

Ministarstvo informisanja i telekomunikacija

Pariska 7, Beograd

Beograd, 24.08.2023.

**Predmet: Komentari i sugestije organizacije Partneri za demokratske promene Srbija na Nacrt zakona o informacionoj bezbednosti**

Poštovani,

Organizacija Partneri za demokratske promene Srbija (Partneri Srbija) pozdravlja napore Ministarstva informisanja i telekomunikacija da nacionalni zakonodavni okvir uskladi sa pravnim okvirom Evropske unije i trendovima razvoja IKT u svetu. Takođe, pohvalna je i inicijativa Ministarstva da kreira sveobuhvatnu radnu grupu koja se sastoji od stručnih lica iz javnog, privatnog i civilnog sektora, kao i da obezbedi da proces javne rasprave bude otvoren, participativan i dostupan svim zainteresovanim licima. Kako bi se to u potpunosti ostvarilo, neophodno je da javnosti budu dostupne sve informacije i akti u vezi rada na Nacrtu. Trenutno to nije slučaj sa Rešenjem o imenovanju Radne grupe, te apelujemo na Ministarstvo da ovaj dokument učini dostupnim na svojoj veb stranici, kao i na portalu eKonsultacije.

U nastavku teksta dajemo načelne komentare na Obrazloženje i Nacrt zakona o informacionoj bezbednosti, kao i sugestije za izmene pojedinih odredaba Nacrta:

- Ovaj Nacrt predviđa efikasne mehanizme zaštite podataka državnih organa, građana i privrede od sajber napada i reagovanja na incidente. Međutim, bitno je istaći da u našoj zemlji problem ne leži samo u nedostatku kvalitetnih propisa, već u nedovoljnoj primeni istih. Mali broj adekvatno obučениh ljudi za inspeksijski nadzor, kao i nedostatak kapaciteta za otkrivanje i pravovremeno reagovanje na opasnosti i incidente često sprečavaju doslednu primenu zakona. Dodatno zabrinjava i dosadašnja praksa nesankcionisanja subjekata i pojedinaca za neadekvatno rukovođenje podacima. Stoga, iako je unapređenje zakonodavnog okvira važno, ono

ne sme ostati izolovana mera. Potrebno je uložiti napore i resurse u izgradnju kapaciteta nadležnih organa i obezbediti doslednu primenu ovog Zakona.

- U obrazloženju je navedeno da za sprovođenje ovog Zakona nije potrebno obezbediti dodatna sredstva iz budžeta Republike Srbije. Imajući u vidu da Nacrt predviđa osnivanje novih tela, obuku novog i unapređenje postojećeg ljudskog kadra, kao i sveobuhvatno unapređenje sistema informacione bezbednosti, postavlja se pitanje da li je finansijski aspekt primene ovog zakona adekvatno isplaniran, odnosno da li se svrha Zakona istinski može i ostvariti.
- Potrebno je pravilno označiti NIS 2 Direktivu u Obrazloženju, imajući u vidu da se trenutno navedena oznaka "2022/2055" odnosi na standarde bezbednosti parking oblasti za kamione u Evropskoj Uniji. Precizno navođenje relevantnih dokumenata je neophodan preduslov da se javnost adekvatano informiše o svim aspektima potebnim za efikasno učešće u procesu javne rasprave.
- **Član 11, Akt o proceni rizika IKT sistema od posebnog značaja** – Potrebno je dopuniti član tako što će se propisati rok u kom je operator dužan da donese predmetni akt;
- **Član 12, Akt o bezbednosti IKT sistema od posebnog značaja** – Potrebno je dopuniti član tako što će se propisati rok u kom je operator dužan da donese predmetni akt;
- **Član 13, Obaveštavanje o incidentima** – Potrebno je dopuniti **stav 7** člana, tako što će nakon: „Ako je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti, organ kome je upućeno obaveštenje o incidentu, obaveštava nadležno javno tužilaštvo, odnosno ministarstvo nadležno za unutrašnje poslove“ dodati: „bez odlaganja, a najkasnije u roku od 24 sata od prijema obaveštenja o incidentu“. Potrebno je dopuniti **stav 8** člana, tako što će se nakon: „Ako je incident povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje odbrane ili nacionalne bezbednosti Republike Srbije, organ kome je upućeno obaveštenje o incidentu obaveštava organe koji su nadležni za poslove odbrane ili nacionalne bezbednosti“ dodati: „bez odlaganja, a najkasnije u roku od 24 sata od prijema obaveštenja o incidentu“. Potrebno je dopuniti **stav 9** člana, tako što će se nakon: „Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura, to obaveštenje prosleđuje Ministarstvu unutrašnjih poslova i ministarstvima nadležnim za sektore kritične infrastrukture u skladu sa zakonom koji uređuje kritičnu infrastrukturu“ dodati: „bez odlaganja, a najkasnije u roku od 24 sata od prijema obaveštenja o incidentu“. Propisivanjem predloženih rokova obezbediće se veća sigurnost i operativnost prilikom reagovanja na incidente, a ovaj propis će se dodatno uskladiti sa direktivama Evropske unije.
- **Član 18, Telo za koordinaciju poslova informacione bezbednosti** – Potrebno je dopuniti stav 1 člana, tako što će se nabrojanim organima čiji predstavnici ulaze u

sastav Tela za koordinaciju poslova informacione bezbednosti dodati i Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. Uključivanjem Poverenika u Telo za koordinaciju, osigurava se prisustvo stručnjaka iz oblasti prava na zaštitu podataka o ličnosti, posebno imajući u vidu da je ovo pravo među prvima na udaru u slučaju incidenata, te da su posledice po prava i slobode lica u ovakvim slučajevima dalekosežne. Takođe, predstavnici Službe Poverenika mogu dodatno doprineti radu Tela svojim razumevanjem balansa između zaštite informacija i prava na slobodan pristup informacijama od javnog značaja. Takođe, uključivanje Poverenika olakšava razmenu informacija između organa nadležnih za upravljanje informacijama. Ovo bi dovelo do efikasnijih rešenja i bolje koordinacije u slučaju potrebe za reagovanjem na incidente koji ugrožavaju informacionu bezbednost.

- **Član 24, Saradnja na nacionalnom nivou** – Potrebno je dopuniti **stav 1.** i **stav 2.** ovog člana, tako što će se među organe sa kojima Nacionalni CERT neposredno saraduje, odnosno održava sastanke, navesti i Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, iz razloga navedenih u predlogu za dopunu člana 18.
  
- **Član 28, Zaštita dece pri korišćenju informaciono komunikacionih tehnologija** Potrebno je dopuniti **stav 3.** člana, tako što će se nakon: „U slučaju da navodi iz prijave upućuju na postojanje krivičnog dela, na povredu prava, zdravstvenog statusa, dobrobiti i/ili opšteg interesa deteta, na rizik stvaranja zavisnosti od korišćenja interneta, prijava se prosleđuje nadležnom organu radu postupanja u skladu sa utvrđenim nadležnostima“ dodati: „bez odlaganja, a najkasnije u roku od 24 sata od prijema prijave“.
  
- **Član 39, član 40, član 41, član 42, Kaznene odredbe** – Trebalo bi detaljnije regulisati visine novčane kazne za specifična kršenja, imajući u vidu da su trenutno propisani kazneni rasponi za niz različitih činjenja ili nečinjenja veoma visoki (na primer, član 39. predviđa novčanu kaznu u rasponu od 50.000,00 do 2.000.000,00 dinara). Dodatno preciziranje bi obezbedilo viši nivo predvidivosti i pravne sigurnosti, a i omogućilo nadležnim organima da brže i efikasnije donose odluke o kaznama, jer imaju jasne smernice o tome koje kazne su primerene za koje vrste kršenja.