Dec 2018

Serbia: The Law on Personal Data Protection

On 9 November 2018, the National Assembly of Serbia adopted the long awaited (and debated) new Law on Personal Data Protection[1] ('the Law') which, *inter alia*, seeks to harmonise Serbia's data protection legal framework with the provisions of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). Uroš Popovič, Partner at Bojović Drašković Popović & Partners, provides an overview of the Law and the unique aspects entities operating in Serbia should consider.

Vlajko611/Signature collection/istockphoto.com

Short overview of the previous Law on Personal Data Protection 2008

The Law replaces the previous Law on Personal Data Protection 2008[2] ('2008 DP Law'), after more than ten years of it being in force, a far longer period than predicted and probably intended by the lawmakers. The 2008 DP Law was, according to general opinion, obsolete even at the time of its adoption. Yet, despite its initial inconsistency with the Data Protection Directive (Directive 95/46/EC) as assessed by the European Commission ('Commission'), the 2008 DP Law was amended on only two occasions, and not significantly. The authority competent for supervision of the application of the 2008 DP Law, that is, the Commissioner for Information of Public Interest and Personal Data Protection ('Commissioner'), has pointed out on many occasions the normative deficiencies of the 2008 DP Law, as well as the deficiencies in its application and implementation. Namely, secondary legislation, which was supposed to regulate various matters in a detailed manner, and which was necessary for the implementation of the 2008 DP Law, was never adopted. This primarily refers to the protection of particularly sensitive data. Another major problematic area in practice was the cross-border transfer of personal data, especially when it comes to the transfer of data to non-European

countries. Moreover, the constant increase in the use of modern means of technology, electronic communications, devices for video surveillance, processing of biometric data and the like was not accompanied by appropriate modern legal solutions. Therefore the adoption of a new law was just a matter of time.

Background for adoption of the Law

More recently, and especially when the GDPR came into force, it seemed that the Government completely gave up on the 2008 DP Law, and did not plan to improve its text or make its application easier in practice. However, the enactment of a new law has been postponed several times, often as a result of disagreement between the Commissioner and the Government on the text and form of any new legislation. In March 2017, the Commissioner published a model Law on Personal Data Protection, which was an effort to offer a document to the public which brings the field of data protection closer to the GDPR. In the course of 2017, the Government abandoned the idea of using this model as the basis for the adoption of a new law on personal data protection and soon introduced its own draft version. This represented the culmination of the fact that the dynamic between the Government and the Commissioner was far from ideal.

In any event, the main reason behind the adoption of the finally enacted Law was to achieve harmonisation with EU rules, i.e. ensuring the same level of protection of personal data as in the EU Member States. The introduction of the Law is part of Serbia's obligations as part of its process of accession to the EU.

The Commissioner's stance regarding the text of the Law is that it represents a literal translation of the GDPR, and therefore exhibits a high level of formal compliance with the GDPR, but the practical application in Serbia is highly questionable. We have to point out that the Commissioner, and some participants in the public consultation process which assessed the draft version of the Law, concluded that the subsequent proposal was a non-functional document that does not take into account the specific features of Serbia's legal system.

Further, despite the Commissioner's numerous complaints and suggestions, the Law does not regulate video surveillance, which remains a grey area. The Commissioner has also found Article 40 of the Law to be quite controversial, as it allows the limitation of certain fundamental rights and obligations envisaged by the Law in a rather imprecise manner, and without legal grounds for such limitation. We will have to wait to assess the impact of this provision on such rights until it is implemented.

Overview of the text of the Law

As stated, the Law in general relies heavily on the solutions envisaged by the GDPR, and is significantly more extensive than its predecessor.

Firstly, the Law clearly defines situations when it is applicable. Namely, it applies in cases where the data controller or the data processor with a seat or residence or temporary residence in the territory of the Republic of Serbia carries out personal data processing within the scope of activities that are carried out in the Republic of Serbia, regardless of whether the processing itself is done in the territory. Additionally, regardless of the seat or residence or temporary residence of the data controller or the data processor, the Law applies to cases of data processing if the persons to whom the data relates have residence or temporary residence in the Republic of Serbia. This applies in two cases; in the case of offering goods and services, and in the case of monitoring activities of persons whose activities are carried out in the Republic of Serbia. It is not hard to notice that the Law completely accepted the GDPR principles in this regard.

The provisions for lawful processing are strictly defined under the Law. First of all, data processing is lawful if it is based on the consent of the data subject. The definition of consent is now wider compared to the 2008 DP Law, which only recognised the written form. Now, an affirmative action can be deemed as an expression of the data subject's will. Besides consent, the Law envisages several exceptions, such as situations in which the processing is necessary for the performance of a contract, for compliance with a legal obligation to which the controller is subject, in order to protect the vital interests of the data subject or of another natural person, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Also, the 'legitimate interest' of the data controller or third party as the basis for lawful processing has been introduced by the Law for the first time. This is very important, especially for multinational companies, bearing in mind that in the EU, legitimate interest acts as the legal basis for processing of personal data in a significant number of cases. Regarding this provision, the data subject has the right to oppose such data processing at any time.

The Law maintains the concept that the data subject should be informed of data processing before the processing starts. This obligation is now fully in line with the relevant provisions of the GDPR.

In accordance with the Law, the Commissioner now primarily performs inspection activities, but in addition enjoys many other competencies. Thus, the Commissioner takes appropriate corrective measures, ensures the implementation of the Law, prepares standard contractual clauses regarding the processing of data, approves the provisions of the agreement or contract between authorities regarding the transfer of data, keeps internal records of violations of the Law, reviews issued certificates, performs international cooperation activities, and gives prior opinions regarding risk analysis, etc. In that regard, it should be pointed out that the Commissioner will certainly need additional resources to be made available, including professional staff, in order to perform these duties efficiently.

The Law envisages a range of different options for the protection of data subject rights, which represent a significant step forward. First of all, an objection to the data controller on data processing can be filed, but additionally a data subject may file a complaint with the Commissioner against the decision of the Commissioner if such a decision has not been made within 60 days from the date of submission of the complaint. In such cases an administrative dispute may be initiated. In addition, direct court protection can be achieved independently from other procedures.

The Law clearly stipulates, for the first time, special provisions that apply only to relevant state bodies/authorities, thus ensuring the legality of their actions, and at the same time determining cases where there are exceptions from the general regime. A significant portion of the Law is dedicated to the collection and processing of data by the competent authorities and the many exemptions on which the authorities can now rely, which comprises over 40 articles. Therefore, it seems that the criticism of the Commission on the structure and readability of the Law itself (back then in draft form) was highly justified. Namely, the stand of the Commission was, *inter alia*, that the draft Law was overly complicated and consequently less transparent.

The Law introduces an obligation to conduct an impact assessment prior to the commencement of processing operations, and if the level of risk is high, it recommends requesting an opinion from the Commissioner. Article 54 of the Law replicates the GDPR solution when it comes to cases where such assessments are obligatory. Namely, the data protection impact assessment shall be required:

- in the case of a systematic and extensive evaluation of personal information relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that could produce a legal impact on a natural person; and

- processing of special categories of data, or data relating to criminal convictions and offences, on a large scale or through systematic monitoring of a publicly accessible area.

The impact assessment must contain at least a description of the envisaged processing operations and the purposes of the processing, including, where applicable:

- the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to its purposes; and
- an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address such risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and demonstrate compliance with the Law. Furthermore, the impact assessment must consider the rights and legitimate interests of data subjects and other persons concerned.

The Law now explicitly stipulates the right to compensation, which implies that a person who suffered material or non-material damage due to a violation of the provisions of the Law has the right to financial compensation from the offending data controller or processor.

Another important development of the Law is that the Central Registry of Data Collections has been abolished, and will cease to exist when the Law enters into force. There is no longer any obligation to notify the Commissioner of the intention to establish data collection, nor the obligation to register one. Namely, in the future, the data collections will be kept at the data controller's level, i.e. internally, and in accordance with the Law.

The transfer of data from the Republic of Serbia is now subject to a significantly different and more elaborate regime. Namely, the personal data may be transferred to another country based on its appropriate level of protection, if the controller or processor has provided appropriate safeguards.

Besides the aforementioned, the Law also introduces several other new provisions which clearly have their roots in the GDPR. These include binding corporate rules, certification issuance, obligation for determining persons responsible for personal data protection in specific cases, and codes of conduct, etc. Finally, the applicable provisions regulating penalties and fines are now much more stringent, while the conditions for determination of fines are also introduced.

Next steps

The Law entered into force on 21 November 2018, but its application will start nine months from this date. During this period, relevant by-laws are to be adopted. The only exception when it comes to the application of the Law is the provision which legislates for the termination of the obligation to maintain the Central Registry of Data Collections, since it applies immediately upon its entry into force. The existing data held within the Central Registry of Data Collections is to be archived. The provisions of other laws pertaining to personal data processing are to be harmonised with the provisions of the Law by the end of 2020. It seems that these deadlines are quite optimistic, especially bearing in mind the lengthy period which preceded the adoption of the Law.

Overall, though not ideal, the new Law provides a sound basis for improving the landscape of data protection in the Republic of Serbia. However, it is of course too early to draw any final conclusions about its impact.

Uroš Popović Partner
uros.popovic@bd2p.com
Bojović Drašković Popović & Partners

1. Zakon o zaštiti podataka o ličnosti, Official Gazette of the Republic of Serbia, no. 87/2018.
2. Zakon o zaštiti podataka o ličnosti, Official Gazette of the Republic of Serbia, no. 97/2008, 104/2009, 68/2012, and 107/2012.

RELATED CONTENT

NEWS POST

UK: ICO and DCMS release data protection guidance and notice in case of no-deal Brexit

NEWS POST

EU: EDPB publishes opinion on EU and Japan draft adequacy decision

NEWS POST

USA: CDT issues draft federal privacy bill for discussion

NEWS POST

Canada: Budget Implementation Act 2018 No. 2 receives Royal Assent

NEWS POST

USA: OCR seeks feedback on modifying HIPAA rules