DATA PROTECTION LAWS OF THE WORLD

Serbia

SERBIA

Last modified 17 January 2024

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 9 November 2018 (published in the Official Gazette of the Republic of Serbia, no. 87 /2018) (“**DP Law**”). Although the DP Law entered into force 21 November 2018, its effective date was postponed until 21 August 2019 (except for the maintenance of the Central Register of Personal Databases which has already been terminated).

The DP Law was long awaited, as it has been 10 years since the previous data protection law was passed. Its content is largely harmonized with the GDPR. It is now fully effective as of 21 August 2019.

DEFINITIONS

Definition of personal data

Under the 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 značaja i zaštitu podataka o ličnosti*) (“**DPA**”).

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

REGISTRATION

The obligation for the maintenance of the Central Register of Personal Databases by the DPA, which existed under the previous data protection law, was terminated immediately upon the entering into force of the DP Law. Under the DP Law, controllers and processors are only required to internally maintain the database records and only if they have more than 250 employees or if they are involved in certain types of processing or process certain types of personal data (such as, for example, special categories of data or personal data relating to criminal convictions and offences). The latter two conditions are applicable regardless of the number of employees a processer or controller has.

DATA PROTECTION OFFICERS

According to the DP Law, controllers and processors are required to designate a data protection officer (“**DPO**”), whose primary task is 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 / offences 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 to 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 (substantially the same as under the GDPR), there are a few instances where a data subject's personal data may be processed without the data subject’s consent, as follows:

i. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
ii. processing is necessary for compliance with a legal obligation to which the data controller is subject;
iii. processing is necessary to protect the vital interests of the data subject or of another natural person;
iv. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; and
v. processing is necessary for the purposes of the legitimate interest pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a minor (i.e. an individual under the age of 18) (“**Specific Cases**”).

Apart from the Specific Cases, prior informed consent from data subjects is generally required to collect and process personal data, meaning that any request for consent 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 and legal grounds for the processing, information on other recipients of the data in cases when the data is disclosed to entities other than the data controller and information on the statutory rights of the data subjects in relation to the respective processing, etc.).

Although consent is necessary (when none of the Specific Cases is applicable), 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).

In addition to written consent, the DP Law explicitly introduces other forms of consent, such as online consent, oral consent or consent by other clear affirmative action provided that the controller is able to demonstrate that the data subject has indeed consented.

The conditions for obtaining consent have become much stricter under the DP Law than compared to the previous legislation. Similar to the GDPR, consent must be freely given, specific, informed and unambiguous. For example 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 important novelty introduced by the DP Law (and similar to the GDPR), is that it does not apply only to the processing of data carried out by Serbian controllers and processors, but also 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 representatives in Serbia for correspondence with the DPA and the data subjects on all issues related to processing.

TRANSFER

Under the previous data protection law, the DPA’s prior approval was a precondition for a legitimate data transfer whenever a transfer was to be made to any country which had not signed and ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("**Relevant Convention**"). The data transfer regime has now been completely revamped and liberalized under the DP Law, which is a much-welcomed change from the previous overly restrictive concept. The DP Law explicitly applies to both direct and indirect data transfers, unlike the previous law for which it was not fully clear whether it covers indirect transfers at all.

This means that, under the DP Law, substantially the same as under the GDPR, there is a whole set of mechanisms enabling legitimate data transfer out of Serbia. Specifically, subject to circumstances of each particular case, controllers will be entitled to transfer personal data abroad if one of the following situations (among others) occurs:

- Personal data is to be transferred to a country that ratified the Relevant Convention.
- Data transfers are to a country included on the Serbian government’s list of countries providing an adequate level of data protection (EU Countries, other countries which are member states of the Relevant Convention and some other countries such as, for example, Canada (for business subjects only) and Japan).
- 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 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 on the possible risks.

This should create more options for the transfer of data to non-European countries, especially since the DPA has prepared the aforementioned standard contractual clauses, which are adopted and applicable as of 30 January 2020 (keeping however in mind that, under the DP Law, the respective SCC mechanism will be available only when a data importer is a data processor). In addition, when it comes to the process of obtaining the DPA’s aforementioned specific approval for a data transfer, such procedure should be completed within 60 days, as explicitly prescribed under the DP Law.

SECURITY

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

- Implement, maintain and update appropriate technical, organizational and human resources measures to ensure a level of security appropriate to the risk involved by taking into account state of the art and 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 assessments for those processing operations that are likely to cause a high risk to the rights and freedoms of individuals (whereas the specific cases when conducting such assessments is mandatory, are explicitly prescribed as well, e.g. when special categories of personal data are processed on a large scale).

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 implement 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 (e.g. that, by default, privacy settings on one’s social network profile do not make the data public).

BREACH NOTIFICATION

The DP Law imposes data breach notification obligations that largely track the GDPR. Furthermore, the Law on Electronic Communications ('Official Gazette of the Republic of Serbia', no. 35/2023) (“**EC Law**”) imposes a duty on business entities performing electronic communication activities, to notify the Regulatory Body 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 have influenced their work significantly, whereas RATEL, when it assesses that it is in public interest to publish the respective information, is authorized to inform the public on any such breach or to request from the respective business entity to do that. Additionally, if there is a particular risk of breach of public electronic communication networks and services' security and integrity (e.g. risk of endangering safety of personal data), a business entity is obliged to inform users on such risk and if such risk is out of the scope of the measures the operator is obliged to implement, to inform users on possible measures of protection and costs of their implementation.

Nonperformance of this statutory obligation can lead to liability and fines of up to EUR 17,000 for a legal entity, and up to EUR 1,275 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 DP Law, the data breach obligations present a significant responsibility, as data controllers will generally be required to document each data breach as well as to notify the DPA of such breach (if it may result in a risk to the rights and freedoms of individuals) 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 may 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 individual concerned without undue delay. However, this does not apply if the controller has implemented appropriate technical, organizational and human resources measures, such as encryption that has rendered the relevant data unintelligible to any unauthorized person, or has subsequently undertaken measures which ensure that the data breach can no longer lead to consequences for the concerned individual, 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. Namely, the DPA is authorized and obliged to monitor whether the law is implemented and it conducts such monitoring both on its own accord 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 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 fines up to EUR 17,000 for a legal entity and up to EUR 1,275 for a responsible person in a legal entity. Additionally, the DPA is now also able to directly fine controllers and processors in certain situations, with fines in the amount of EUR 850. Prior to the adoption of the 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 offence of unauthorized collection of personal data. The prescribed sanctions are a fine (of an amount to be determined by the court) or imprisonment of up to one year (i.e. up to three years if the offence is committed by a public official / state servant when performing his duties). 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, 95/2018 and 2/2023), 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 option has not yet been tested in practice, to the best of our knowledge.

ELECTRONIC MARKETING

Electronic marketing is only mentioned in the DP Law in the context of the data subjects' right of complaint. The rules on this subject are envisaged by the Law on Electronic Trade ('Official Gazette of the Republic of Serbia', nos. 41/2009, 95/2013 and 52 /2019), EC Law (as defined above in the section on Breach Notification), the Law on Advertising ('Official Gazette of the Republic of Serbia', nos. 6/2016 and 52/2019) and the Consumer Protection Law (Official Gazette of the Republic of Serbia, no. 88/2021) (together, the **"Relevant Legislation").**

In brief, based on the Relevant Legislation, electronic marketing is only allowed if it is covered by an explicit, prior 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.

For the sake of completeness, it should be noted that, under the most recent changes from July 2019 of the aforementioned Law on Electronic Trade, the same principle that previous consent is necessary for electronic marketing, i.e. for electronic commercial communication, remained, but it is also envisaged now that certain types of electronic communication shall not be regarded as commercial communication and, consequently, should not be subject to previous consent. Such exempt communications include (1) providing information which enables direct access to business activities of a particular entity such as information on its e-address or e-mail and (2) providing information on a particular entity's goods, services or business reputation if such information is obtained by research or in some other similar way and if it is provided free of charge.

Finally, it is also envisaged by the new Serbian Consumer Protection Law, as referred to above, which became applicable (with the exception of some of its provisions) on 20 December 2021, that it is forbidden to make phone calls and/or send messages by phone to any individuals/consumers whose phone numbers are inscribed in the register of consumers who do not want to receive calls and/or messages as a part of a promotion and/or sales by phone. This register shall be public in its part relating to the phone numbers and date of the inscription in the register. It should also be noted that, regardless of the inscription in this register, consent of a consumer for direct marketing provided to a particular entity/trader before or after the inscription in the register, remains valid until its withdrawal made in line with the DP Law.

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 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, under which business entities performing electronic communication activities 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, they are obliged to delete the data or to process and keep them in a way that the persons to which the data relates are made unrecognizable, unless in a few explicitly prescribed cases when such obligation does not exist (e.g. if they use the respective data for advertising and services selling purposes on the basis of a data subject's prior consent, to the extent and during the time necessary for the respective purpose).

- Generally process location data 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 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 in Breach notification.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Sanja Spasenović
Attorney at Law in cooperation with Karanović & Partners
Karanovic & Partners
T +381 11 3094 200/ +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.