Data Protection & Privacy 2022

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY®
Getting The Deal Through

© Law Business Research 2021

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between May and July 2021. Be advised that this is a developing area.

© Law Business Research Ltd 2021
No photocopying without a CLA licence.
First published 2012
Tenth edition
ISBN 978-1-83862-644-0

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

Data Protection & Privacy

2022

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

Lexology Getting The Deal Through is delighted to publish the tenth edition of *Data Protection & 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 Jordan, Pakistan and Thailand.

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 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

© Law Business Research 2021

Contents

© Law Business Research 2021

© Law Business Research 2021

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

Sectoral laws also apply to PII processing in particular areas.

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).

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

As a supervisory authority, the Commissioner has the power to supervise PII controllers through 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?

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 examples, to the exchange of information and legal assistance in carrying out inspections. The law does not specify 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 may result in an 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, ordering rectification or erasure of PII, and so on.

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 the possibility 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.

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

However, the DP Act exempts many of its provisions from application to the personally identifiable information (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 DP Act do not apply to the processing for journalistic purposes or the purpose of scientific, artistic or literary expression, if the exemptions are necessary for the 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 Data Protection Act 2018 (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.

There are also sectoral laws regulating PII processing in these fields. For example, the Electronic Communications Act 2010 regulates the interception of communications, while the E-commerce Act 2009, Consumer Protection Act 2014 and Advertising Act 2016 regulate

© Law Business Research 2021

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:

- the Patients' Rights Act 2013 on the obligation of health professionals to keep the patients' PII confidential;
- the 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;
- the Labour Records Act 1996 on collecting and keeping the PII in the employment sector;
- the Healthcare Documentation and Healthcare Records Act 2014 on collecting and keeping the PII in the healthcare sector;
- the High Education Act 2017 on PII processing within the sector of higher education;
- the 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;
- the Pension and Disability Insurance Act 2003 on collecting and keeping PII within the sector of pension and disability insurance;
- the Health Insurance Act 2019 on collecting and keeping PII within the health insurance sector; and
- the 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 covers 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?

Article 3.3 of the DP Act states that it applies to the processing of PII 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. The Commissioner has shown willingness to interpret the concept of 'business seat or residence' as corresponding to the concept of 'establishment' in the GDPR.

The DP Act also applies 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 or set of actions that is performed on personal data or sets of personal data, whether or not by automated means, such as: collection, recording, classification, grouping, or structuring, storage, adaptation or alteration, consultation, use, disclosure by transmission or provision, reproduction, dissemination or otherwise making available, comparison, restriction, erasure, or destruction.

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. The latter have the status of 'data processors' and are responsible for processing the entrusted PII 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 PII, responding to the individuals' requests regarding their PII, 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 for Information of Public Importance and Personal Data Protection and the individuals, and enabling the 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 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 Data Protection Act 2018 (the DP Act), the processing has to be based on one of the six grounds to be lawful:

- 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.

Legitimate processing – types of PII

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

In general, the DP Act prohibits the processing of 'special categories of personal data'. These categories of personal data include the PII

© Law Business Research 2021

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. 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 Data Protection Act 2018 (the DP Act) the notice has to 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 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 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 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?

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

Where PII 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 individual's legitimate interests; or
- where the personal PII must remain confidential subject to an obligation of professional secrecy regulated by European Union or EU 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 the use of their PII by not consenting to the PII processing, where consent is the legal basis for the processing. Also, individuals may exercise the right to access their personal information held by PII controllers and other substantive rights.

Data accuracy

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

The DP Act prescribes that the PII must be adequate and relevant concerning the purposes for which they are processed. Also, the PII 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 PII without delay.

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 outlines 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 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?

The DP Act has adopted the 'finality principle': the purpose of the processing of PII has to be clearly determined and permissible. As a rule, processing for 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 archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

SECURITY

Security obligations

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

The Data Protection Act 2018 (the DP Act) includes 'integrity and confidentiality' among the principles relating to the processing of PII. Processing must be performed in a manner that ensures the security of

© Law Business Research 2021

PII, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage of PII.

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

- 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 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.

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 includes the obligation of data controllers 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 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, the data controller, as a rule, has to communicate the breach to the individuals. The duty to notify the Commissioner for Information of Public Importance and Personal Data Protection (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.

Also, 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.

INTERNAL CONTROLS

Data protection officer

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

Under the Data Protection Act 2018 (the DP Act), the appointment of a data protection officer (DPO) is mandatory 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 personally identifiable information (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 and the individuals, types of the processing activities, and purpose of the 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 they carry out can result in a high risk to the rights and freedoms of the individuals, the processing is not occasional, or the processing includes special categories of PII or PII relating to criminal convictions and offences.

New processing regulations

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

Under the DP Act, a controller must assess 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 individuals.

REGISTRATION AND NOTIFICATION

Registration

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

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

Formalities

26 | What are the formalities for registration?

Not applicable, because the 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?

Not applicable, because the DP Act does not require registration with the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner).

Refusal of registration

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

Under the DP Act, the issue of a refusal does not arise, because the DP Act does not require registration with the Commissioner.

Public access

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

A Central Data Filing System Register was publicly available on the official site of the Commissioner before the adoption of the current DP

© Law Business Research 2021

Act in November 2018. Since then, the register has been closed to the public. Under the current DP Act, the Commissioner does not maintain a register of PII controllers and processors.

Effect of registration

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

No register of PII controllers and processors exists under the DP Act in force.

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?

No specific provisions regulate the transfer of PII to entities providing processing services to the PII controllers. Under the Data Protection Act 2018 (the DP Act), 'data processor' is a subject who processes the PII on behalf of the PII controller, and their relationship must be governed by a contract or other legally binding act. The DP Act specifies the elements which the contract or other legally binding act 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 if there is a legal basis for the disclosure as a PII processing operation and, in the case of 'special categories of personal data', an exception from the general prohibition to process the PII applies.

Cross-border transfer

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

The cross-border transfer of PII from the Republic of 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 the 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 PII 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 the authorisation from the Commissioner, the appropriate safeguards may also be provided for by a transfer agreement between the controller or processor and the controller, processor or the recipient of the PII 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 controller requires 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, an authorisation from the Commissioner is not required.

Notification of cross-border transfer

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

The Commissioner's authorisation of a cross-border transfer of PII is required if none of the conditions for an authorisation-free transfer is met. The Commissioner is obliged to decide on the request for authorisation within 60 days from receiving it.

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?

No specific provisions regulate further transfers of PII. 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.

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. 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 Business Research 2021

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 a restriction of the processing. Also, individuals have 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 Data Protection Act 2018 (the DP Act) envisages the right of individuals to object to the 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 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?

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).

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 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.

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 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 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 for Information of Public Importance and Personal Data Protection.

SPECIFIC DATA PROCESSING

Internet use

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

The Electronic Communications Act provides that the personally identifiable information (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 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.

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 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 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.

© Law Business Research 2021

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?

No updates at this time.

Coronavirus

47 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

In the early stages of the covid-19 crisis, the Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner) emphasised that an employer who processes personal data related to the symptoms of a potentially coronavirus infected employee, job candidate or other person entering the employer's premises, has to abide by the principles relating to the processing of personal data from article 5 of the Data Protection Act 2018 (identical to those in article 5 of the EU General Data Protection Regulation).

According to the Commissioner, an employer may take the temperature of its employees based on the employer's legal obligation to ensure safety and health at work. However, an employer is not authorised to record the temperature. An employer may only prevent individuals with a high temperature from entering the premises.

Employers are authorised to share the data on infected individuals with other employees. This enables those who were in contact with the infected employees to test themselves and to take other appropriate measures. Before the sharing of data, employers are obliged to notify the infected individuals of the disclosure.

Concerning working from home, where such work entails the processing of the employee's personal data, the Commissioner called on the controllers and processors to respect the principle of integrity and confidentiality and to employ protective measures such as security verification of website links and email correspondence.

The Commissioner also established that where the controllers make the data on infected individuals publicly available, they should ensure that those individuals are not identified or identifiable. The identity of an infected individual may be disclosed only exceptionally, and in such instances, data controllers must apply the data minimisation principle. The Commissioner reacted on several occasions to the public disclosures of data on the health of individuals as well as the broadcasting of images where the identity of the patients could be established.

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

© Law Business Research 2021

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
Business & Human Rights
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
Drone Regulation
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
Healthcare M&A
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
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
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

an LBR business

ISBN 978-1-83862-644-0

© Law Business Research 2021