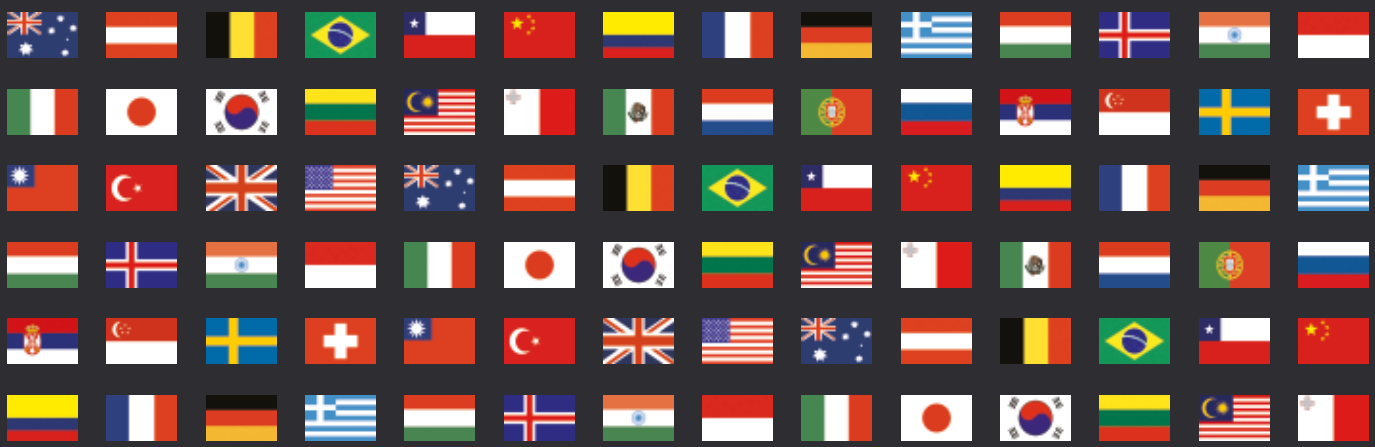
# Data Protection & Privacy 2020

Contributing editors
**Aaron P Simpson and Lisa J Sotto**



LEXOLOGY
Getting The Deal Through

**Publisher**
Tom Barnes
tom.barnes@lbresearch.com

**Subscriptions**
Claire Bagnall
claire.bagnall@lbresearch.com

**Senior business development managers**
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

**Published by**
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910


First published 2012
Eighth edition
ISBN 978-1-83862-146-9

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

# Data Protection & Privacy

2020

Contributing editors
**Aaron P Simpson and Lisa J Sotto**
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the eighth edition of *Data Protection and Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Hungary, Iceland, Indonesia and Malaysia.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

# Contents

# Serbia

**Bogdan Ivanišević and Milica Basta**
BDK Advokati

## LAW AND THE REGULATORY AUTHORITY

### Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The Personal Data Protection Act 2008 (DP Act), governs the collection and use of PII. Serbia is not an EU member, but the DP Act has adopted some of the basic principles of the Data Protection Directive.

In November 2018, the parliament adopted the New Data Protection Act (New DP Act) that for the most part copies the provisions of the EU General Data Protection Regulation (GDPR). The New DP Act will apply from late August 2019.

Sectoral laws also apply to PII processing in particular areas (see questions 6 and 7).

### Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

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).

In the performance of its tasks, the Commissioner has the right to access and examine:

- PII and PII files;
- all documents relating to collection of PII and to other processing activities, as well as to the exercise of the rights of the individual;
- PII controllers' general enactments; and
- premises and equipment that the PII controllers use.

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

### Cooperation with other data protection authorities

3 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??

Both under the DP Act and the New DP Act, the Commissioner has an explicit obligation to cooperate with data protection authorities from other countries. The DP Act does not give further details on the manner of cooperation. The New DP Act refers, by way of examples, to exchange of information and legal assistance in carrying out inspections. Neither law specifies mechanisms to resolve different approaches.

### Breaches of data protection

4 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, established in the process of supervision, may result in an issuance of warnings or orders by the Commissioner. When the Commissioner detects a breach, he or she may:

- order the rectification of the irregularity within a specified period of time;
- temporarily ban the processing carried out in breach of the provisions of the DP Act; or
- order deletion of the PII collected without a proper legal basis.

Some of the breaches of law are set out as misdemeanours for which the DP Act prescribes fines. The Commissioner is authorised to initiate misdemeanour proceedings, while misdemeanour courts conduct the proceedings and impose sanctions.

The New DP Act increases twofold the misdemeanour fines against the data controller, data processor, and user. Also, the New DP Act provides for the possibility for individuals to protect their rights before the courts.

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

## SCOPE

### Exempt sectors and institutions

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

In general, the DP Act covers all sectors and types of organisation, as well as areas of activity. As a partial exception, the DP Act does not apply to political parties, organisations, trade unions and other forms of associations who process PII pertaining to their members, provided that the member has waived in writing the application of specified provisions of the Act for a specified period of time not exceeding the termination of his or her membership.

In addition, most of the provisions of the DP Act do not apply to journalists and other media operatives when they process PII for the sole purpose of publishing the information in the mass media. The law fully applies, however, to the processing of PII for advertising purposes.

The New DP Act exempts many of its provisions from application to the PII processing for the purpose of prevention, investigation and

detection of criminal offences, prosecution of the offenders, or enforcement of criminal sanctions. Also, parts of the New DP Act will not apply to the processing for journalistic purposes or for the purpose of scientific, artistic, or literary expression, if the exemptions are necessary for protection of the freedom of expression and information.

**Communications, marketing and surveillance laws**

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The DP Act is an 'umbrella regulation' in the field of PII protection in Serbia. Therefore the general principles set out in the DP Act apply to all forms of PII processing, including interception of communications, electronic marketing, and monitoring and surveillance of individuals. The reach of the New DP Act will be similarly broad.

There are also sectoral laws regulating PII processing in these fields. For example, the Electronic Communications Act 2010 regulates interception of communications, while the E-commerce Act 2009, Consumer Protection Act 2014, and Advertising Act 2016 regulate electronic marketing. Comprehensive regulation of the monitoring and surveillance of individuals is still missing.

**Other laws**

7 Identify any further laws or regulations that provide specific data protection rules for related areas.

The following laws provide for specific data protection rules:

- Patients' Rights Act 2013 on the obligation of health professionals to keep the patients' PII confidential;
- Labour Act 2005 on PII processing within the employment sector. The law provides for the right of employees to access the PII held by their employer and to have specific parts of their PII corrected or erased;
- Labour Records Act 1996 on collecting and keeping the PII in the employment sector;
- Healthcare Documentation and Healthcare Records Act 2014 on collecting and keeping the PII in the healthcare sector;
- High Education Act 2017 on PII processing within the sector of higher education;
- Education System Act 2017 on PII processing within the education sector. The processing includes collecting and keeping the PII of pupils, parents, teachers and other employees;
- Pension and Disability Insurance Act 2003 on collecting and keeping PII within the sector of pension and disability insurance;
- Health Insurance Act 2005 on collecting and keeping PII within the health insurance sector; and
- E-Commerce Act 2009, Consumer Protection Act 2014 and Advertising Act 2016 on obtaining consent for direct marketing targeting the consumer.

**PII formats**

8 What forms of PII are covered by the law?

The DP Act and the New DP Act cover all forms of PII, without any restriction or exemption.

**Extraterritoriality**

9 Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The DP Act applies to all PII controllers, users and processors who process PII in the territory of the Republic of Serbia, regardless of where they have been established or where their seat is.

The New DP Act will apply to the processing of PII in the context of the activities in Serbia of data controllers or data processors who have business seat or residence in Serbia, regardless of whether the processing itself takes place in Serbia or not. The New DP Act will also apply to the processing of PII 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 as far as their behaviour takes place in Serbia.

**Covered uses of PII**

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

The DP Act covers all forms of use or other processing of PII. The Act defines PII processing as any action taken in connection with the information, including: collection, recording, transcription, multiplication, copying, transmission, search, classification, storage, separation, adaptation, modification, making available, use, dissemination, recording, storage, disclosure through transmission or otherwise, dislocation, as well as other actions carried out in connection with the PII, regardless of whether such actions are automated, semi-automated, or carried out otherwise. The New DP Act contains an essentially identical definition.

There is a distinction between those who control the processing of PII and those who process PII on behalf of the controllers. The former have the status of 'data controllers'. Under the DP Act, they are entirely responsible for PII. They are in charge of establishing and maintaining PII processing records, notifying the Commissioner of their intent to establish a PII file, registering a PII file with the Central Data Filing System Register, responding to individuals' requests to access the PII, and so on. The latter have the status of 'data processors' and are responsible for processing the entrusted PII properly, in accordance with law or contract provisions, and also for the implementation of adequate security measures.

The New DP Act does not require the data controllers to notify the Commissioner of the intent to process PII, except where the strength of the risks arising from the processing require prior consultation with the Commissioner. Also, the law dispenses with the obligation to register the processing activities with the Commissioner. At the same time, data controllers have a series of obligations under the New DP Act that were absent from the DP Act, including the obligation to carry out a 'data protection impact assessment', appoint a data protection officer, notify data breaches to the Commissioner and the individuals, and enable the individuals to effectively exercise a broad set of rights that the law grants them.

The New DP Act also expands the scope of obligations on the part of data processors. A processor now has to 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 PII. Individuals have the right to an effective judicial remedy against the data processor.

## LEGITIMATE PROCESSING OF PII

### Legitimate processing – grounds

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

Under the DP Act, the processing has to be based on the individual's consent, a statutory provision, preparation of a contract to which the individual is or intends to be a party; or protection of the vital interests or the individual. The consent must be given in a proper form (ie, in writing or orally on the record).

The New DP Act introduces two additional grounds for lawful processing: performance of a task carried out in the public interest or in the exercise of official authority; and, most importantly, the legitimate interests pursued by the data controller or by a third party. Consent may be expressed by a statement or a clear affirmative action.

### Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

The DP Act has strict requirements concerning the processing of 'particularly sensitive data', defined as PII relating to ethnicity, race, gender, language, religion, political party affiliation, trade union membership, health status, receipt of social support, status of a victim of violence, criminal record and sex life. Only the individual's consent may constitute legal basis for the processing of particularly sensitive PII. The form of the consent, as prescribed by the DP Act, is more stringent than the form of consent for the processing of other types of PII.

Under the New DP Act, the 'special categories of personal data' include the PII revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data processed for the purpose for uniquely identifying a natural person, PII concerning health, and PII concerning a natural person's sex life or sexual orientation. Processing of such PII is generally prohibited, however, the law sets out 10 situations or purposes that render the processing lawful.

## DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

### Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

The obligation to inform individuals on all relevant aspects of the PII processing falls on the data controller. The notice has to be provided at the time the PII is collected. Under the DP Act, the notice has to contain information about:

- the name and address or business name of the data controller or the identity of another person responsible for PII processing (if any);
- the purpose of PII collection and the subsequent processing;
- the manner in which the PII will be used;
- the identity or categories of the users of the PII;
- the mandatory nature of, and the legal basis for, the processing; or, conversely, the voluntary nature of providing the PII;
- the individual's right to withdraw his or her consent to the processing and the legal consequences in the event of a withdrawal (the individual should compensate the data controller for any reasonable costs and damages caused by the withdrawal);
- the individual's rights in the case of unlawful processing (eg, the right to request deletion of PII and suspension of the processing); and
- any other information, which, if withheld, could be considered contrary to 'conscientious practice'.

The New DP Act removes the vague requirement to provide 'information which, if withheld, could be considered contrary to conscientious practice'. The law introduces additional types of information to be furnished to the individual. The information includes the following:

- the contact details of the data protection officer;
- the legitimate interests pursued by the controller or by a third party, when such interest is the legal basis for the processing;
- where applicable, the fact that the controller intends to transfer PII to a third country or international organisation and the legal basis for the transfer;
- the period for which the PII 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 PII or restriction of processing concerning the individual or to object to processing as well as the right to data portability;
- the right to lodge a complaint with the Commissioner; 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.

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

### Exemption from notification

14 | When is notice not required?

Under the DP Act, notice is not required when giving a notice would be impossible, evidently unnecessary, or unsuitable, especially if the individual has already been informed or the individual is unavailable. The Commissioner has provided little guidance on this issue.

The New DP Act prescribes that the obligation to provide a notice does not exist if the individual already has the information.

When a data controller collects PII from a third party, the DP Act stipulates that notice to the individual is not required if notification is impossible, unnecessary, or requires excessive use of time or efforts.. The New DP Act formulates the exemptions from notification in the following manner:

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

**Control of use**

15 Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Individuals may control use of their PII by not consenting to the PII processing, as well as by exercising the right to access their personal information held by PII controllers and other substantive rights (see questions 37 and 38).

**Data accuracy**

16 Does the law impose standards in relation to the quality, currency and accuracy of PII?

The DP Act prescribes that the processing of PII is impermissible if the information is inaccurate or incomplete, or if it is not based on a credible source or is out of date.

The New DP Act includes accuracy and, where necessary, currency of PII among the principles related to processing of PII.

**Amount and duration of data holding**

17 Does the law restrict the amount of PII that may be held or the length of time it may be held?

The DP Act and the New DP Act set forth as one of the main principles that the amount of PII that may be processed has to be proportionate to the purpose of the processing. Further processing is forbidden if the purpose of the processing has been achieved. The New DP Act contains an exception to the effect that PII may be stored for longer periods insofar as the PII will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

**Finality principle**

18 Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Both the DP Act and the New DP Act adopt the 'finality principle': the purpose of the processing of PII has to be clearly determined and permissible. As a rule, processing for the purposes other than those specified is not allowed.

**Use for new purposes**

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Personal information collected and processed for a particular purpose may also be processed for historical, statistical, or scientific purposes. In that case, the information has to be properly secured. The New DP Act also adds archiving purpose to the list of purposes that justify further processing.

## SECURITY

**Security obligations**

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

The DP Act does not impose specific obligations on PII controllers and other processors concerning data security, but provides for their general duty to undertake proper 'technical, human resources, and organisational measures to protect the data in accordance with established standards and procedures in order to protect data from loss, damage, inadmissible access, modification, publication and any other abuse'. The law also requires from the data controllers and processors to provide for an obligation for all persons involved in PII processing to maintain confidentiality of the PII.

The New DP Act, apart from laying down the general security obligations, provides examples technical, human resources, and organisational measures which are appropriate:

- the pseudonymisation and encryption of PII;
- 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 PII in a timely manner 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.

**Notification of data breach**

21 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 does not require PII controllers to notify the Commissioner or the affected individuals of a data breach. The Commissioner has not issued any guidance in relation to this matter. The Electronic Communications Act (2010, as amended) states that an 'operator' (a person or entity carrying out or authorised to carry out electronic communications activities) must notify the Regulatory Agency for Electronic Communications and Postal Services of any breach of security and integrity of public communication networks or services affecting the operator's work, and especially of breaches that undermine the protection of PII or impinge on subscribers' or users' right to privacy.

The New DP Act introduces the obligation to notify security breaches both to individuals and to 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 has to 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, data controller, as a rule, has to communicate the breach to the individuals. The duty to notify the Commissioner and to notify the individuals triggers when the breach 'can result' in the relevant risk. It is unclear whether this departure from the GDPR's 'likely to' standard was purposeful or resulted from poor translation of the relevant GDPR provision, and whether it will have any bearing in practice.

## INTERNAL CONTROLS

**Data protection officer**

22 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The DP Act does not include any reference to a 'data protection officer' or similar position. The New DP Act mandates the appointment of a data protection officer in the following cases:

- the processing is carried out by a public authority, except for courts acting in their 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 of PII relating to criminal convictions and offences.

**Record keeping**

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

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

The DP Act does not require from PII processors to maintain internal records or establish internal processes or documentation. The New DP Act, in contrast, introduces the obligation for the processor to maintain a record of all categories of processing activities carried out on behalf of a controller.

**New processing regulations**

24 | Are there any obligations in relation to new processing operations?

The DP Act requires from the data controller to notify the Commissioner of the intended new processing, so that the Commissioner may conduct a prior checking procedure and determine whether the processing would entail specific and significant risk for the rights and freedoms of individual.

The New DP Act introduces the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of PII, where the type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

## REGISTRATION AND NOTIFICATION

**Registration**

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

PII controllers are required to notify the Commissioner of the intended processing of PII, as well as to register with the Commissioner the PII processing records (filing systems) and any subsequent change in the records. The Commissioner maintains the Central Data Filing Systems Register, which includes both the notifications and the PII processing records. The obligation to notify about the intended processing does not exist if a specific law determines the purpose of the processing, the categories of PII to be processed, the categories of users of the PII, and the period during which the PII will be held. In contrast, there are no exceptions to the obligation to register the PII processing records. PII processors do not have an obligation to register with the supervisory authority.

The New DP Act abolishes data controllers' obligation to register with the Commissioner.

**Formalities**

26 | What are the formalities for registration?

When PII controllers submit to the Commissioner the PII processing records, the records have to include the information referred to in the response to question 23 (categories of PII, name of the PII file, types of processing activities, purpose of the processing, and other information).

There is no payable fee for registration. Registration is valid for an indefinite period of time, so it does not have to be periodically renewed.

The New DP Act does not require registration with the Commissioner.

**Penalties**

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Under the DP Act, failure of the PII controller to register a data filing system or changes in the system within the required 15-day period constitutes a misdemeanour. The fine ranges from 50,000 to 1 million Serbian dinars for PII controllers with the status of legal entities, and from 20,000 to 500,000 Serbian dinars for entrepreneurs. The fine for a natural person is 5,000 to 50,000 Serbian dinars. The same penalty applies to the responsible officer of a legal entity, state agency, or a governing body of the territorial autonomy or local self-government.

The New DP Act does not require registration with the Commissioner.

**Refusal of registration**

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

The Commissioner may decide, when reviewing the notification files, that conditions for a lawful processing of PII are not met owing to a lack of statutory basis for the processing or lack of consent, impermissible or undetermined purpose, impermissible means of processing, inadequacy of the PII for the achievement of the purpose, disproportionate amount or categories of the PII, or non-truthfulness or incompleteness of the information. If the prior checking results in a positive finding, the Commissioner has to allow an entry on the register.

Under the New DP Act, the issue of a refusal does not arise (see questions 25 to 27).

**Public access**

29 | Is the register publicly available? How can it be accessed?

The Central Data Filing System Register was publicly available on the official site of the Commissioner before the adoption of the New DP Act in November 2018. Since then, the register has been closed to public. Under the New DP Act, the Commissioner will not maintain a data filing system register.

**Effect of registration**

30 | Does an entry on the register have any specific legal effect?

The main purpose of an entry on the Central Data Filing Systems Register was to ensure transparency of the PII processing, that is, to make the information about the filing systems and the PII controllers available to the general public.

**Other transparency duties**

31 | Are there any other public transparency duties?

There are no other public transparency duties.

## TRANSFER AND DISCLOSURE OF PII

**Transfer of PII**

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

There are no specific provisions regulating the transfer of PII to entities providing processing services to the PII controllers. Under the DP Act, 'data processor' is a subject to whom the PII controller delegates certain processing-related activities on the basis of a law or contract. The New DP Act specifies the elements which the contract must contain.

**Restrictions on disclosure**

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

Under the DP Act, PII controllers may disclose the PII to other recipients (PII users) only on the basis of a statutory provision or consent of the individual. The purpose of the disclosure must be legitimate. The New DP Act adds other legal bases for PII processing, including for the disclosure of PII to other recipients (see question 11).

**Cross-border transfer**

34 | Is the transfer of PII outside the jurisdiction restricted?

The cross-border transfer of PII from the Republic of Serbia to a country that is party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) is not restricted nor subject to any authorisation. In a case of this kind, lawful processing of PII is the sole condition that PII controllers have to meet in order to transfer the information lawfully.

On the other hand, for cross-border transfer to countries that are not parties to Convention 108 and to international organisations, under the DP Act it is necessary to obtain prior approval from the Commissioner. The New DP Act provides for several grounds for a lawful transfer without requiring any specific authorisation from the Commissioner, of which the following are likely to be most frequently used:

- transfer is to a country that ensures an adequate level of protection as determined by the European Union and formally confirmed by Serbian government;
- the PII exporter and importer enter into an agreement containing standard contractual clauses which the Commissioner may adopt (however, the Commissioner is yet to enact such clauses);
- transfer occurs among members of the group of undertakings, or group of enterprises engaged in a joint economic activity, who have adopted the 'binding corporate rules', approved by the Commissioner; or
- 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.

**Notification of cross-border transfer**

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

The DP Act requires issuance of written authorisation from the Commissioner as a condition for cross-border transfers of PII to countries not parties to Convention 108 and to international organisations. In such cases, data controllers have to submit copies of the transfer agreements with the importers. The Commissioner then assesses the safeguard measures and other relevant circumstances of the intended transfer, and issues a decision. The procedure may take any time from a few months to one year, or even more. The proceedings are lengthy and arduous, so most data controllers evade it and transfer the PII without Commissioner's authorisation. Although the practice is contrary to the law, the Commissioner has only exceptionally taken any measures against the exporter.

It follows from the relevant provisions in the New DP Act that the lawmakers' intent was to liberalise cross-border transfer and make the use of Commissioner's approval only an exception. Standard contractual clauses, to be adopted by the Commissioner, are expected to be the most frequently used mechanism for transfers not requiring Commissioner's authorisation. However, the New DP Act left it to Commissioner's discretion to create, or not create, the clauses, and representatives of the Commissioner have publicly stated that they did not consider it a priority to adopt such clauses. This might result, initially at least, in a continuation of the past framework, with many PII exporters having to apply for transfer authorisation.

**Further transfer**

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

There are no specific provisions regulating further transfers of PII. However, according to the recent practice of the Commissioner, such transfers do not require prior approvals.

## RIGHTS OF INDIVIDUALS

**Access**

37 | Do individuals have the right to access their personal information held by PII 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 PII, the right to access the PII and the right to obtain a copy of the PII. To exercise these rights, the individual must submit a request to the PII owner. Restrictions on the enjoyment of the rights include the situation in which the individual requests information pertaining to the PII already in the public domain, whether in public registers or otherwise, and the situation in which the individual abuses his or her rights.

**Other rights**

38 | Do individuals have other substantive rights?

Upon obtaining access to the PII, individuals have the right to require from the PII owners to correct, modify, update or delete the PII. They also may require suspension of the processing.

The New DP Act adds to the list of individuals' rights the right to PII portability. This right entitles the individuals to receive their PII, 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 those PII to another data controller.

Also, the New DP Act envisages the right of individuals to object to processing of their PII, 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 in the exercise of official authority vested in the data controller.

**Compensation**

39 | 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?

Under the Obligations Act (1978), which contains general provisions on indemnity for torts, individuals are entitled to compensation of damage caused by violations of their right to protection of PII. PII controllers may be liable both for actual damage and for moral damage (injury to feelings).

The New DP Act explicitly provides for an individual's right to receive compensation from the controller or processor for the material or non-material damage suffered.

**Enforcement**

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

If the PII owner rejects or denies the individual's request for exercising his or her rights, 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 the Commissioner. The Commissioner issues a ruling, which may be challenged in administrative proceedings before the Administrative Court.

Damages must be brought to a civil court.

## EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

**Further exemptions and restrictions**

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The New 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 the Republic of Serbia, including monetary, budgetary and taxation a 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 Act;
- the protection of the individual or the rights and freedoms of others; or
- the enforcement of civil law claims.

## SUPERVISION

**Judicial review**

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

PII owners can appeal to the Administrative Court against orders of the Commissioner.

## SPECIFIC DATA PROCESSING

**Internet use**

43 | Describe any rules on the use of 'cookies' or equivalent technology.

The Electronic Communications Act provides that the PII owner can store cookies on the individual's terminal equipment if the individual is provided with clear and comprehensive information about the purpose of the collection and processing of PII and given an opportunity to refuse such processing.

There have been no authoritative rulings by the Commissioner or the courts as to adequacy of the specific modes of cookie notification.

BDK Advokati

**Bogdan Ivanišević**
bogdan.ivanisevic@bdkadvokati.com

**Milica Basta**
milica.basta@bdkadvokati.com

Bulevar kralja Aleksandra 28
Belgrade 11000
Serbia
Tel: +381 11 3284 212
Fax: +381 11 3284 213
www.bdkadvokati.com

**Electronic communications marketing**

44 | Describe any rules on marketing by email, fax or telephone.

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 by means of sending out electronic messages or by other means of direct electronic communication is prohibited, unless the recipient of the advertising message has given his prior consent. The Consumer Protection Act 2014 prohibits direct marketing via devices for distant communication, including but not limited to telephone, fax machine or email, without the consumer's prior consent. And, the Electronic Communications Act 2010 provides that the use of systems for automatic calling and communications without human intervention, of faxes, emails or other means of electronic messages for direct advertising is only permitted with the prior consent of the user or subscriber.

**Cloud services**

45 | Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific provisions in the legal system of Serbia regulating cloud computing services.

## UPDATE AND TRENDS

**Key developments of the past year**

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

Adoption of the GDPR-based Data Protection Act in November 2018 (New DP Act) marks a watershed event in the development of data protection law in Serbia. The DP Act 2008 has proved to be an overly restrictive, and ultimately self-defeating, piece of legislation, which

most data controllers honoured in breach rather than in observance. The law's absolute reliance on individual's written consent as the legal basis for processing PII proved unworkable in many contexts, including in relation to the collection of PII online. Equally ineffective have been the provisions in the DP Act that require the controllers to seek Commissioner's authorisation for each cross-border transfer to the United States or other non-European countries. The New DP Act dispenses with most of the DP Act's unnecessary restrictions on the processing of PII, while at the same time strengthening the individuals' rights and introducing new, but realistic, requirements from the PII controllers and PII processors.

## Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-146-9