DATA PROTECTION LAWS OF THE WORLD

Serbia

SERBIA

Last modified 1 February 2019

LAW

In late 2018, Serbia updated its data protection law to better align with the EU General Data Protection Regulation. Serbia enacted a new Data Protection Law on November 9, 2018 (published in the Official Gazette of the Republic of Serbia, no. 87/2018) (New DP Law). The New DP Law entered into force November 21, 2018, but its effective date has been postponed until August 21, 2019 (except for the maintenance of the Central Register of Personal Databases which has already been terminated). The New DP Law was long awaited, as it has been 10 years since the existing law was passed. Its content is largely harmonized with the GDPR.

Until the New DP Law becomes fully applicable on August 21, 2019, the Serbian law governing data protection issues remains the Law on Protection of Personal Data (Official Gazette of the Republic of Serbia, nos. 97/2008, 104/2009, 68/2012 and 107/2012) (DP Law). It became applicable on January 1, 2009, and its current version (incorporating supplements made in 2012) is in force as of November 17, 2012.

DEFINITIONS

Definition of personal data

Under the DP Law and the New DP Law, personal data is any information about a natural person through which the respective person is identified or identifiable (for example, name, address, email address, photo, etc.).

NATIONAL DATA PROTECTION AUTHORITY

The Serbian data protection authority is the Commissioner for Information of Public Importance and Protection of Personal Data (*Poverenik za informacije od javnog znaaja i zaštitu podataka o linosti*) (DPA).

It is seated at Bulevar kralja Aleksandra 15 Belgrade and its website is www.poverenik.rs.

REGISTRATION

The only exception to the New DP Law's postponed implementation is the obligation of the maintenance of the Central Register of Personal Databases by the DPA, which is terminated immediately upon the entering into force of the New DP Law. Notwithstanding the above, the transitional provisions of the New DP Law did not formally terminate the existing obligation for the companies to file the database notifications (probably due to a technical omission), and therefore formally this obligation still applies until August 21, 2019. Under the New DP Law, controllers and processors will only be required to internally maintain the database records and, in certain cases, even that obligation will not apply to companies with up to 250 employees.

Under the DP Law, any person or legal entity that processes personal data in Serbia (and, based on the relevant processing, establishes a database containing personal data) has to report the relevant processing to the DPA.

This database reporting obligation generally consists of two phases. The first phase is to notify the DPA of the intention to

establish a database (at the latest 15 days prior to the intended database establishment date). The second phase is to report to the DPA that the respective database was created (at the latest 15 days from the date of its creation). Both phases are performed by filing prescribed forms with the DPA; the respective forms contain specific data on the data controller (such as its name and address of its registered seat) and on the database itself (for example, the purpose of and legal ground for its establishment, identification of exact processing activities, types of processed data, categories of data subjects, etc.). Any subsequent change to the reported database (for example, change of the initially reported processing activities) has to be reported to the DPA as well, at the latest 15 days from the date when the particular change occurred.

DATA PROTECTION OFFICERS

According to the DP Law, there is no statutory obligation for an entity which processes personal data to have a data protection officer (DPO).

However, according to the New DP Law, controllers and processors will be required to designate the DPO, whose primary tasks will be to ensure compliance with the data processing law and regulations and to communicate with the DPA and the data subjects on all data protection matters. Similar to the GDPR, this obligation applies if the following criteria are met:

- The processing is carried out by a public authority (with the exception of a court performing its judiciary authorizations).
- The core activities of the controller/processor require the regular and systematic monitoring of data subjects on a large scale, or the large-scale processing of special categories of personal *data—eg,* health data or trade union memberships, or criminal convictions / offenses data.

The DPO may be employed or engaged under a service contract, and in any case must have sufficient expert knowledge. A group of companies may appoint a single DPO, provided that he is equally accessible by each company.

Controllers and processors are required to ensure the DPO's independence in the performance of his tasks. This means the following:

- No instructions may be given to the DPO.
- The DPO must report directly to the manager of the controller / processor.
- The DPO may not be dismissed or penalized for performing his or her tasks.

COLLECTION & PROCESSING

The collection and further processing of personal data has to be legitimate and legally grounded, meaning pursuant to the data subject's consent or as specifically provided by law.

Under the DP Law and the New DP Law, there are a few cases when a data subject's personal data may be processed without the data subject's consent (for example, when the processing is necessary for fulfilment of the data controller's statutory obligations or for preparation or realization of an agreement concluded between a data controller and data subject) (Exceptional Cases).

Apart from the Exceptional Cases, prior, informed consent from data subjects is generally required to collect and process personal data, meaning that it has to contain all the information on the particular processing which is explicitly prescribed by the DP Law and the New DP Law (for example, the data subject must be notified of the purpose of the processing, identification of exact processing activities, information on other users of the data in cases when the data controller is not its only user, information on statutory rights of the data subjects in relation to the respective processing, etc.)

Although consent is necessary, it does not automatically mean that any processing, to which a data subject has consented, will be regarded by the DPA as compliant with the DP Law and the New DP Law. There are also other conditions which must be met under the DP Law and the New DP Law (*eg*, the purpose must be legitimate and clearly determined and the type and scope of processed data must be proportionate to the respective purpose).

As opposed to the existing law, which recognizes only hand-signed consent in the written form — creating significant issues in the digital age — the New DP Law explicitly introduces other forms as well, such as online and oral consent, or consent by other clear affirmative action, provided that the controller is able to demonstrate that the data subject has indeed consented.

On the other hand, the conditions for obtaining consent have become much stricter under the New DP Law: similar to the GDPR, consent must be freely given, specific, informed and unambiguous. For example, there is a presumption that consent will not be valid unless separate consents are obtained for different processing operations, where appropriate; and the request for consent—when presented in a written document—must be clearly distinguishable from all other matters, using clear and plain language (meaning catch-all clauses will not be valid. Further, consent will not be considered freely given if the performance of a contract is conditional on the consent to the processing of personal data that is not necessary for its performance.

In addition, one among many important novelties introduced by the New DP Law (and similar to the GDPR), is that it will not apply only to the processing of data carried out by Serbian controllers and processors, but will also apply to the processing of data by controllers and processors based outside of Serbia whose processing activities relate to the offering of goods or services (even if offered for free) or monitoring the behavior of Serbian data subjects within Serbia. As a result, a number of these controllers and processors will need to appoint their representatives in Serbia, to be addressed by the DPA and the data subjects on all issues related to processing.

TRANSFER

The rules on the transfer of personal data, as envisaged by the DP Law, are quite general. Under the respective rules, there are two regimes for data transfer out of Serbia depending on whether the transfer will take place with or without the DPA's prior approval. The determining factor is whether a country to which the data is to be transferred is a member state of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Relevant Convention"). If a country to which the data is to be transferred has signed and ratified the Relevant Convention (such as, for example, the EU countries), the transfer from Serbia is free in the sense that it is not conditional upon prior data transfer approval of the DPA ("Transfer Approval"), otherwise, Transfer Approval is necessary (such as, for example, for a transfer to the US).

However, according to the New DP Law, the data transfer regime has been completely revamped and liberalized, which is a much-welcomed change from the current overly restrictive concept. The New DP Law explicitly applies to both direct and indirect data transfers, unlike the existing law for which it is not fully clear whether it covers indirect transfers at all.

Under the New DP Law, controllers will be entitled to transfer personal data abroad if one of the following conditions (among others) is met:

- Personal data is to be transferred to a country that ratified the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.
- Data transfers are performed to a country included on the EU list or the Serbian government's list of countries providing an adequate level of data protection.
- Data transfers are performed to a country which has a bilateral agreement with Serbia regulating data transfers.
- The transfer is based on the standard contractual clauses prepared by the Serbian DPA.
- The transfer is based on binding corporate rules or a code of conduct approved by the Serbian DPA, or on certificates issued in accordance with the new law.
- The Serbian DPA has issued a specific approval for the transfer to be performed on the basis of an agreement between the data exporter and the data importer.
- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks.

This should create more options for the transfer of data to non-European countries, especially once the DPA prepares the standard contractual clauses, which should be based on those approved by the EU Commission. In addition, it is expected that the process of obtaining the DPA's approval for such transfers will be more efficient, and should be completed within 60 days (currently the procedure often lasts for more than one year).

SECURITY

There are no specific security measures prescribed by the DP Law. It is only generally prescribed that:

- Personal data must be adequately protected from abuse, destruction, loss, unauthorized alterations or access
- Both data controllers and processors are to undertake all necessary technical, human resources and organizational measures to protect data from loss, damage, inadmissible access, modification, publication and any other abuse, as well as

to provide for an obligation of keeping data confidentiality for all persons who work on data processing

Similar to the GDPR, the New DP Law introduces burdensome accountability obligations on data controllers, which are required to "demonstrate compliance." This includes their obligation to all of the following:

- Implement, maintain and update appropriate technical and organizational measures to ensure a level of security appropriate to the risk-taking into account the state of the art, the associated implementation costs etc.
- Have in place certain documentation, such as data protection policies and records of processing activities
- Implement data protection by design and by default
- Conduct a data protection impact assessment for those processing operations that are considered more of risk to the rights and freedoms of individuals

Data protection by design requires the controllers to adopt, as well as maintain and update when needed, appropriate measures—such as pseudonymization, data minimization—which will integrate the safeguards necessary for processing. Data protection by default, on the other hand, requires the controllers to adopt measures so that, by default, only the processing which is necessary for the specific purpose will be possible (*eg*, that, by default, privacy settings on one's social network profile do not make his data public).

BREACH NOTIFICATION

While the DP Law does not impose a duty to notify a data security breach, as explained below, the New DP Law imposes data breach notification obligations that largely track the GDPR. Further, the Law on Electronic Communications ('Official Gazette of the Republic of Serbia', nos. 44/2010, 60/2013, 62/2014 and 95/2018) (EC Law) imposes a duty on entities which perform or are authorized to perform electronic communications' activities (Operators) to notify the Regulatory Agency for Electronic Communications and Postal Services (RATEL) as the competent state authority, of any breach of security and integrity of public communication networks and services, which has influenced their work significantly, and particularly on the breaches which resulted in violation of protection of personal data or privacy of the respective networks/services' users / subscribers.

Nonperformance of this statutory obligation can lead to liability and fines ranging from €4,250 to €16,950 for a legal entity, and in range from €425 to €1,270 for a responsible person in a legal entity. Protective measures may also be implemented: for a legal entity, a prohibition against performing business activities for a duration of up to three years, and, for a responsible person in a legal entity, a prohibition against performing certain duties for a duration of up to one year. According to the New DP Law, the data breach obligations present a significant novelty, as data controllers will generally be required to document each data breach—as well as to notify the DPA of most of them—without undue delay and, when feasible, within 72 hours after becoming aware of the breach. In addition, data processors will have to notify the controllers of the breach without undue delay.

If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller is also required to communicate the personal data breach to the concerned individual as well, without undue delay. However, this does not apply if the controller has implemented appropriate technical and organizational measures, such as encryption that has rendered the relevant data unintelligible to any unauthorized person; or, if the notification would involve disproportionate efforts, a public communication or a similar measure must be made in order to properly inform the individuals.

ENFORCEMENT

The DPA is responsible for the enforcement of the DP Law and the New DP Law. Namely, the DPA is authorized and obliged to monitor whether the law is implemented and it conducts such monitoring both ex officio and based on any complaints it receives. If it establishes, when performing the respective monitoring, that a particular person / entity which processes personal data has acted in contravention to the statutory rules on processing, the DPA shall issue a warning to the particular data controller. It may also issue a decision by which it can, among other things:

- Order the data controller to eliminate the existing irregularities within a certain period of time
- Temporarily forbid particular processing
- Order deletion of the data collected without a legal ground

The DPA's decision cannot be appealed, but an administrative dispute can be initiated against the respective decision before a

competent Serbian court.

Depending on the gravity of the particular misconduct and the data controller's behavior with respect to the same, the DPA can initiate an offense proceeding against the respective data controller before the competent court. The offenses and sanctions for such are explicitly prescribed by the DP Law. The respective sanctions are fines (ranging from €425 to €8,480 for a legal entity and from €42 to €425 for a responsible person in a legal entity). According to the New DP Law, the respective sanctions are fines up to €16,950 for a legal entity and up to €1,270 for a responsible person in a legal entity. Additionally, the DPA is now also able to fine the controllers and processors directly in certain situations, with fines in the amount of €850. Until the adoption of the New DP Law, only the Court of Offences was entitled to impose fines.

Criminal liability is also a possibility since the Serbian Criminal Code prescribes a criminal offense of unauthorized collection of personal data. The prescribed sanctions are a monetary fine (of an amount to be determined by the court) or imprisonment of up to one year. Both natural persons and legal entities can be subject to the respective liability.

Formally speaking, under the Law on Administrative Procedure ('Official Gazette of the Republic of Serbia', nos. 18/2016 and 95/2018), the DPA is also authorized to enforce its orders by threatening a company with a fine of up to 10% of its annual income in Serbia, in case it fails to comply with the order. This is a relatively new option for Serbian authorities that has not yet been tested in practice, to the best of our knowledge.

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law, while in the New DP Law is only mentioned in the context of data subjects' complaint right. The rules on this subject are envisaged by the Law on Electronic Trade ('Official Gazette of the Republic of Serbia', nos. 41/2009 and 95/2013), EC Law (as defined above in the section on Breach Notification), the Law on Advertising ('Official Gazette of the Republic of Serbia', no. 6/2016) and the Consumer Protection Law (Official Gazette of the Republic of Serbia, nos. 62/2014, 6/2016 and 44/2018) (together, the "Relevant Legislation").

In brief, based on the Relevant Legislation, electronic marketing is only allowed if it is covered by an explicit, prior written consent of the person to whom the respective marketing is directed. Additionally, recipients should always be:

- Clearly informed of the identity of the sender and commercial character of the communication (this information should be provided in the Serbian language prior to commencing the marketing)
- Provided with a way to opt out of future marketing messages, at any time and free of charge

ONLINE PRIVACY

There are no specific regulations explicitly governing online privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law and the New DP Law, are, to the extent applicable, relevant for online privacy as well.

On the other hand, it should be noted that the EC Law, as defined in the section on Breach Notification above, introduces rules on the processing of traffic data and location data, which are obligatory for entities which are the Operators (as defined above in the section on Breach Notification) of public communication networks and publicly available electronic communication services. Under these rules, these Operators are allowed to do the following:

- Process traffic data only as long as such data is necessary for a communication's transmission and thus, when such necessity ceases to exist, the Operators are obliged, unless exceptionally (for example, in the case when they have obtained prior consent of the data subjects for using the respective data for marketing purposes), to delete such data or to keep them but only if they make the persons to which the date relates unrecognizable
- Process location data generally only if the persons to which the data relates are made unrecognizable or if they have such persons' prior consent for the purpose of providing them with value added services (but even if such consent does exist, only in the scope and for the time during which the processing is needed for the respective purpose's realization)

Violations are subject to the fines set forth above in the Breach Notification section.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Sanja Spasenovic
Attorney at law in cooperation with Karanovic & Partners
Karanovic & Partners
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.