

LAW ON PERSONAL DATA PROTECTION

1.08

WHITE BOOK BALANCE SCORE CARD

Recommendations:	Introduced in the WB:	Significant progress	Certain progress	No progress
Provide the Commissioner with better working conditions, equipment and staff to ensure an effective implementation of the new Law.	2009		√	
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.	2019			√
Harmonize Article 55 paragraph 10 of the new Law with Article 36, paragraph 5 of GDPR.	2019			√
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.	2019			√
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.	2019			√
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.	2019			√
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)".	2020			√
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.	2020			√
Enact conditions for the issuance of licenses to certification bodies by the Commissioner.	2020			√

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 spe-

cifics 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 such as manner of providing consent for processing of personal

data, introducing legitimate interest as the ground for processing, recognising new rights for data subject (data portability, right to objection, right not to be subject to automated processing) or improving or improving content recognized by the old Law on Personal Data Protection. The controllers now have to implement additional measures to protect rights of data subjects: when the processing is likely to result in high risks for rights and freedoms of data subjects, controllers have to perform data protection impact assessment and to cooperate with supervisory authority in case organisational and technical measures proposed in data protection assessment cannot mitigate risks for rights and freedoms of data subject to acceptable level. The most important novelty is that controllers and processors have to perform risk assessment to identify risks for information security, personal data and rights and freedoms of data subject and to define and implement adequate organisational and technical measures proportional to risk identified to mitigate risks to acceptable level. In addition, controllers shall demonstrate that they implement adequate organisational and technical measures. Controllers have obligation to report data breach to supervisory authorities and in certain case to inform data subjects affected by data breach. Apart from this, controller must have written data processing agreements with controller processors in which they shall define subject and nature of processing, data which are processed, relation with sub processors, organisational and technical measures applied and manner how controllers verifies their implementations and obligations of the contractual parties in regard to data protection impact assessment and data breach etc. The Law introduces obligations to controllers and processors to appoint data protection officer in certain cases and to establish and maintain records of processing activities.

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.

POSITIVE DEVELOPMENTS

The Commissioner has continued to participate in public explaining importance of privacy and data protection for citizens and controllers and processors and to publish extracts from its opinions on implementation of the Law on its websites. It has published certain explanations in regard to application of legitimate interest as legal ground for processing of personal data. The number of the Commissioner's staff has been increased for 15 full time employees.

REMAINING ISSUES

Despite slight increase of the Commissioner's staff, a major issue is that the state does not allocate sufficient funds for the activities of the Commissioner remains. Such practice is 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. The Commissioner is not the only state body which has obligation to promote implementation of the new Law. In addition, the state bodies should put more efforts to implement the new Law. Lack of implementation of the Law by state bodies creates atmosphere that other addressee of the Law should not implement the Law. Despite the official warnings of the Commissioner that most of the controllers have not appointed data protection officers, many of them still have not fulfilled this obligation.

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 until the end of 2020 is not implemented. The 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 seems to be irrelevant.

From the statements of the officials of the Commissioner and the Ministry of Justice in regard to application of Articles 41 and 50 of the Law, FIC came to conclusion that these provisions seem to be inapplicable. These articles are crucial for implementation of the Law. Namely, the substance of the provisions is that controller must implement adequate organisational and technical measures to ensure and to be able to demonstrate that processing is performed in accordance with the Law. Implementation of adequate organisational and technical measures identification of risks of varying likelihood and severity for security of processing and the rights and freedoms of natural persons. There is no official attitude of both state bodies how controllers shall perform risk assessment to identify risks for security of processing and risks for rights and freedoms of natural persons, i.e., which risk assessment methodologies shall be applied for such assessments. Moreover, there are no sanctions prescribed in the Law for non-compliance with the mentioned provisions. Absence of clear guidance for implementation of these provisions creates enormous

space for improvisation and leads to absence of legal certainty for controllers.

Gap in new Law in regard authorisation of the Commissioner in Law to render standard contractual clauses to enable transfer to controllers located in countries which do not ensure adequate protection of personal data make transfer in these situations impossible. Moreover, referencing to authorisation of the Commissioner to render standard contractual clauses for transfer in internal market in case of standard contractual clauses which serve as ground for transfer of personal data to countries which do not ensure adequate protection of personal data is inadequate. The Ministry of Justice must consider content of the new standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR) issued by European Commission on June 4, 2021.

The Commissioner amended its Decision on processing activities for which data protection assessment shall be performed and request for opinion of the Commissioner must be submitted in terms request for opinion of the Commissioner must be submitted only in cases when a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Such amendment is not in line with Article 55 paragraph 10 of the Law which authorises the Commissioner to render and publish the list of processing activities for which requests of his opinion must be submitted and in line with Article 36 paragraph 5 of GDPR which prescribes that 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 by the controller in the public interest, including processing in relation to social protection and public health. Instead of defining processing activities for which request for his opinion must be submitted due to high risks of such processing activities for rights and freedoms of data subjects, the Commissioner pointed out to situation when measures proposed in data protection assessment cannot mitigate risks in data protection assessment. This solution is not in line with his authorisation in Article 55 paragraph 10 of the 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 certi-

fication bodies. In addition, ambiguities in Article 60 of the new Law in regard to accreditation of the legal entity which supervises implementation of codes of conducts and competencies of the Commissioner makes supervision over implementation of codes of conducts impossible.

FIC expects that the Government of Republic of Serbia, in the context of the judgment of European Court of Justice C-311/18 amends the its 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 Ensured and deletes formulation: "United States (limited to Privacy Shield Framework) and that competent bodies (Commissioner and the Ministry of Justice) provide guidance on impact of this judgement on transfers of personal data to countries which do not ensure adequate protection of personal data.

FIC RECOMMENDATIONS

- Provide the Commissioner with better working conditions, equipment and staff to ensure an effective implementation of the new Law.
- 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.
- Harmonize Article 55 paragraph 10 of the new Law with Article 36, paragraph 5 of GDPR.
- Amend Article 65, paragraph 2 item 2 of the new Law in line with Article 46, paragraph 2, item c of GDPR, ECJ judgement (Case C-311/18) and new standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR) issued by European Commission on June 4, 2021 providing for the possibility for transfer personal data from a controller to a controller and a controller to a processor registered in third countries without authorization from the Commissioner and in internal market on the basis of standard contractual clauses drafted by the Commissioner, based on best European practice.
- 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.
- 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 on 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,
- Provide an official interpretation including interpretation of Articles 41 and 50 of the new Law;
- Provide sanctions for non-compliance with Articles 41 and 50 of the new Law;
- 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 Ensured – deleting formulation "United States (limited to Privacy Shield Framework)".

- 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.
- Enact conditions for the issuance of licences to certification bodies by the Commissioner and resolve ambiguities in Article 60 of the new Law in regard to competences of competent authorities for accreditation of the legal entities supervising implementation of codes of conduct.