LAW ON PERSONAL DATA PROTECTION

CURRENT SITUATION

The Parliament of the Republic of Serbia enacted a new Law on Personal Data Protection, (RS Official Gazette No 87/2018), (hereinafter: "the new Law") on November 13, 2018. The new Law entered into force on 21 November 2018, to be applied in nine months from the day of entering into force, i.e. on 21 August 2019. The new Law represents a translation of the General Data Protection Regulation 2016/679 (GDPR), without its recitals and with minor specifics reflecting features of the legal system of the Republic of Serbia. Although the new Law has been assessed as a robust document, which does not take into account specifics of Serbia's legal system, the FIC is of the opinion that it may serve as solid legal ground for the promotion of European values in Serbia.

Legal solutions in the new Law clarify ambiguities, which existed in the previous Law on Personal Data Protection. A requirement that consent to the processing of personal data must be provided in writing, which made giving consent on a website impossible, has now been now changed. According to the new Law, consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative act, signifies agreement to the processing of personal data relating to him or her. This provision enables lawful processing of personal data on websites.

The new Law provides for additional legitimate grounds for processing personal data such as the legitimate interest controller or a third party. This legal institute covers situations in which no specific law provides a basis for processing and there are no legitimate reasons to require the data controller to obtain consent from the data subject. What is missing is an official interpretation by the legislator as to what can be considered a legitimate interest, especially because the recitals from GDPR explaining this legal ground for data processing are not incorporated into the new Law.

New rights have been recognised to data subjects such as the right to data portability and the right to objection, while the list of cases where the right to erasure (the right to be forgotten) can be exercised have been expanded. The new Law introduces new obligations to the controller with the aim to protect personal data, such as the obligation to comply with the privacy by design or privacy by default principle and the obligation to perform, in certain situations, data privacy impact assessment and in certain situations the obligation for controllers and processors to appoint data protection officers. Not only controllers, but also processors are responsible for the implementation of organizational and technical measures to secure personal data.

The legal regime applying to the transfer of personal data is now more liberal. Personal data can be transferred to countries which have not ratified the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and to countries which the European Union (EU) considers to provide an appropriate level of personal data protection (third countries) on the ground of contractual clauses approved by the Commissioner for Information of Public Importance and Personal Data Protection ("the Commissioner"). New legal grounds for the transfer of personal data to third countries are codes of conduct and certificates issued by certification bodies. In addition, personal data can be transferred to companies belonging to multinational companies and having registered seats on the territory of third countries, based on binding corporate rules. The new Law introduces the possibility of setting up certification bodies authorized to verify the level of compliance of companies with the new Law and to issue certificates of compliance.

The new Law has abolished the provision of the still applicable law prescribing that the provisions of the Law on Personal Data Protection do not apply to data that are available to everyone and published in public media and various other publications., as well as data that a person capable of caring for his/hers interests, has published about himself/herself. The above should improve data protection regarding telesales (a form of sales widely present in Serbia), so vendors of such companies will no longer be able to contact persons whose data is publicly disclosed on websites or in different publications for the purpose of concluding various types of contracts and selling various types of goods. A data subject can now be contacted for marketing purposes in cases where it can be reasonably expected, due to an existing relationship with data controllers, that they may be contacted (legitimate interest of controllers or third parties) or when a data subject, in the course of establishing a business relationship, gives consent for personal data collection for marketing purposes.

The Commissioner has not yet issued guidance on legitimate interest. The application of the new Law will start soon, while, on the other hand, data controllers might take several months to evaluate the lawfulness of process-

ing based on legitimate interest. It shall be clarified by the Commissioner whether controllers, in the course of evaluating the lawfulness of processing based on legitimate interest shall rely on GDPR recitals, opinions of other European supervisory authorities and opinions of the European Data Protection Board or whether they should expect that the Commissioner shall issue guidance for data controllers in regard to legitimate interest. In addition, the Commissioner shall issue an explanation whether and to what extent it takes into account the practice of European legislators when interpreting the new Law, particularly bearing in mind that there has been no practice in Serbia so far.

COVID-19

There were no special reactions due to COVID-19 epidemic.

The competent ministries and the Commissioner have not issued any guidance in regard to application of the new Law in relation to remote work and measures implemented by companies to prevent spread of SARS-CoV-2 virus in working environment.

POSITIVE DEVELOPMENTS

In November 2019, in accordance with Law on Inspection Supervision, the Commissioner published control lists for controllers - public authorities and private entities. These lists are useful tools for controllers to evaluate level of compliance and prepare to undertake necessary steps and draft documents to comply their business with the Law. In addition, since the Commissioner is obliged to apply control lists in the course regular and mixed supervision over the compliance with the Law, these may be a useful guidance for controller to understand what they should expect in the course of supervision. On January 16, 2020, on the ground of Article 45 of the Law, the Commissioner adopted Decision on Determination the Standard Contractual Clauses (“Commissioner’s Decision”). An integral part of the Commissioner’s Decision is Standard Contractual Clauses (“Clauses”). Clauses must be used by controllers and processors when concluding agreement in writing defining their mutual obligation (transfer of data to processors located in Serbian or in countries which provide adequate level of protection of personal data. These can be used by controllers when transferring personal data to countries which do not provide adequate level of protection of personal data and avoid necessity of issuance the approval by the Commissioner for transfer of personal data.

The Commissioner has continued to participate in public explaining importance of privacy and data protection for citizens and controllers and processors . The Government rendered Decision on List of Countries, Parts of their Territories or One or More Sectors of Certain Activities in these States or of International Organisations for Which It Is Considered that Adequate Level of Protection Personal Data is Provided (“Official Herald RS” No. 55/2019), (“Governmental Decision”). Governmental Decision provides for solution that countries, parts of their territories or one or more sectors of certain activities in these states or of international organisations providing adequate level of protection of personal data are countries which ratified Convention of Council of Europe No.108 and countries, parts of their territories or one or more sectors of certain activities in these states or of international organisation for which the European Commission determined that provide adequate level of protection of personal data.

The new Law introduces the concept of joint controllers - if two or more controllers jointly determine the purpose and method of personal data processing, they are considered joint controllers. The joint controllers referred to in Article 43 of the new Law should determine in a transparent manner the responsibility of each of them for the fulfilment of the obligations prescribed by the new Law, and in particular the obligation regarding the exercise of the rights of data subjects and the fulfilment of their obligations to provide that person with the relevant information on data processing prescribed by the new Law. A data subject may exercise his or her rights prescribed by the new Law by reaching any of the joint controllers.

REMAINING ISSUES

A major issue is that the state does not allocate sufficient funds for the activities of the Commissioner, contrary to commitments outlined in the Action Plan for Chapter 23 (on Judiciary and Fundamental Rights) of the EU acquis, released by the Government of Serbia in September 2015, proclaiming the strengthening of the Commissioner’s resources as its goal.

The other important issue is whether and to which extent the state has the intent to promote values proclaimed in the new Law. The state should put much more efforts in raising data subjects’ awareness of the significance of the abovementioned values by organizing broadcast public debates or public conferences where data subjects can

learn more about their rights contained in the new Law. In addition, the state should exercise its authorities to implement the new Law at state bodies and to align the work of state bodies with measures imposed by the Commissioner.

The new Law does not regulate specific forms of personal data processing, such as video surveillance, processing employees' personal data, and processing for the purpose of scientific and historical research and for statistical purposes. The absence of regulations creates legal uncertainty for controllers that will significantly hamper their ability to conduct business. The provision stipulated in Article 100 of the Law – "provisions of other laws which are related to processing of personal data will be harmonised with provisions of this Law" probably will not be implemented. Except statement of the official of Ministry of Justice that working group has been formed with the task to work towards the harmonisation of other laws with this Law, there have been no public statements by state officials confirming that any further steps have been taken to implemented Article 100 of the Law.

Article 65, paragraph 2, item 2, governing the transfer of personal data to third countries with the application of appropriate safeguards without a specific authorization from the Commissioner prescribes that appropriate safeguards may be provided by standard contractual clauses drafted by the Commissioner, in accordance with Article 45 of the new Law, defining in whole the relationship between the controller and the processor. Reference to Article 45 is not appropriate because GDPR recitals 79 and 81 and Articles 26 and 28 of GDPR do not prescribe that personal data can be transferred to third countries on the ground of contracts whose content is defined by the said articles. Standard contractual clauses which serve as legal ground for transfer of personal data to countries which do not provide adequate level of protection of personal data without a specific authorization from the Commissioner should predominately provide contractual guarantees taken over by controllers and processors to ensure level of protection of personal data recognized by the new Law in the countries of data importers. Controllers and processors are not prevented to supplement standard contractual clauses with provisions stipulated in Article 45. However, the main focus of standard contractual clauses must be in ensuring adequate level of protection of personal data to citizens of the country of exporter. Moreover, Article 65, paragraph 2, item 2 does not prescribe possibility for controllers registered in Serbia to transfer personal data to controllers in third countries on the basis of standard contractual clauses drafted by the Commissioner and without requiring any specific authorization from the Commissioner. This condition is not in line with Article 46, paragraph 2, item c) of GDPR, which prescribes that the appropriate safeguards may be provided for, without requiring any specific authorization from a supervisory authority, with standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93 of GDPR. In addition, Article 77 of the new Law does not provide for the obligation of the Commissioner to draft standard contractual clauses enabling the transfer of personal data to third countries without authorization of the Commissioner, but only the obligation to draft standard contractual clauses by making reference to Article 45 of the new Law.

By the time this edition of the White Book was closed, the Commissioner had not yet consummated its authorisation to prescribe conditions for the issuance of licences to certification bodies.

On July 16, 2020, European Court of Justice ("ECJ") rendered judgement upon request for preliminary ruling from the High Court (Ireland) – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Judgement"). By the Judgement, ECJ invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield and considered Commission Decision 2010/87 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries valid. In the Judgement, it pointed out that monitoring programs of the authorities based on U.S law are not limited to the absolutely necessary extent provided in EU law and such restrictions on data protection are disproportionate under EU law. Furthermore, ECJ determined that US law does not provide efficient legal remedies to EU citizens i.e. "Ombudsperson mechanism does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services." On the other side, as per Standard Contractual Clauses, ECJ stressed that controller and processors (exporters and importers), before personal data being transferred, must check "whether

that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses". In case the level protection in third country is not essential equivalent to EU law, controller is obliged to suspend the transfer or terminate the contract. Such reasoning is based on interpretation of Clauses 4 and 5 of Annex of Standard Contractual Clauses. At the end, ECJ concludes that "competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of all the circumstances of that transfer, that the standard data protection clauses are not or cannot be complied with in that country and that the protection of the data transferred that is required by EU law cannot be ensured by other means, where the data exporter established in the EU has not itself suspended or put an end to such a transfer".

Having in mind the Judgment cited above, it is obvious that formulation in Article 65 paragraph 2 item 2 of the new Law "by standard contracting clauses drafted by the Commissioner in accordance with Article 45 of this Law by which in whole legal relationship between controller and processor in defined" does not understand the substance of transfer of personal data to country which does not provide adequate level of protection of personal data by means of standard contractual clauses – that both controller and controller/processor by providing contractual guarantees must ensure adequate level of protection of personal data of data subjects recognized by the law the country of exporter. For this reason FIC proposes amendment of Article 65 paragraph 2 item 2 of the new Law as follows: "by standard contracting clauses drafted by the Commissioner based on best European practice in regard to transfer of personal data from data controller to data controller/data processor in countries that do not provide adequate level of protection of personal data".

FIC expects that the Government of Republic of Serbia, in the context of the Judgment amends the Governmental Decision and deletes formulation: " United States (limited to Privacy Shield Framework) and that competent bodies provide guidance on impact of the Judgement on transfers of personal data to countries which do not provide adequate protection of personal data.

Article 55, paragraph 10 of the new Law has not been aligned with Article 36, paragraph 5 of GDPR. Concerning the obligation of a data controller to request an opinion of the supervisory authority regarding data privacy impact assessment, Article 36, paragraph 5 of GDPR prescribes that EU Member states may require controllers to consult with, and obtain prior authorisation from the supervisory authority in relation to processing by a controller for the performance of a task carried out in the public interest, including processing in relation to social protection and public health. On the other side, Article 55 paragraph, 10 of the new Law prescribes that the Commissioner may draft and publish on its website a list of processing activities for which its opinion must be requested. Based on authorities provided in Article 55, paragraph 10 of the new Law, the Commissioner has rendered the Decision on processing activities for which data privacy impact assessment must be performed and the opinion of the Commissioner requested (RS Official Gazette RS 45/2019).

GDPR limits the authority of Member States to prescribe cases in which controllers, with regard to data privacy impact assessment, shall consult with, and obtain prior authorization from, the supervisory authority. The cases are limited in relation to processing by a controller for the performance of a task carried out in the public interest, including processing in relation to social protection and public health. The new Law authorizes the Commissioner to determine processing activities for which its opinion must be requested. As a result of the broad authority of the Commissioner to determine processing activities in relation to which its opinion about data privacy impact assessment must be requested, the Commissioner has prescribed that its opinion is required for all processing activities for which data privacy impact assessment is obligatory.

The FIC is of the opinion that such broad legal authorities of the Commissioner and the list of activities in relation to which its opinion about data privacy impact assessment must be requested are not in line with the intent of GDPR to limit Member States' capacities to define the types of processing activities in relation to which an opinion of the supervisory authority about data privacy impact assessment must be requested.

FIC RECOMMENDATIONS

- Provide the Commissioner with better working conditions, equipment and staff to ensure an effective implementation of the new Law. (3)
- Render/amend laws governing specific forms of personal data processing, such as video surveillance, processing employees' personal data, and processing for the purpose of scientific and historical research and for statistical purposes. (3)
- Harmonize Article 55 paragraph 10 of the new Law with Article 36, paragraph 5 of GDPR. (3)
- Amend Article 65, paragraph 2 of the new Law in line with Article 46, paragraph 2, item c of GDPR and ECJ judgement (Case C-311/18) providing for the possibility to transfer personal data from a controller to a controller and a controller to a processor registered in third countries without authorization from the Commissioner on the basis of standard contractual clauses drafted by the Commissioner, based on best European practice. (3)
- Amend Article 77 of the new Law and provide for the obligation of the Commissioner to draft standard contractual clauses for the transfer of personal data from controllers in Serbia to controllers in third countries, applying best European practice. (3)
- Provide an official interpretation of the legislator as to what can be considered a legitimate interest and provide other interpretations for all other issues closely explained in the recitals of GDPR, including impact of ECJ judgement (Case C-311/18) on data transfer of personal data to countries which do not provide adequate level of protection of personal data. (3)
- Amend Decision on List of Countries, Parts of their Territories or One or More Sectors of Certain Activities in these States or of International Organisations for Which It Is Considered that Adequate Level of Protection Personal Data is Provided – deleting formulation "United States (limited to Privacy Shield Framework". (3)
- Issuance of guidance in regard to application of the new Law in relation to remote work and other measures implemented by companies to prevent spread of SARS-CoV-2 virus in working environment. (3)
- Enact conditions for the issuance of licenses to certification bodies by the Commissioner. (3)