SKUPŠTINA CRNE GORE
Predsjedniku Andriji Mandiću

Obavještavamo Vas da iz procedure povlačimo amandmane 1, 2, 3, 4, 5, 6 na Predlog Zakona o informacionoj bezbjednosti (koji su podnijeti pod brojem akta: 08-040/24-2525/4) i podnosimo nove amandmane (EPA:246, broj akta:10-2/24-1)

Poslanici:

Slađana Kaluđerović Slađana Kaluđerović

Bogdan Božović Bogdan Božović

AMANDMAN 1

U članu 5 stav 2 briše se.

AMANDMAN 2

U članu 6 poslije stava 1 dodaje se novi stav koji glasi:

"Agencija iz stava 1 ovog člana predstavlja jedinstvenu nacionalnu kontakt tačku za informacionu bezbjednost i sarađuje sa jedinstvenim nacionalnim kontakt tačkama drugih država."

OBRAZLOŽENJE AMANDMANA 1 I 2

U skladu sa čl. 8 stav 3 NIS2 direktive, države članice su obavezne da imenuju jedinstvenu kontakt tačku (Single Point of Contact - SPOC) za sajber bezbjednost kako bi se osigurala efikasna prekogranična saradnja, koordinacija i razmjena informacija sa drugim državama članicama EU, Evropskom komisijom i Evropskom agencijom za sajber bezbjednost (ENISA). Predlog da Agencija za sajber bezbjednost preuzme ovu ulogu temelji se na nekoliko ključnih argumenata koji proističu iz zahtjeva Direktive i institucionalnog okvira EU i prakse drugih država:

Član 8 stav 4 NIS2 direktive propisuje da SPOC mora osigurati funkciju povezivanja radi prekogranične saradnje i koordinacije između nadležnih tijela države članice i relevantnih institucija EU. Imajući u vidu da Agencija za sajber bezbjednost, kako je definisana predlogom Zakona o informacionoj bezbjednosti "obavlja poslove zaštite mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata, osim organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata, uključujući stručni nadzor nad primjenom mjera informacione bezbjednosti kod tih organa i drugih subjekata", ima institucionalne kapacitete i mandat za upravljanje sajber prijetnjama i incidentima kod ključnih i važnih subjekata iz različitih sektora. Dakle, isključivo Agencija posjeduje direktne operativne nadležnosti nad ključnim i važnim subjektima u različitim sektorima kao što su energetika, zdravstvo, digitalna infrastruktura i saobraćaj, što je ključno za osiguranje interoperabilnosti i koordinisanog odgovora na sajber incidente. Prema zahtjevima NIS2 direktive, jedinstvena kontakt tačka mora osigurati prekograničnu saradnju ne samo između država članica, već i između sektora unutar države, čime se omogućava efikasan, pravovremen, jedinstven i centralizovan odgovor na incidente i prijetnje. Dakle, Agencija za sajber bezbjednost, svojim operativnim kapacitetima i postojećim zakonodavnim mandatom, već sarađuje sa sektorima kao što su energetika, saobraćaj, zdravstvo i digitalna infrastruktura, što je presudno za koordinaciju na nacionalnom nivou i osiguranje usklađenosti sa zahtjevima Direktive.

Drugo, član 8 stav 5 NIS2 direktive zahtijeva da SPOC i nadležna tijela imaju adekvatne resurse za efikasno i djelotvorno izvršavanje svojih zadataka. Ovo podrazumijeva tehničku ekspertizu, operativne procedure i infrastrukturu za reagovanje na složene sajber incidente, što je neophodno za efikasno obavljanje funkcije SPOC-a. Kako je propisano članom 40 stav 3, Agencija je nadležna za proaktivno skeniranje mrežnih sistema, upravljanje incidentima i sprovođenje stručnog nadzora nad primjenom mjera sajber bezbjednosti kod ključnih i važnih subjekata. Nasuprot tome, Ministarstvo javne uprave ima širi mandat upravljanja javnom administracijom, a nadležno je za poslove zaštite mrežnih i informacionih sistema isključivo organa državne uprave, što može ograničiti fokus, dostupnost resursa i brzinu reakcije na sajber incidente, rezultirajući negativnim posljedicama za ključne i važne sektore.

Analiza prakse država članica Evropske unije jasno pokazuje da većina njih za SPOC imenuje nadležna tijela koja su specijalizovana za nadzor informacione bezbjednosti kod ključnih i važnih subjekata, u skladu sa zahtjevima NIS2 direktive. Ova praksa proističe iz potrebe za tehničkom ekspertizom, operativnim kapacitetima i institucionalnom nadležnošću koje su ključne za usklađivanje sa zahtjevima člana 8 Direktive.

Na primjer, Francuska je imenovala Nacionalnu agenciju za sigurnost informacionih sistema (ANSSI) kao jedinstvenu kontakt tačku. ANSSI ima direktnu nadležnost za nadzor i zaštitu mrežnih i informacionih sistema u ključnim sektorima poput energetike, zdravstva i digitalne infrastrukture, omogućavajući efikasnu koordinaciju između ovih sektora i prekograničnu saradnju s institucijama EU. Slično, u Njemačkoj, Savezni ured za bezbjednost informacionih tehnologija (BSI) funkcioniše kao SPOC sa jasnim mandatom nad mjerama informacione bezbjednosti kod ključnih i važnih subjekata.

Takođe, SPOC u Srbiji je Kancelarija za informacionu bezbjednost, u Hrvatskoj Ured Vijeća za nacionalnu bezbjednost, u Italiji – Nacionalna Cybersecurity Agencija.

Kako Agencija, svojim fokusom na ključne i važne subjekte, ima kapacitet da implementira standardizovane procedure i protokole koji omogućavaju razmjenu informacija u realnom vremenu i harmonizovan odgovor na sajber prijetnje, njeno imenovanje za SPOC predstavlja optimalno rješenje za usklađivanje sa NIS2 direktivom i unapređenje interoperabilnosti i sposobnosti države da odgovori na prekogranične i međusektorske izazove u sajber prostoru.

AMANDMAN 3

Član 7 mijenja se i glasi:

"Ovaj zakon ne primjenjuje se na organ državne uprave nadležan za poslove odbrane, Vojsku Crne Gore, Agenciju za nacionalnu bezbjednost, organizacionu jedinicu organa državne uprave nadležnog za unutrašnje poslove koja vrši policijske poslove, Skupštinu Crne Gore, sudstvo i Centralnu banku Crne Gore, kao i na podatke čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka."

OBRAZLOŽENJE

Prema članu 6, stav 35 NIS2 direktive, definicija javnih upravnih entiteta ("public administration entity") izričito isključuje parlamente, sudstvo i centralne banke. Ovo pravilo usmjereno je na očuvanje autonomije ovih ključnih institucija i sprečavanje potencijalnog uticaja izvršne vlasti na njihove funkcije, što je od suštinskog značaja za demokratski poredak i vladavinu prava. Međutim, član 7 Predloga zakona o informacionoj bezbjednosti Crne Gore predviđa izuzeća isključivo za organe državne uprave nadležne za poslove odbrane, Vojsku Crne Gore, Agenciju za nacionalnu bezbjednost i policiju, ali ne uključuje parlament, sudstvo, niti centralnu banku, što nije u skladu sa zahtjevima NIS2 direktive. Od kritičnog značaja je propisivanje ove odredbe Zakonom o informacionoj bezbjednosti, koji je lex specialis za oblast informacione bezbjednosti, naročito imajući u vidu da je članom 2 Predloga Zakona predviđeno "da su po ovom zakonu obavezni da postupaju državni organi, ministarstva i drugi organi uprave, organi jedinica lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, pravna lica koja vrše javna ovlašćenja (u daljem tekstu: organi), privredna društva **i druga pravna lica i fizička lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemom (u daljem tekstu: drugi subjekti)**." Ovakva formulacija ostavlja prostor za ekstenzivnu primjenu Zakona i na subjekte koji nisu predviđeni Direktivom, stoga je ovaj amandman ključan kako za usklađenost sa odredbama Direktive, a tako i za **očuvanje nezavisnosti i specifične funkcije institucija koje su od strateškog značaja za svaku državu članicu EU**. Samim tim, ignorisanje ove odredbe NIS 2 Direktive može ugroziti nezavisnost ključnih institucija poput sudstva i centralne banke, čije su funkcije direktno vezane za nacionalnu bezbjednost i finansijsku stabilnost. Imajući u vidu da se novim Zakonom, osim mjera informacione bezbjednosti, propisuju i nadzorna ovlašćenja izvršne vlasti, uključivanje ovih institucija u opšti zakon o informacionoj bezbjednosti, osim što ne bi bilo u skladu sa Direktivom, narušilo bi princip podjele vlasti, jer bi omogućilo izvršnoj vlasti, kroz nadzor i regulaciju informacionih sistema, da vrši kontrolu nad zakonodavnom i sudskom granom vlasti. Takva situacija bi predstavljala **ozbiljan rizik za autonomiju parlamenta, sudstva i centralne banke, institucija koje su garant demokratskog poretka, vladavine prava i ekonomske stabilnosti.** Bezbjednost informacionih sistema ovih institucija se mora osigurati kroz njihove interne mehanizme, koji su posebno prilagođeni funkcijama koji obavljaju, a ne kroz opšti zakon o informacionoj bezbjednosti i nadzor izvršne vlasti.

AMANDMAN 4

U članu 42 uvodna rečenica stava 2 mijenja se i glasi:

"Odbor za bezbjednost i odbranu Skupštine Crne Gore, na osnovu javnog poziva koji se objavljuje najkasnije 180 dana prije isteka mandata Predsjedniku Savjeta, odnosno neposredno po razrješenju,".

U stavu 2 tačka 4 mijenja se i glasi:

"Odbor za bezbjednost i odbranu Skupštine Crne Gore, na osnovu javnog poziva koji se objavljuje najkasnije 180 dana prije isteka mandata članu Savjeta, odnosno neposredno po razrješenju."

OBRAZLOŽENJE

Predlogom zakona je predviđeno da Ministarstvo javne uprave predlaže Predsjednika Savjeta Agencije, čime bi se mogla potencijalno kompromitovati nezavisnost Agencije, a postoji i opravdana zabrinutost da bi razvojne politike Ministarstva mogle uticati na prioritizaciju i odlučivanje unutar Agencije, što bi moglo dovesti do sukoba interesa. Ministarstvo koje promoviše tehnološki razvoj možda neće adekvatno ocjenjivati rizike koji su povezani sa sajber bezbjednošću, narušavajući time nepristrasnost u upravljanju sajber rizicima.

Takođe, predlogom zakona je predviđeno i da jednog člana Savjeta predlaže Agencija iz reda zaposlenih.

Ovim amandmanom se u izbor Predsjednika Savjeta i jednog člana Savjeta direktno uključuje Odbor za bezbjednost i odbranu, kao tijelo važno za nacionalnu infrastrukturu, čije bi učešće omogućilo bolje razumijevanje specifičnih rizika i potreba u kontekstu pitanja iz oblasti bezbjednosti i odbrane Crne Gore i njenih građana, jer informaciona bezbjednost u savremenom društvu nije samo oblik nacionalne bezbjednosti, već presjek svih drugih oblika bezbjednosti u kojima informacione tehnologije zauzimaju važno mjesto.

AMANDMAN 5

U članu 58 dodaje se stav 2 i glasi:

"U postupku nadzora, nadzornici i inspektori su obavezni da precizno definišu tražene informacije i jasno navedu svrhu zahtjeva za pristupom informacijama, kod zahtjeva za:

1) informacijama neophodnim za procjenu mjera za upravljanje rizikom u oblasti sajber bezbjednosti koje je usvojio dotični subjekat, uključujući dokumentovane politike;
2) pristup podacima, dokumentima i informacijama neophodnim za obavljanje njihovih nadzornih zadataka;
3) dokazima o primjeni politika sajber bezbjednosti, kao što su rezultati bezbjednosnih revizija koje je sproveo kvalifikovani revizor i za odgovarajućim osnovnim dokazima."

OBRAZLOŽENJE

NIS2 Direktiva u članu 33 eksplicitno zahtijeva da nadležni organi, prilikom korišćenja svojih ovlašćenja za nadzor, jasno navedu svrhu zahtjeva i preciziraju informacije koje se traže, posebno u vezi sa povredama bezbjednosnih mjera.

Član 32 i stav 33 stav 3 navodi obavezu nadležnih organa da, prilikom korišćenja svojih ovlašćenja prema tačkama (e), (f) i (g) iz stava 2 (što uključuje zahtjeve za informacijama, pristup dokumentima, i dokaze o sprovođenju politika sajber bezbjednosti), jasno navedu svrhu zahtjeva i precizno definišu tražene informacije.

Međutim, Predlog zakona pokazuje da su ovlašćenja nadzornih organa ekstenzivno propisana članovima 54 i 67, koji propisuju obaveze nadziranih subjekta da u postupku nadzora, inspektoru/nadzorniku "omoguće pristup prostoru, računarskoj opremi i uređajima, kao i da bez odlaganja stave na uvid ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora". Imajući u vidu senzitivnost podataka u posjedu državnih organa, ključnih i važnih subjekata i potencijalne zloupotrebe nadzornih ovlašćenja, specifična obaveza jasnog navođenja svrhe i traženih informacija u svakom nadzornom postupku je ključno za osiguranje transparentnosti i integriteta nadzora.

NIS2 Direktiva, kao pravni okvir za harmonizaciju sajber bezbjednosti u Evropskoj uniji, naglašava potrebu za transparentnim postupcima nadzora kako bi se osigurala proporcionalnost i zaštita prava subjekata, uključujući zaštitu podataka i poslovne povjerljivosti. Iz tog razloga, član 32 i 33 Direktive zahtijevaju da se za svaku nadzornu aktivnost jasno definišu tražene informacije i obavezno obrazloži njihova svrha, kako bi se izbjegli prekomjerni ili nepotrebni zahtjevi koji bi mogli narušiti prava nadziranih subjekata ili dovesti do neopravdanog administrativnog opterećenja. Ovim pristupom se smanjuje rizik od zloupotreba ovlašćenja i osigurava balans između efikasnog nadzora i zaštite osnovnih prava svih uključenih strana.

Na ovaj način predloženim amandmanom nacionalni pravni okvir se usklađuje sa evropskim standardima u oblasti sajber bezbjednosti, čime se doprinosi povećanju povjerenja u regulatorne procese i jačanju međunarodne saradnje. Implementacijom ovakvih mjera, Crna Gora šalje jasnu poruku o svojoj posvećenosti izgradnji otpornog i transparentnog sistema informaciono-komunikacionih tehnologija, što je ujedno i jedan od ključnih ciljeva NIS2 Direktive. Usvajanjem ovog amandmana, Crna Gora se pozicionira kao odgovoran akter u razvoju sajber bezbjednosti, predano ispunjavajući obaveze proistekle iz procesa harmonizacije sa evropskim zakonodavstvom.