CROATIAN GDPR IMPLEMENTATION LAW – MAIN FEATURES AND UNANSWERED QUESTIONS

Maja Šutalo, CIPP/E

Croatian Law on Implementation of General Data Protection Regulation (Cro. Zakon o provedbi Opće uredbe o zaštiti podataka) was passed April 27, 2018, officially published May 3 and entered into force May 25.

The law regulates the supervisory authority's composition, authorities and principles of work, as well as specificities related to administrative fines and to the proceedings in front of supervisory authority and administrative courts. The law also provides some specific provisions related to processing of genetic and biometric data, video surveillance, children's data and processing for statistical purposes. Opposite to the Law on Personal Data Protection, which was brought to implement the goals set by Directive 95/46/EZ, the current law does not provide for specific provisions related to data protection officers. Also, there is no longer a provision that data made available to the public by data subject represent the lawful processing basis itself.

Supervisory authority — composition, powers, proceedings

The supervisory authority remains the Agency for Personal Data Protection (Cro. Agencija za zaštitu osobnih podataka). It consists of a principal, deputies and expert service. Besides common supervisory authorities' powers and duties, the new law prescribes the agency's duty to publish on its website decisions and opinions issued in relation to processing that can cause a high risk for rights and freedoms of individuals. If published opinions or decisions are related to children, their personal data must be anonymised. All other personal data have to be either pseudonymised or anonymised. The agency also publishes on its website final and binding decisions, without anonymisation of the offender's data, if the decision is brought for data breach committed in relation to data of children, special categories of personal data, automated individual decision or profiling. The decision will also be published if it was rendered against a controller/processor who has already committed a breach of the law or GDPR provisions in the past, or whenever the offender is charged with the amount higher than HRK 100,000.00.

Besides typical agency investigatory powers during the inspections, the law prescribes one restriction. If the agency inspects personal data designated as classified ones according to specific regulations, only those agency's officers having a specific certificate can have access to those data during the inspection.

The law also brings specificity in relation to charging fees for the agency's advisory services. While the agency has an advisory function and provides free consultation to data subjects, data protection officers, journalists and public authority bodies, it is, on the other side, authorized to charge for consultations provided to business subjects requesting the consultation within their regular business (law firms, GDPR consultants, etc.). This provision was widely criticized during the public e-consultation. Its retention in the final text of the law was justified by the reasoning that activities of those business subjects will expectedly result in their financial benefit.

There is no legal possibility to file a complaint against the agency's decision related to data subjects' rights, but there is the possibility to file a lawsuit in front of the competent administrative court. If the controller or processor were ordered by the agency to erase certain data, they may request from the administrative court a postponement of that obligation if they prove that they would need to put unreasonable efforts into recovering that data afterwards. Would the court adopt such request, the controller/processor must refrain from any other kind of processing (apart from mere retention) of such data until the court issues final and binding judgement.

Genetic data processing

The law prescribes one derogation from Article 9.2.(a) of the GDPR where the special category of personal data cannot be processed in any case, even not on the basis of data subject's explicit consent. It refers to processing of genetic data for the purpose of calculation of disease occurrence probability or other health aspects of data subjects within activities related to conclusion or execution of life insurance contracts or pure endowment clauses. The controllers bound by this provision are the ones having business residence or providing the services in Republic of Croatia.

Biometric data processing

Both public authority bodies and private entities are allowed to process biometric data if as determined by law it is necessary for the protection of persons, property, classified data or business secrets, taking into account that there are no prevalent interests of data subjects that are opposite to such processing. However, regulating the lawful processing criteria for public authority bodies, the law puts the word "and" between the criterion "if determined by law" and other lawful processing criteria, drawing the possible conclusion that those criteria need to be fulfilled cumulatively in order to process biometric data lawfully. Regulating the lawful processing criteria for private entities, the law puts the word "or" between the criterion "if determined by law" and other lawful processing criteria, indicating that those criteria need to be fulfilled alternatively in order to process biometric data lawfully. There is no publicly available legislation history explaining such difference in the wording. Anyway, it is uncertain how this "cumulative" lawful processing criteria for public authority bodies will work in practice.

The law also prescribes some specific provisions regarding the processing of employees' biometric data with the purpose of forming the working hours evidence and enabling entrance in/exit from the business premises. Such processing is allowed if determined by law or if it is an alternative to another solution for forming working hours evidence and enabling entrance in/exit from the business premises, subject to explicit prior consent given in accordance with the provisions of the GDPR. There were public reactions on this provision in the course of e-consultation, emphasizing that processing of employees' biometric data should not be the "*alternative for another solution*" and that there should be

only one processing solution that would be less intrusive for employees' privacy. However, those suggestions were not taken into account when deciding on the final wording of that provision.

Video surveillance

The law prescribes specific provisions regarding video surveillance of business premises, residential buildings and public areas. There is a general rule that data subjects must be informed of video surveillance properly at least at the moment of entering the monitored area. The controller/processor performing video surveillance activities is due to establish automated evidence of access to data collected by it. That evidence must record approaching time, place and persons. Furthermore, any person given the authority by controller/processor to access the data collected through video surveillance can process those data strictly in accordance with the determined purpose of collecting. Breach of the provisions related to video surveillance can result in a specific penalty prescribed by the law in the amount up to HRK 50,000.00. The law also puts a strong emphasize on the storage limitation principle prescribing that personal data collected in the course of video surveillance activities cannot be kept longer than six months unless the data is necessary for the purposes of judicial, arbitral or similar proceedings.

Other provisions — Children's data and statistical purposes

The law explicitly confirmed that processing of children's data with residence in Republic of Croatia in relation to information technology is lawful if the child is at least 16, without further derogations and/or setting lower age limits.

State bodies performing official state statistics activities are not required to enable data subjects to exercise the right to access, right to rectification, right to limitation of processing or right to objection in cases when the exercising of those rights would threaten or disable the state body in performing the statistic activities.

Administrative fines

State administrative bodies, other state bodies and units of local and regional self-government are excluded from the charging of administrative fines. On the other side, an administrative fine can be charged from the legal entity performing public authorities or legal entity providing public services, but in the amount which cannot put in danger performance of such public authorities/services.

Public e-consultations brought a discussion about what should be deemed "other state body," which would be excluded from the charging of administrative fines. The clear definition of that term was not adopted under the explanation that several laws in Republic of Croatia define "other state bodies" in different ways and with different scopes, due to which there can be no strict and preliminary definition of it.

The agency is authorized to render a decision on installment payment of administrative fine. If there is no installment payment ordered in particular case, total amount of fine becomes due upon the expiry of 15 days from the day the decision became final and binding.

Conclusion

The law sets quite clear frames for the agency's powers and duties, for its composition and proceedings it undertakes. On the other side, the legislator did not use a number of the possibilities that the GDPR left to national laws, such as derogations related to data protection officers, specific rules on certification procedure, codes of conduct, etc. However, the rules that are brought, especially the ones related to biometric data processing and exclusion of state bodies from administrative fines, are completely new in comparison to previous Law on Personal Data Protection. Having in mind possible ambiguities implied in those rules, it will be interesting to monitor how they will be applied in practice.

Author

Maja Šutalo, CIPP/E