



Crna Gora  
Ministarstvo finansija i socijalnog staranja

Adresa: ul. Stanka Dragojevića 2,  
81000 Podgorica, Crna Gora  
tel: +382 20 242 835  
fax: +382 20 224 450  
www.mif.gov.me

Br: 02-03-17353/1

Podgorica, 13.12.2021. godine

**MINISTARSTVO JAVNE UPRAVE, DIGITALNOG DRUŠTVA I MEDIJA**  
**-n/r ministarke, gospođe mr Tamare Srzentić-**

Poštovana gospodo Srzentić,

Na osnovu Vašeg akta broj: 01-039/21-5007 od 06.12.2021. godine, kojim se traži mišljenje na *Predlog strategije sajber bezbjednosti Crne Gore 2022-2026, i prateći Akcioni plan za 2022-2023. godinu*, Ministarstvo finansija i socijalnog staranja daje sljedeće

**MIŠLJENJE**

Na tekst Predloga strategije i pripremljeni Izvještaj o analizi uticaja propisa sa aspekta uticaja na poslovni ambijent, nemamo primjedbi.

Uvidom u Izvještaj o analizi uticaja propisa navedeno je da je za implementaciju aktivnosti koje proizilaze iz Predloga akcionog plana za 2022-2023. godinu, za sprovođenje Strategije sajber bezbjednosti Crne Gore 2022-2026, potrebno obezbijediti finansijska sredstva okvirno u iznosu od 3,50 mil.€.

Kako je navedeno u dopisu, za realizaciju aktivnosti iz Akcionog plana za 2022. godinu sredstva su sadržana u predloženom Zakonu o budžetu za 2022.godinu. S obzirom da su kao nosioci aktivnosti prepoznati budžetski korisnici i da se obezbjeđivanje sredstava iz budžeta odnosi na narednu fiskalnu godinu, kako bi se obezbijedila nesmetana implementacija Strategije bilo bi potrebno da se nosioci aktivnosti formalno izjasne o obezbijedenim sredstvima za sprovođenje istih, iz svoje nadležnosti, u okviru planiranih sredstava Predlogom Zakona o budžetu Crne Gore za 2022. godinu.

*S tim u vezi, ukazujemo takođe na član 40 Zakona o budžetu i fiskalnoj odgovornosti kojim se uređuje da ugovorene obaveze moraju biti usklađene sa planiranim i odobrenim sredstvima, kao i da je budžetski izvršilac odgovoran za zakonito korišćenje sredstava odobrenih potrošačkoj jedinici.*

Shodno navedenom, Ministarstvo finansija i socijalnog staranja, u načelu, nema primjedbi na Predlog strategije i prateći Akcioni plan za 2022-2023. godinu, s tim da će sredstva za aktivnosti iz Akcionog plana čija je realizacija planirana za 2023.godinu biti predmet razmatranja prilikom izrade Zakona o budžetu Crne Gore za 2023. godinu. Ističemo, da će iznos sredstava potreban za realizaciju predmetne Strategije u narednim godinama biti predmet razmatranja prilikom procesa izrade godišnjeg Zakona o budžetu.

S poštovanjem,



**MINISTAR**  
mr. Miloško Spajić

IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA	
PREDLAGAČ PROPISA	Ministarstvo javne uprave, digitalnog društva i medija
NAZIV PROPISA	Predlog Strategije sajber bezbjednosti Crne Gore 2022-2026, sa Akcionim planom za period 2022-2023. godine
<b>1. Definisane probleme</b> <ul style="list-style-type: none"> <li>- Koje probleme treba da riješi predloženi akt?</li> <li>- Koji su uzroci problema?</li> <li>- Koje su posljedice problema?</li> <li>- Koji su subjekti oštećeni, na koji način i u kojoj mjeri?</li> <li>- Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)?</li> </ul>	
<p style="text-align: center;"><b>1. Koje probleme treba da riješi predloženi akt?</b></p> <p>Predlog Strategije sajber bezbjednosti Crne Gore 2022-2026, sa Akcionim planom za period 2022-2023. godine, pretenduje da ispuni definisane strateške ciljeve: unapređenje kapaciteta za sajber odbranu i sistem upravljanja kriznim situacijama izazvanim sajber napadima/incidentima širih razmjera, uspostavljanje sistema zaštite kritične informatičke infrastrukture, osnaživanje odgovora na sajber kriminal i harmonizacija sistema zaštite podataka, unapređenje procesa edukacije u oblasti sajber bezbjednosti u javnom i privatnom sektoru i jačanje javno-privatnog partnerstva i međunarodne saradnje.</p> <p style="text-align: center;"><b>2. Koji su uzroci problema?</b></p> <p>Napadi na sajber prostor Crne Gore s godinama eksponencijalno rastu<sup>1</sup>, postaju kompleksniji i s većim posljedicama po infrastrukturu, funkcionisanje javne uprave, naročito u dekadi digitalizacije društva, i građane - korisnike informaciono-komunikacionih tehnologija i e-servisa. Pojavom hibridnih prijetnji, koje sve više zamjenjuju konvencionalne metode ratovanja, sajber prostor postaje još više značajan, odnosno pogodan za kanalisanje široke lepeze hibridnog ratovanja. Drugim riječima, neminovna digitalizacija društva otvara vrata zlonamjernim akterima, koji u kontinuitetu pokušavaju da izvrše maliciozne sajber napade, radi ostvarenja različitih ciljeva. U takvom ambijentu, dostizanje definisanih strateških ciljeva postaje imperativ.</p> <p style="text-align: center;"><b>3. Koje su posljedice problema?</b></p> <p>Posljedice problema su: krivična djela izvršena u ovom domenu, objavljivanje osjetljivih podataka državnih i drugih institucija, kompromitovanje i onesposobljavanje ključnih informacionih sistema na kojima su bazirani poslovni i društveni procesi, kompromitovanje reputacije kako državnih, privatnih institucija, tako i pojedinaca.</p> <p style="text-align: center;"><b>4. Koji su subjekti oštećeni, na koji način i u kojoj mjeri?</b></p> <p>Oštećeni su brojni subjekti - kako institucije, tako i pojedinci.</p>	

<sup>1</sup> Prema godišnjim izvještajima CIRT-a o incidentnim situacijama na internetu, tokom 2017. godine CIRT-u je prijavljeno ukupno 532 incidenta, tokom 2018. godine 537, tokom 2019. godine 604, a tokom 2020. godine 641 incident.

Način na koji su oštećene institucije su: narušavanje ugleda objavljivanjem lažnih informacija ili krađom informacija, onemogućavanjem rada informacionih sistema na kojima se zasnivaju biznis procesi, kao i procesi od nacionalne bitnosti (npr. nacionalni telekomunikacioni sistemi, sl).

Mjera u kojoj su oštećeni na skali od 1 do 5, gdje je 1 minimalno oštećenje, a 5 maksimalno, odnosno onemogućenje obavljanja većeg dijela biznis funkcija u okviru državnih i privatnih institucija.

### 5. Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)?

Bez realizacije aktivnosti iz Akcionog plana koji doprinose postizanju strateških ciljeva iz Strategije sajber bezbjednosti Crne Gore 2022-2026, a koje podrazumijevaju i unaprijeđivanje legislativnog okvira, odnosno zadržavanjem „status quo“ opcije sajber prostor Crne Gore ostavljamo nezaštićenim, a nacionalno zakonodavstvo neusklađenim sa smjernicama i direktivama naših međunarodnih partnera (NATO, EU, OEBS) u ovoj oblasti što može imati dugoročne negativne posledice. Na primjer, uspješan sajber napad na kritične informatičke infrastrukture bi mogao da zaustavi isporuku električne energije i telekomunikacionih usluga, vodosnabdijevanje, transportnih servisa i sl, što bi u zavisnosti od brzine odbrane odnosno oporavka funkcionalnosti moglo da ima za posledicu višemilionsku finasijsku štetu po budžet i privredne aktivnosti u Crnoj Gori.

## 2. Ciljevi

- **Koji ciljevi se postižu predloženim propisom?**
- **Navesti usklađenost ovih ciljeva sa postojećim strategijama ili programima Vlade, ako je primjenljivo.**

### 1. Koji ciljevi se postižu predloženim propisom?

Implementacijom Strategije sajber bezbjednosti Crne Gore 2022-2026. i realizacijom aktivnosti iz Akcionog plana za period 2022-2023. namjeravaju se dostići sledeći ciljevi: unapređenje kapaciteta za sajber odbranu i sistem upravljanja kriznim situacijama izazvanim sajber napadima/incidentima širih razmjera kroz, između ostalog, uspostavljanje centralnog tijela za sajber bezbjednost u okviru kojeg bi funkcionisao i Nacionalni CIRT (Tim za odговор na računarske incidente), uspostavljanje sistema zaštite kritične informatičke infrastrukture, osnaživanje odgovora na sajber kriminal i harmonizacija sistema zaštite podataka, unapređenje procesa edukacije u oblasti sajber bezbjednosti u javnom i privatnom sektoru i jačanje javno-privatnog partnerstva i međunarodne saradnje.

### 2. Navesti usklađenost ovih ciljeva sa postojećim strategijama ili programima Vlade, ako je primjenljivo.

Izrada Predloga Strategije sajber bezbjednosti Crne Gore 2022-2026, kao i Akcionog plana 2022-2023. predviđena je Programom rada Vlade za 2021. godinu.

Dodatno, izrada nacionalne strategije za sajber bezbjednost je propisana i NIS EU Direktivom 2016/1148.

## 3. Opcije

- **Koje su moguće opcije za ispunjavanje ciljeva i rješavanje problema? (uvijek treba razmatrati "status quo" opciju i preporučljivo je uključiti i neregulatornu opciju, osim ako postoji obaveza donošenja predloženog propisa).**
- **Objasniti preferiranu opciju?**

Obzirom da izrada Predloga Strategije sajber bezbjednosti Crne Gore 2022-2026, kao i Akcionog plana 2022-2023. je obaveza predviđena Programom rada Vlade za 2021. godinu, a propisana i NIS EU

Strateški  
operativni  
ciljevi

Direktivom 2016/1148 gdje se Crna Gora na putu ka članstvu u EU usaglašava sa legislativom EU, druge opcije za ispunjavanje ciljeva definisanih usvojenim strateškim okvirom nema.

#### 4. Analiza uticaja

- Na koga će i kako će najvjerovatnije uticati rješenja u propisu - nabrojati pozitivne i negativne uticaje, direktne i indirektne.
- Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim i srednjim preduzećima)
- Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti.
- Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija.
- Uključiti procjenu administrativnih opterećenja i biznis barijera.

Implementacija Strategije će doprinijeti izgradnji integrisanog, funkcionalnog i efikasnog sajber prostora u skladu sa međunarodnim standardima i principima, te samim tim pozitivno uticati na državne institucije i društvo u cjelini.

Obezbjediće se sigurno funkcionisanje informacionih sistema odnosno servisa na kojima se oslanjaju ključni poslovni procesi kako državnih institucija, tako i privrednih subjekata. Glavni pozitivni uticaj predstavlja jačanje kapaciteta za sajber odbranu kroz uspostavljanje centralnog tijela za sajber bezbjednost, kao i snaženje kapaciteta u institucijama koje su prepoznate kao nosici sajber bezbjednosti, te jačanje sajber bezbjednosti kritične informatičke infrastrukture koja se nalazi u vlasništvu privatnog sektora, a na kojima se baziraju ključni društveni, ekonomski procesi, čime se stvara sigurniji sajber prostor Crne Gore.

Predlog Strategije sajber bezbjednosti Crne Gore 2022-2026, i Akcionog plana 2022-2023, neće izazvati troškove građanima i privredi, a neće izazvati ni administrativna opterećenja, niti biznis barijere.

#### 5. Procjena fiskalnog uticaja

- Da li je potrebno obezbjeđenje finansijskih sredstava iz budžeta Crne Gore za implementaciju propisa i u kom iznosu?
- Da li je obezbjeđenje finansijskih sredstava jednokratno, ili tokom određenog vremenskog perioda? Obrazložiti.
- Da li implementacijom propisa proizilaze međunarodne finansijske obaveze? Obrazložiti.
- Da li su neophodna finansijska sredstva obezbijeđena u budžetu za tekuću fiskalnu godinu, odnosno da li su planirana u budžetu za narednu fiskalnu godinu?
- Da li je usvajanjem propisa predviđeno donošenje podzakonskih akata iz kojih će proistići finansijske obaveze?
- Da li će se implementacijom propisa ostvariti prihod za budžet Crne Gore?
- Obrazložiti metodologiju koja je korišćenja prilikom obračuna finansijskih izdataka/prihoda.
- Da li su postojali problemi u preciznom obračunu finansijskih izdataka/prihoda? Obrazložiti.
- Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?
- Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.

#### 1. Da li je potrebno obezbjeđenje finansijskih sredstava iz budžeta Crne Gore za implementaciju propisa i u kom iznosu?

Da, implementacija aktivnosti iz predložene Strategije, odnosno dvogodišnjeg Akcionog plana zahtjeva obezbjeđivanje sredstava iz budžeta Crne Gore, što je i iskazano u samom dokumentu. Kumulativno, za dvije godine, potreban je iznos od: 3,5 miliona eura okvirno i zavisi od usvajanja Zakona o budžetu.

**2. Da li je obezbjeđenje finansijskih sredstava jednokratno, ili tokom određenog vremenskog perioda? Obrazložiti.**

Predviđeno je izdvajanje definisanog iznosa sredstava, u skladu sa planiranom realizacijom predloženih aktivnosti u Akcionom planu, tokom 2022. i 2023. godine.

**3. Da li implementacijom propisa proizilaze međunarodne finansijske obaveze?**

Ne.

**4. Da li su neophodna finansijska sredstva obezbijedena u budžetu za tekuću fiskalnu godinu, odnosno da li su planirana u budžetu za narednu fiskalnu godinu?**

Za realizaciju aktivnosti iz Akcionog plana za 2022. godinu sredstva su sadržana u predloženom Zakonu o budžetu za 2022. godinu, i njihovo povlačenje je uslovljeno usvajanjem navedenog Zakona u Skupštini Crne Gore.

Sredstva za aktivnosti iz AP čija realizacija je planirana za 2023. godinu biće planirana kroz Budžet za 2023. godinu kako bi se obezbijedio kontinuitet na planu realizacije strateških ciljeva u oblasti sajber bezbjednosti.

**5. Da li je usvajanjem propisa predviđeno donošenje podzakonskih akata iz kojih će proisteći finansijske obaveze?**

Da. Predloženi Akcioni plan za 2022-2023. godinu sadrži aktivnosti koje podrazumijevaju snaženje ljudskih resursa, konkretnije, povećanje broja službenika u CIRT-u, odnosno novom tijelu za sajber bezbjednost.

**6. Da li će se implementacijom propisa ostvariti prihod za budžet Crne Gore?**

Direktan prihod neće biti ostvaren, međutim mogu se smanjiti izdaci za otklanjanje posledica od sajber napada ukoliko se implementiraju predložene aktivnosti iz Akcionog plana i posleđično ostvare ciljevi iz Strategije sajber bezbjednosti Crne Gore 2022-2026, a koji su značajno veći od sredstava potrebnih za prevenciju istih.

**7. Obrazložiti metodologiju koja je korišćenja prilikom obračuna finansijskih izdataka/prihoda.**

Prilikom definisanja Predloga Strategije sajber bezbjednosti Crne Gore 2022-2026, kao i Akcionog plana za implementaciju iste za period 2022-2023, analizirani su neophodni minimalni tehnički i ljudski kapaciteti za stvaranje potrebnog nivoa sajber bezbjednosti na nacionalnom nivou. Uzete su u obzir i preporuke, zahtjevi, najbolje prakse EU, NATO-a, kao i drugih međunarodnih partnera.

Prepoznati finansijski izdaci su podijeljeni na izdatke za unapređenje tehničkih kapaciteta i izdatke potrebne za snaženje i povećanje ljudskih resursa u ovoj oblasti. Za prve, procjena je napravljena na osnovu informacija dobijenih od strane ponuđača potrebne opreme i usluga. Za druge, procjena je napravljena na osnovu dostupnih informacija o sredstvima koja su potrebna za stručno osposobljavanje postojećeg kadra (radionice, programi obuke i sl), kao i poznatih koeficijenata za zarade zaposlenih u javnom sektoru na osnovu kojih se mogao utvrditi „trošak“ angažovanja novog kadra.

**8. Da li su postojali problemi u preciznom obračunu finansijskih izdataka/prihoda?**

Ne.

U predloženom Akcionom planu za 2022-2023. godinu su definisane su aktivnosti, kvalitativni i kvantitativni indikatori prema kojima će se mjeriti ispunjenje planiranih aktivnosti i definisanih ciljeva. (Odgovor na pitanja 2 i 3).

**4. Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?**

Za koordinaciju aktivnosti biće zadužen Savjet za informacionu bezbjednost, u čijem sastavu se nalaze predstavnici svih ključnih institucija iz oblasti koju tretira predložena Strategija i AP.

**Datum i mjesto**

Podgorica, 6.12.2021. godine

