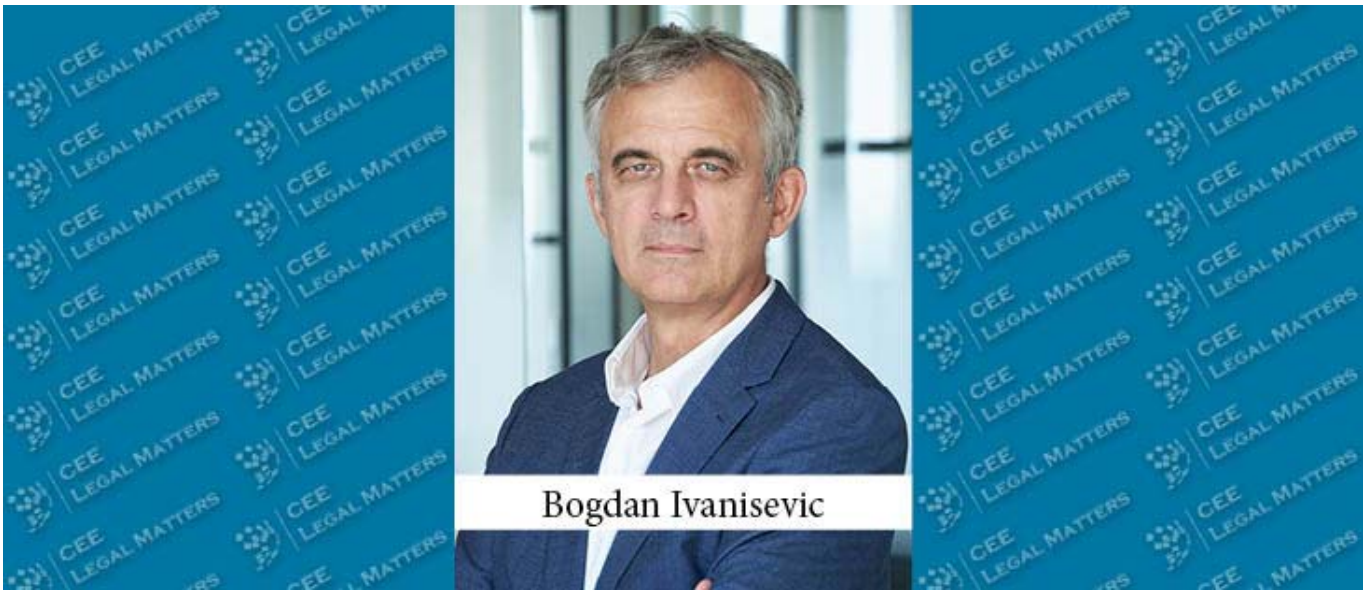
New Legal Framework on the Horizon for Cybersecurity in Serbia

BDK ADVOKATI / 13 NOVEMBER 2024 /



By the spring of 2025, Serbia will likely have a new cybersecurity law. The law is aimed at bringing the national legal framework in line with that in Europe as expressed in the *NIS2 Directive* (2022). The draft law that passed the process of the public consultation in 2023 and underwent minor additional changes in 2024 (Draft Law) nevertheless differs from NIS2 in certain important aspects.

The existing *Information Security Act* in Serbia was enacted in January 2016, half a year before the adoption of *Directive (EU) 2016/1148* (NIS Directive). In 2019, the Serbian legislature amended the 2016 law to align it with the NIS Directive.

Compared to the existing law from 2016, the Draft Law comprises a wider range of entities that are subject to the law and introduces new obligations concerning risk assessment, frequency of compliance checks, mandatory protection measures, and incident reporting. The Draft Law distinguishes – as does the *NIS2 Directive* – between two relevant categories of the operators of information and communications technology (ICT) systems: “essential” and “important” entities.

The Draft Law attaches much lesser significance to the distinction between essential and important entities than does the *NIS2 Directive*. In particular, the Draft Law does not submit the essential entities more than the important ones to proactive and intrusive supervision by the cybersecurity authorities. The only differences under the Draft Law are the following ones: mandatory compliance checks are to take place twice a year for the essential entities and once a year for the important ones, and essential entities can be fined for certain violations of the law with RSD 2 million (approximately EUR 17,000), whereas the maximum fine for violations by the important entities is twice as low.

Generally, in comparison to the *NIS2 Directive*, the Draft Law has stricter formal requirements, but the enforcer's hand is significantly lighter than under the EU directive.

Internal acts and compliance checks: The Draft Law requires more frequent compliance checks than the *NIS2 Directive* and the implementing laws adopted by early October 2024 in the EU member states (Croatia, Belgium, Latvia, and Italy specifically).

Incident handling: A dozen provisions in the draft law put high demands before the operators of ICT systems. Even the early incident notification needs to be detailed, and intermediate reports are mandatory and frequent. Companies and organizations falling within the scope of the law are also required to submit annual statistical reports to the authorities and to report on near misses that amount to serious threats to the security of ICT systems.

Protection measures: The Draft Law sets forth 34 organizational, people, technological, and physical controls to protect ICT systems. The number of explicitly enumerated cybersecurity risk-management measures in the *NIS2 Directive* (Article 21) and the recently enacted cybersecurity laws in the member states is far lower, and the measures are formulated at a higher level of generality.

Where the Draft Law departs from the *NIS2 Directive* the most is on the issue of sanctions for the failure to meet the law's requirements.

Under the directive, the competent authorities of the EU member states may order temporary suspension of certification or authorization concerning part or all of the services provided, or activities carried out, by the essential entity. Authorities may also prohibit temporarily individuals at the chief executive officer or legal representative level in the essential entity from exercising managerial functions in the entity. Neither of these measures is included in the Draft Law in Serbia.

As stated above, the Draft Law sets the maximum fines for violations of the law at EUR 17,000 for the essential entities and half that amount for the important entities. These are negligible figures compared to those under the *NIS2 Directive*: the bigger of a maximum of at least EUR 10 million or a maximum of at least 2% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, and EUR 7 million or 1.4% respectively in the case of important entities.

Assuming, then, that the final version of the cybersecurity law will lack provisions that ensure meaningful deterrence, the strongest motive for Serbian companies to comply with the law will be not the fear of its enforcement but the interest in protecting themselves from cyber threats and incidents.

By Bogdan Ivanisevic, Senior Partner, BDK Advokati

This article was originally published in Issue 11.10 of the CEE Legal Matters Magazine. If you would like to receive a hard copy of the magazine, you can subscribe here.