DATA PROTECTION LAWS OF THE WORLD

Serbia

SERBIA

Last modified 24 January 2018

LAW

The Serbian law governing data protection issues is 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 1 January 2009 and its current version (after supplements made in the course of 2012) is in force as of 17 November 2012.

However, the Ministry of Justice prepared a draft of a new Law on Protection of Personal Data in November 2017, with the general objective of harmonizing the Serbian data protection law with the General Data Protection Regulation ("GDPR"). The public discussion regarding this draft Law commenced on 1 December 2017 and lasts until 15 January 2018. The Serbian Minister of Justice has stated that the expected timeframe for the adoption of this new draft Law and the commencement of its implementation is by May 2018. The final version of this draft law and whether/when exactly it will be adopted and implemented remains to be seen.

DEFINITIONS

Definition of personal data

Under the DP Law, personal data is any information on a natural person based on which the respective person is identified or identifiable (for example, name, address, e-mail 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

Any person or legal entity which 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 (i.e. has to register both the respective database and itself as the data controller).

This database registration obligation generally consists of two phases – the first one is to notify the DPA of the intention to establish a database (at the latest 15 days prior to the intended database establishment date) and the second one 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 (both on-line through the so-called Central Register of the DPA and in hard copy via post); 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 of the registered database (for example, change of the initially registered 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

There is no statutory obligation for an entity which processes personal data to have a data protection officer.

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 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 realisation of an agreement concluded between a data controller and data subject) ("Exceptional Cases").

Apart from the Exceptional Cases, consent is a precondition for legitimate collection and processing of personal data, and must be informed consent, meaning that it has to contain all the information on the particular processing which is explicitly prescribed by the 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.)

Moreover, 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. There are also other conditions which must be met under the DP Law (e.g. the purpose must be legitimate and clearly determined and the type and scope of processed data must be proportionate to the respective purpose).

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).

In addition to the above, it should also be noted that the DPA's position regarding data transfer out of Serbia is very strict, and, thus, the procedure for obtaining the Transfer Approval (which is initiated by a written request submitted to the DPA by the Serbian entity which intends to transfer the data out of the country) is very complex and time consuming and the outcome is rather uncertain.

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, unauthorised alterations or access; and
- both data controllers and processors are to undertake all necessary technical, human resources and organisational 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.

BREACH NOTIFICATION

The DP Law does not impose a duty to notify a data security breach. However, it should be mentioned, for the sake of

completeness, that the Law on Electronic Communications ('Official Gazette of the Republic of Serbia', nos. 44/2010, 60/2013 and and 62/2014) ("EC Law") imposes a duty on entities which are operators of public communication networks and publicly available electronic communication services ("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.

Non performance of this statutory obligation can lead to offence liability and fines ranging from approx. EUR 4,098.00 to EUR 16,393.00 for a legal entity, and in range from approx. EUR 410.00 to EUR 1,230.00 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 (3) years, and, for a responsible person in a legal entity, a prohibition against performing certain duties for a duration of up to one (1) year).

ENFORCEMENT

The DPA is responsible for the enforcement of the DP Law. Namely, the DPA is authorised and obliged to monitor whether the DP 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:

- order the data controller to eliminate the existing irregularities within a certain period of time;
- temporarily forbid particular processing; or
- 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 behaviour with respect to the same, the DPA can initiate an offence proceeding against the respective data controller before the competent court. The offences and sanctions for such are explicitly prescribed by the DP Law. The respective sanctions are monetary fines (ranging from approx. EUR 410.00 to EUR 8,197.00 for a legal entity and from approx. EUR 41.00 to EUR 410.00 for a responsible person in a legal entity).

Moreover, criminal liability is also a possibility since the Serbian Criminal Code prescribes a criminal offence 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 (1) year. Both natural persons and legal entities can be subject to the respective liability.

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law. 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 and 6/2016) (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); and
- 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 on-line privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law, are, to the extent applicable, relevant for on-line 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). Under these rules, the Operators are allowed:

- to 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 unrecognisable; and
- to process location data generally only if the persons to which the data relates are made unrecognisable 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 realisation).

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 Karanovi & Nikoli
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation'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.