Srbija: Novi zakon o informacionoj bezbednosti (Deo I)
Serbia: New Law on Information Security (Part I)

JPM | PARTNERS

Srbija: Novi zakon o informacionoj bezbednosti (Deo I)/Serbia: New Law on Information Security (Part I)

Publisher: JPM | Partners
Delta House, 8a Vladimira Popovića street
www.jpm.law
Authors: Ivan Milošević ,Partner
Design and prepress: JPM | Partners

Skupština Republike Srbije usvojila je novi Zakon o informacionoj bezbednosti 22. oktobra 2025. godine. Usvajanje novog Zakona o informacionoj bezbednosti je korak napred ka usklađivanju srpskog zakonodavstva sa pravnim tekovinama EU u oblasti informacione bezbednosti.

Novi zakon predviđa jasnije definicije pojmova, uvodi nove termine, povećava broj operatera IKT sistema i propisuje strožije obaveze za operatere IKT sistema. Operaterima IKT sistema je ostavljeno 18 meseci da usklade svoje IKT sisteme sa novim zakonom.

The Serbian Parliament adopted the new Law on Information Security on October 22, 2025. The adoption of the new Law on Information Security is a step forward in aligning Serbian legislation with the acquis in the field of information security.

The new law provides for clearer definitions of terms, introduces new terms, increases the number of ICT systems operators, and imposes stricter obligations on ICT systems operators. ICT system Operators are left 18 months to comply with their ICT systems with the new law.

I Definicije pojmova

Novi Zakon o informacionoj bezbednosti („Novi zakon“) predviđa jasne definicije osnovnih pojmova.

Rizik se definiše kao mogućnost gubitka ili poremećaja izazvanog incidentom i izražava se kao kombinacija veličine takvog gubitka ili poremećaja i verovatnoće da se incident dogodi. Ova novina uvodi uzročnost u definiciju rizika, što ukazuje da se u proceni rizika procenjuju verovatnoću gubitka ili poremećaja i incidenta ili verovatnoće događaja rizika.

Dalje, definicija upravljanja rizicima obuhvata sve integrativne i naredne faze u upravljanju rizicima u celini - identifikaciju, analizu, procenu i uspostavljanje sistema kontrole ublažavanja rizika koji obuhvata planiranje, organizaciju i usmeravanje mera zaštite kako bi se osiguralo da se rizici izbegnu, ublaže ili ostanu u propisanim i prihvatljivim granicama.

.

I Definitions of terms

The new Law on Information Security (“the New Law”) provides for clear definitions of basic terms.

The risk is defined as the possibility of loss or disruption caused by an incident and is expressed as a combination of the magnitude of such loss or disruption and the likelihood of the incident occurring. This novelty introduces causality in the definition of the risk, implying that both the probability of loss or disruption and the probability of incident or risk event shall be assessed in risk assessment.

Further, the definition of risk management covers all integrative and subsequent phases in the risk management in its entirety - identification, analysis, assessment, and establishment of a risk mitigation control system that covers the planning, organization, and direction of protective measures to ensure that risks are avoided, mitigated, or remain within prescribed and acceptable limits.

Definicije rizika i upravljanja rizicima u prethodnom Zakonu o informacionoj bezbednosti („Prethodni zakon“) bile su nejasne i apstraktne, ostavljajući prostor za različita tumačenja. Samo najistaknutiji stručnjaci sa jakim akademskim iskustvom bili su u stanju da pravilno protumače definicije u Prethodnom zakonu, dok su, s druge strane, takve definicije ostavljale ogroman prostor za (ne)namerna pogrešna tumačenja koja su rezultirala izbegavanjem ispunjenja obaveza procene i tretmana rizika i pravnom nesigurnošću.

Novi zakon uvodi definicije novih pojmova koristeći formulacije iz NIS Direktive 2 („NIS 2“). Ovaj koncept omogućava stvaranje boljeg pravnog okvira za odgovor na nove pretnje sajber bezbednosti i uvođenje novih ili strožijih obaveza (novim) operaterima u rastućoj digitalnoj ekonomiji. Na primer, novi zakon uvodi definicije „usluge računarstva u oblaku“, „usluge data centra“, „pružaoca upravljanih usluga“, „pružaoca upravljanih bezbednosnih usluga“, „sistema naziva domena (DNS)“, „pružaoca DNS usluga“ itd. Iz ugla informacione bezbednosti, položaj ovih pravnih lica bio je potpuno nedefinisan u nacionalnom zakonodavstvu, a usklađenost IKT sistema ovih subjekata prepuštena je nejasnim politikama i procedurama akreditacije bez sankcija ili kontrole.

The definitions of the risk and the risk management in the previous Law on Information Security (“the Previous Law”) were vague and abstract, leaving space for different interpretations. Only the most prominent experts with a strong academic background were able to interpret the definitions in the Previous Law properly, while, on the other side, such definitions left enormous space for (un)intentional misinterpretations, resulting in avoidance of fulfillment of obligations to assess and treat the risk and legal uncertainty.

The New Law introduces definitions of new terms using formulations from NIS Directive 2 (“NIS 2”). This concept enables the creation of an improved legal framework for response to new cybersecurity threats and imposing new or stricter obligations on (new) operators in the growing digital economy. For example, the new Law introduces definitions of “cloud computing service”, “data centre service”, “managed service provider”, “managed security service provider”, “domain name system (DNS)”, “DNS service provider“, etc. The position of these entities from an information security aspect was completely undefined in the national legislation, and the compliance of ICT systems of these entities was left to vague policies and accreditation procedures with no sanctions or control.

Novi zakon daje netačne definicije nekih pojmova. Na primer, IKT proces je definisan kao skup aktivnosti koje se sprovode u svrhu kreiranja, razvoja, korišćenja i održavanja IKT proizvoda ili IKT usluga. Pravilna definicija bi bila skup procedura koje sadrže aktivnosti..., jer odsustvo procedura koje definišu aktivnosti može dovesti do improvizacije, a što može da rezultira odsustvom jasnih pravila za kreiranje, razvoj, korišćenje i održavanje IKT proizvoda ili IKT usluga.

Dalje, novi zakon uvodi obaveze za istraživačke organizacije jer ove organizacije mogu da obavljaju važne poslove za razvoj novih proizvoda i usluga u digitalnoj ekonomiji.

The New Law provides for inaccurate definitions of some terms. For example, the ICT process is defined as a set of activities carried out for the purpose of creating, developing, using, and maintaining ICT products or ICT services. The proper definition would be a set of procedures containing activities..., as the absence of procedures defining activities could result in improvisation, resulting in the absence of clear rules for creating, developing, using, and maintaining ICT products or ICT services.

Further, the New Law introduces obligations for research organisations, as these organizations can play important tasks for the development of new products and services in the digital economy.

II Nove obaveze za (nove) operatere

Novi zakon prati metodologiju utvrđenu NIS 2 i daje definiciju operatera IKT sistema od posebnog značaja, pri čemu su ovi operateri dalje podeljeni na operatere prioritetnih IKT sistema i operatere važnih IKT sistema.

Operateri prioritetnih IKT sistema upravljaju IKT sistemima u sledećim sektorima: energetika, saobraćaj, bankarstvo i finansije, zdravstvo, upravljanje vodom za piće i otpadnim vodama, digitalna infrastruktura, nuklearna energija, usluge poverenja, usluge upravljanja sadržajem, DNS usluge, elektronske komunikacije, državni organi, pružaoci usluga upravljanja, pružaoci usluga upravljanja bezbednošću, tačka razmene interneta, operateri kritične infrastrukture itd.

Imajući u vidu da Novi zakon predviđa obaveze za većinu segmenata poslovanja u navedenim sektorima, operateri iz ovih sektora bi trebalo da obrate posebnu pažnju na to da li je njihova aktivnost predmet Novog zakona.

II New obligations for (new) operators

The New Law follows methodology established by the NIS 2 and provides a definition of special importance ICT systems operators, whereby these operators are further divided into priority ICT systems operators and essential ICT systems operators.

The priority ICT systems operators manage ICT systems in the following sectors: energy, traffic, banking and finance, health, drinking water and waste water management, digital infrastructure, nuclear energy, trust services, content management services, DNS services, electronic communications, state bodies, managed service providers, managed security service providers, internet exchange point, operators of critical infrastructure, etc.

Having in mind that the New Law imposes obligations for most of the business segments of the said sectors, and for this reason, operators from these sectors shall pay special attention to the fact whether their activity is subject to the New Law.

Nadalje, Novi zakon ovlašćuje ministarstvo nadležno za informacionu bezbednost da podzakonskim aktom odredi subjekte kao operatere prioritetnih IKT sistema i to u slučajevima kada prekid u radu IKT sistema ili poremećaj u funkcionisanju IKT sistema:

1. može imati značajan uticaj na javnu bezbednost, nacionalnu bezbednost ili javno zdravlje;
2. može izazvati značajan sistemski rizik, posebno u sektorima u kojima poremećaj može imati prekogranične posledice.

Further, the New Law authorises the ministry competent for information security to enact a by - law to determine entities as priority ICT systems operators in cases where an interruption in the operation of ICT systems or a disruption in the functioning of ICT systems:

1. may have a significant impact on public safety, national security, or public health;

2. may cause significant systemic risk, particularly in sectors where a disruption may have cross-border effects.

Operateri važnih IKT sistema upravljaju IKT sistemima u sledećim sektorima:

- poštanske usluge,
- upravljanje otpadom,
- upravljanje ambalažnim otpadom,
- proizvodnja i snabdevanje hemikalijama,
- proizvodnja, prerada i distribucija hrane u segmentu veleprodaje i industrijske proizvodnje i prerade,
- proizvodnja računara, elektronskih i optičkih proizvoda,
- proizvodnja električne opreme, proizvodnja mašina i opreme,
- proizvodnja motornih vozila, prikolica i poluprikolica i proizvodnja ostale transportne opreme,
- proizvodnja medicinskih sredstava i proizvodnja in vitro dijagnostičkih medicinskih proizvoda,
- usluge informacionog društva u skladu sa Zakonom o elektronskoj trgovini,
- proizvodnja, trgovina i transport oružja i vojne opreme,
- svemirske usluge koje se oslanjaju na zemaljsku infrastrukturu, posebno aktivnosti koje uključuju upravljanje kontrolnim centrima, objektima za praćenje i komunikaciju i pružanje usluga lansiranja, istraživačke institucije i itd.

The essential ICT systems operators manage ICT operators in the following sectors:

- postal services,
- waste management,
- package waste management,
- production of supply of chemicals,
- production, processing, and distribution of food in the wholesale and industrial production and processing segment,
- production of computers, electronic and optical products,
- production of electrical equipment, production of machinery and equipment,
- production of motor vehicles, trailers, and semi-trailers, and production of other transport equipment,
- production of medical devices and production of in vitro diagnostic medical products,
- information society services as defined by the Electronic Commerce Law,
- production, trade, and transport of weapons and military equipment,
- space services that rely on ground infrastructure, particularly activities involving the management of control centers, tracking and communication facilities, and the provision of launch services, research institutions, etc.

Pravna i fizička lica koja ne spadaju u operatere prioritetnih IKT sistema prema kriterijumima za određivanje operatera prioritetnih IKT sistema spadaju u operatere važnih IKT sistema.

Ministarstvo nadležno za informacionu bezbednost poseduje isto ovlašćenje u pogledu donošenja podzakonskog akta kojim se definišu dodatni operateri važnih IKT sistema na osnovu istih kriterijuma koji se primenjuju na operatere prioritetnih IKT sistema.

Novi zakon predviđa značajne nove obaveze za sve operatere IKT sistema od posebnog značaja (pored postojećih prema Prethodnom zakonu):

a) donošenje akta o proceni rizika;
b) donošenje akta o bezbednosti, na osnovu akta o proceni rizika;
c) dostavljanje obaveštenja CERT-u o svakom incidentu koji značajno ugrožava bezbednost IKT sistema, bez odlaganja;
d) prijavljivanje izbegnutih incidenata koji predstavljaju ozbiljnu pretnju.

Procena rizika se sprovodi, uzimajući u obzir nivo izloženosti riziku, veličinu i značaj operatera, verovatnoću nastanka incidenta i njegovu ozbiljnost, kao i njegov potencijalni društveni i ekonomski uticaj.

Legal and natural persons who do not fall under the priority ICT systems operators according to the criteria for determining the priority ICT system operators fall under of essential ICT systems operators.

The ministry competent for information security possesses the same authorisation with respect to rendering by a by-law defining additional essential ICT systems operators using the same criteria applied to the priority ICT systems operators.

The New Law imposes substantial new obligations for all ICT systems of special importance operators (besides the existing ones according to the Previous Law):

a) to render the risk assessment act;
b) to render the Security Act, based on the Risk Assessment Act;
c) to provide notifications to CERT, without delay, about any incident that significantly undermines the security of ICT systems;
d) to report near misses that pose a serious threat.

A risk assessment is carried out, taking into account the level of exposure to risk, the size and importance of the operator, the likelihood of an incident occurring and its severity, as well as its potential social and economic impact

Izveštaj o proceni rizika treba da se pripremi u skladu sa opštom metodologijom za procenu rizika u prioritetnim i bitnim IKT sistemima od posebnog značaja, koju treba da usvoji organ ili organizacija u kojoj se sprovode aktivnosti Nacionalnog CERT-a.

Ključne nove bezbednosne mere koje će se primenjivati na sve IKT od posebnog značaja su sledeće:

a) prikupljanje podataka o novim pretnjama za IKT sisteme;
b) primena adekvatnih mera za sprečavanje curenja informacija;
c) primena adekvatnih mera u oblasti pružanja usluga u oblaku;
d) praćenje IKT sistema, uključujući testiranje sistema na ranjivosti, radi identifikacije ranjivosti i potencijalnih pretnji koje mogu iskoristiti te ranjivosti;
e) ograničavanje pristupa veb stranicama koje bi potencijalno mogle ugroziti bezbednost IKT sistema;
f) redovno kreiranje rezervnih kopija podataka, softvera i sistema putem odgovarajućih načina za razmenu podataka;
g) mere koje obezbeđuju kontinuitet poslovanja u vanrednim situacijama, na način kako je definisano strategijom i Planom kontinuiteta

The risk assessment report is to be prepared in accordance with the general methodology for risk assessment in priority and essential ICT systems of special importance, which is to be adopted by the authority or organization where the activities of the National CERT are carried out.

The key new security measures to be applied to all ICT systems of special importance are as follows:

a) collection of data on new trends for ICT systems;
b) application of adequate measures for the prevention of leakage of information;
c) application of adequate measures in the field of provision of cloud services;
d) monitoring ICT systems, including testing of the system for vulnerabilities to identify vulnerabilities and potential threats that may use such vulnerabilities;
e) restriction of access to web pages that could potentially compromise the security of ICT systems;
f) regular creation of backups of data, software, and systems through appropriate data exchange means;
g) measures that ensure the continuity of business operations in emergency situations, as defined by the strategy of the Business Continuity Plan;

h) usvajanje dokumenata kojima se definišu procedure za proveru adekvatnosti mera zaštite;
i) korišćenje rešenja za višefaktorsku autentifikaciju ili kontinuiranu autentifikaciju, za zaštitu glasovne, video i tekstualne komunikacije, kao i bezbednih komunikacionih sistema u vanrednim situacijama unutar IKT sistema operatera.

Mere zaštite IKT sistema sprovodiće se u skladu sa procenjenim rizicima kako bi se obezbedila adekvatna zaštita sistema i minimizirao uticaj potencijalnih incidenata.

Vlada će doneti podzakonski akt kojim se definišu mere zaštite za prioritetne i važne IKT sisteme.

h) adoption of documents defining procedures for verifying the adequacy of protection measures;
i) the use of multi-factor authentication or continuous authentication solutions, for the protection of voice, video, and text communications, as well as secure communication systems in emergencies within ICT system operators.

The implementation of ICT system protection measures shall be carried out in accordance with assessed risks to ensure adequate system protection and minimize the impact of potential incidents.

The Government shall render a law defining the protection measures for priority and essential ICT systems.

III Obaveze izveštavanja

Novi zakon predviđa obavezu IKT operatera od posebnog značaja da obaveste nadležne regulatore o incidentima.

Dalje, u slučaju incidenta koji može prouzrokovati ili prouzrokuje štetan uticaj na pružanje i korišćenje usluga, IKT operateri su dužni da blagovremeno obaveste korisnike kojima pružaju usluge o incidentu putem odgovarajućih komunikacionih kanala, kao i o merama koje korisnici mogu preduzeti i koristiti za ublažavanje ili otklanjanje štetnih posledica incidenta.

IV Rok za usklađivanje poslovanja

IKT operateri od posebnog značaja su dužni da donesu Akt o proceni rizika i Akt o bezbednosti informacija u roku od 18 meseci od dana stupanja na snagu Novog zakona.

III Reporting obligations

The New Law provides for the obligation of the ICT systems of special importance to notify competent regulators of incidents.

Further, in the event of an incident that may cause or is causing a harmful impact on the provision and use of services. ICT operators are obliged to promptly inform users to whom they provide services about an incident through appropriate communication channels, as well as about measures that users can take and use to mitigate or eliminate the harmful consequences of the incident.

IV Deadline for compliance

The ICT systems of special importance operators are obliged to render the Risk Assessment Act and the Information Security Act within 18 months upon the day of entering the New Law into force.

V Sankcije

Inspektori za informacionu bezbednosti mogu da:

i) izreknu meru zabrane korišćenja postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost u određenom roku;
ii) pokrenu postupak pred nadležnim sudom ili drugim nadležnim organom radi utvrđivanja privremene mere zabrane obavljanja upravljačkih funkcija licu koje u ime nadziranog subjekta vrši rukovodeće poslove, ako je njegovim postupanjem onemogućeno usaglašavanje sa Novim Zakonom i naloženim merama ili postupak za izricanje prekršajnih kazni.

Kancelarija za informacionu bezbednost vrši stručni nadzor i kontroliše:

i) adekvatnost procenjenih rizika s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj;
ii) nivo bezbednosti tehnoloških postupaka i tehničkih sredstava koje operator IKT sistema od posebnog značaja upotrebljava radi primena mera zaštite;

V Sanctions

Information security inspectors may:

i) impose the measure of ban of use of procedures and technical means that endanger or compromise information security within defined deadline;
ii) initiate proceedings before the competent court or other competent authority to determine a temporary measure of ban to a person who performs managerial duties on behalf of the supervised entity to hold executive positions, if their actions have prevented compliance with the New Law and the imposed measures or procedure for imposing misdemeanour fines

The Information Security Office performs expert supervision and controls:

i) the adequacy of assessed risks considering the degree of exposure to risk, the size of the operator, the likelihood of an incident occurring and its severity, as well as its potential social and economic impact;
ii) the level of security of technological procedures and technical means used by an ICT system operator of special importance for the implementation of protective measures;

iii) odgovarajuće sprovođenje procesa provere usklađenosti primenjenih mera IKT sistema sa aktom o bezbednosti; iv) primenu preporuka i mera u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost.

Kancelarija za informacionu bezbednost nalaže da nadziranom subjektu da postupi u skladu sa njenim nalazom u roku od 8 dana. Ukoliko nadzirani subjekt ne postupi u skladu sa nalazom, Kancelarija za informacionu bezbednost o tome obaveštava nadležne inspektore.

iii) proper implementation of the process of verifying the compliance of applied ICT system measures with the security act; iv) the application of recommendations and measures in case of incidents that significantly threaten information security.

The Information Security Office instructs the supervised entity to act in accordance with its findings within 8 days. If the supervised entity does not comply with the findings, the Information Security Office notifies the relevant inspectors.

Autor/Author

Ivan Milošević

Partner

E: ivan.milosevic@jpm.law

JPM | PARTNERS
8a Vladimira Popovića,
DELTA HOUSE, V Floor
11070 Belgrade, Serbia
T:+ 381/11/207-6850
E: office@jpm.law

www.jpm.law