Crna Gora
Ministarstvo finansija

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

Br: 03-02-430/23-4768/2

Podgorica, 21.07.2023.godine

MINISTARSTVO JAVNE UPRAVE
-n/r ministru, gospodinu mr Marashu Dukaju-

Poštovani gospodine Dukaj,

Povodom *Predloga zakona o informacionoj bezbjednosti,* Ministarstvo finansija daje sljedeće

MIŠLJENJE

Uvidom u tekst Predloga zakona i Izvještaj o analizi uticaja propisa, sa aspekta uticaja na poslovni ambijent ukazujemo na sljedeće:

Primjena mjera informacione bezbjednosti podrazumijeva primjenu tehničkih i organizacionih mjera, tako da su organi u obavezi da svoje mrežne i informacione sisteme unaprijede u skladu sa propisanim mjerama za čiju primjenu su potrebna finansijska ulaganja. Ukoliko su oni već uspostavili sistem upravljanja informacionom bezbjednošću u skladu sa međunarodnim standardima i dobrom praksom u ovoj oblasti, ne očekuje se da primjena zakona izazove značajne troškove. Međutim, organi koji su u skladu sa zakonom prepoznati kao ključni i važni subjekti, a koji do sada nijesu uspostavili odgovarajući sistem upravljanja informacionom bezbjednošću imaće određene troškove za ispunjenje zakonskih obaveza koji se ogledaju u eventualnom dodatnom tehnološkom opremanju, obuci zaposlenih, angažovanju novih stručnjaka i slično. Naime, koliko će finansijskih sredstava za primjenu zakona izdvojiti zavisi od njihove veličine, odnosno broja zaposlenih, tehnološke opremljenosti (posjedovanje računarske opreme, informacionog sistema), obučenosti zaposlenih za korišćenje informacionih tehnologija u domenu informacione bezbjednosti, i drugih faktora od kojih funkcionisanje informacione bezbjednosti zavisi.

U Izvještaju o analizi uticaja propisa nije kvantifikovana procjena i na taj način navedeni subjekti su onemogućeni da planiraju buduće troškove i nije izvršena procjena finansijskih izdataka budući da ne postoje zvanični podaci o finansijskim izdacima koji bi se mogli koristiti, kao i zvanična analiza nastale štete.

Uvažavajući da Ministarstvo javne uprave predlaže propis kako bi se stvorio zakonski osnov za izgradnju informacionih i sajber bezbjedonosnih kapaciteta na nivou države Crne Gore, nemamo primjedbi, uz napomenu da uvođenje svakog dodatnog zahtjeva ili uslova ne proizvede barijere i dodatna opterećenja za privredne subjekte.

Takođe, donošenjem novog Zakona o informacionoj bezbjednosti planirano je uspostavljanje Agencije za sajber bezbjednost, kao i stavljanje u funkciju tima za odbranu od sajber prijetnji i incidenata – CIRTa državne uprave, organizacione jedinice u Ministarstvu javne uprave koje je zaduženo za upravljanje Vladinom informatičkom infrastrukturom i informaciono komunikacionom mrežom organa.

Uvidom u dostavljeni Izvještaj o analizi uticaja propisa utvrđeno je da je za implementaciju ovog Zakona potrebno obezbjeđivanje dodatnih finansijskih sredstava iz Budžeta Crne Gore, i to iznos od 2.620.000,00 €, a koji se odnosi na:

1. Ispunjenje tehničkih i drugih uslova za rad Agencije, iznos od 2.090.000,00 €. Najveći dio sredstava za pomenutu namjenu, u iznosu od 1.500.000,00 €, predviđen je za opremanje server sale sa infrastrukturnom i mrežnom opremom u poslovnim prostorijama zgrade RESPA u Danilovgradu koje će se koristiti za rad Agencije, obezbjeđivanje agregatskog napajanja i redudanse svih sistema. Za opremu za redudantne sisteme potreban je iznos od 200.000,00 €, dok je za zaposlene, nabavku softverskih alata za forenziku, analitiku, bezbjedonosnih alata i sredstava komunikacije potrebno obezbijediti 90.000,00 €.

2. Troškove povećanja kapaciteta Ministarstva javne uprave (CIRT državne uprave) potrebna su sredstva u iznosu od 530.000,00 €, i to za redudantne sisteme i rezervne radne prostorije iznos od 300.000,00 €, za opremanje prostorija za rad i Informacione sisteme 50.000,00 €, za sredstva komunikacije koja neće izazvati prekide i adekvatan sistem za prijavljivanje i upravljanje incidentima 60.000,00 €.

Predlogom zakona predviđeno je da se sredstva za rad Agencije za sajber bezbjednost obezbjeđuju u Budžetu Crne Gore, i to u iznosu od 0,2% tekućeg budžeta Crne Gore, dok je za zaposlene u Agenciji predviđen mjesečni dodatak u iznosu od 45%. Takođe, predviđeno da danom donošenja akta o unutrašnjoj organizaciji i sistematizaciji Agencije ista preuzima državne službenike od Direkcije za zaštitu tajnih podataka koji su vršili poslove u okviru organizacione jedinice CIRT, kao i opremu i službenu dokumentaciju.

Razmatrajući dostavljenu dokumentaciju, ističemo sljedeće:

U cilju uspostavljanja adekvatnog planiranja i kontrole potrošnje, potrebno je izvršiti odgovarajuće izmjene u tekstu Predloga zakona. Potrebno je izvršiti dopune člana 46 stav 1 i 2, kao i člana 49 stav 7 i to da na: Finansijski plan kojeg donosi Savjet, kao i na statut i akt o organizaciji i sistematizaciji radnih mjesta Agencije saglasnost daje organ državne uprave nadležan za poslove budžeta. Dodatno, u skladu sa Zakonom o državnim službenicima i namještenicima za pokretanje postupka popune radnih mjesta potrebno je pribaviti potvrdu o obezbijeđenim finansijskim sredstvima od organa državne uprave nadležnog za poslove budžeta.

Ministarstvo finansija nije saglasno sa članom 53 stav 2 kojim se predviđa procentualno izdvajanje za finansiranje rada Agencije. Naime, kako bi se vodila jedinstvena politika za sve potrošačke jedinice i imajući u vidu da je isto u suprotnosti sa načelima programskog budžetiranja član 53 treba da glasi:

- "Sredstva za rad Agencije obezbjeđuju se u budžetu Crne Gore, u skladu sa zakonom kojim se uređuje oblast budžetskog sistema.
- Agencija je dužna da svoje finansijsko poslovanje organizuje i vodi u skladu sa propisima kojima se uređuje oblast budžetskog sistema i budžetskog računovodstva".

Član 54 stav 2 kojim se predlaže da zaposleni u Agenciji imaju mjesečni dodatak na zaradu u iznosu od 45%, potrebno je korigovati, na način da zaposleni u Agenciji na poslovima održavanja i bezbjednosti mrežnih i informacionih sistema mogu da ostvare dodatak na zaradu u visini do 30% osnovne zarade, uz prethodno pribavljenu saglasnost Ministarstva finansija.

Imajući u vidu da sredstva za potrebne namjene nijesu planirana budžetom za 2023. godinu, kao i da u RIA obrascu nije urađena potrebna procjena za 2023. godinu, potrebno je dostaviti informaciju o iznosu sredstava potrebnih za 2023. godinu i izvoru finansiranja istih, dok bi finansiranje za naredni period bilo predmet razmatranja u okviru planiranja godišnjeg zakona o budžetu.

S poštovanjem,

MINISTAR
mr Aleksandar Damjanović

OBRAZAC

IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA	
PREDLAGAČ PROPISA	Ministarstvo javne uprave
NAZIV PROPISA	Predlog zakona o informacionoj bezbjednosti

1. Definisanje problema

- **Koje probleme treba da riješi predloženi akt?**
- **Koji su uzroci problema?**
- **Koje su posljedice problema?**
- **Koji su subjekti oštećeni, na koji način i u kojoj mjeri?**
- **Kako bi problem evoluirao bez promjene propisa ("status quo" opcija)?**

Koje probleme treba da riješi predloženi akt?

Važeći Zakon o informacionoj bezbjednosti u Crnoj Gori donijet je 2010. godine, kada je prvi put uređena oblast bezbjednosti u informaciono-komunikacionim tehnologijama.
Prvi Zakon o informacionoj bezbjednosti u Crnoj Gori donijet je 2010. godine i uredio je mjere i standarde informacione bezbjednosti, kao i sistem zaštite i prevencije od bezbjednosnih incidenata na internetu. Ovaj zakon donijet je u periodu prije usvajanja Direktive EU o mjerama za visok nivo informacione bezbjednosti mrežnih i informacionih sistema u Evropskoj uniji br. 2016/1148 (NIS Direktiva). Izmjenama i dopunama Zakona iz 2016. godine, kroz prepoznavanje Savjeta za informacionu bezbjednost, kao i osnova za uređivanje mjera zaštite kritične informatičke infrastrukture, ovaj zakon je djelimično usklađen sa pomenutom direktivom.
Evropska unija krajem 2022. godine, usvojila je Direktivu (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2), nakon čega je Crna Gora prateći trendove EU pristupila transponovanju navedene direktive u Predlog zakona o informacionoj bezbjednosti.
Programom rada Vlade za 2023. godinu, u okviru oblasti 5. Digitalna transformacija pod ciljem 5.2 Jačanje Vladine informatičke infrastrukture, kao aktivost pod br. ND 130 predviđen je Predlog zakona o informacionoj bezbjednosti, čiji rok završetka je planiran za III kvartal 2023. godine.

Nakon sajber napada visokog nivoa sofisticiranosti od 20. avgusta 2022. godine, a koji je bio usmjeren na Vladinu informatička infrastruktura i informaciono-komunikacionu mrežu organa, onemogućen je nesmetan rad i funkcionisanje javne uprave, pa se sa elektronskog poslovanja moralo preći na tradicionalni način poslovanja. Ugrožen je veliki broj informacionih sistema, od kojih je zavisio kontinuitet pružanja usluga i ostvarena značajna šteta, koja je iziskivala oporavak u više faza.

Predloženi akt treba da riješi sledeće probleme:

1. Nepostojanje opštih kriterijuma za prepoznavanje ključnih i važnih subjekata od kojih zavisi vršenje djelatnosti od javnog interesa;
2. Upravljanje sajber bezbjednošću;
3. Neobavještavanje o sajber prijetnjama i incidentima;
4. Rješavanje incidenta i postupanje u slučaju sajber prijetnji i incidenata sa značajnim uticajem. Naime, dosadašnjim propisom nije regulisano ko se obavještava, ko rješava ili u saradnji s kim rješava sajber prijetnje i incidente sa značajnim uticajem;
5. Rješavanje i postupanja u slučaju sajber krize. Ko se obavještava? Kada i na koji način se proglašava sajber kriza?
6. Nepostojanje nadležnih tijela odgovornih za sajber bezbjednost i za nadzorne zadake sa propisanim nadležnostima;
7. Nepostojanje obaveze izvještavanja na nivou subjekata;
8. Nepostojanje jasno propisanih mjera u pogledu sajber bezbjednosnih rizika;
9. Nepostojanje stručnog nadzora; i
10. Nepostojanje kaznenih odredbi.

Koji su uzroci problema?

Uzroci nabrojanih problema prije svega su:

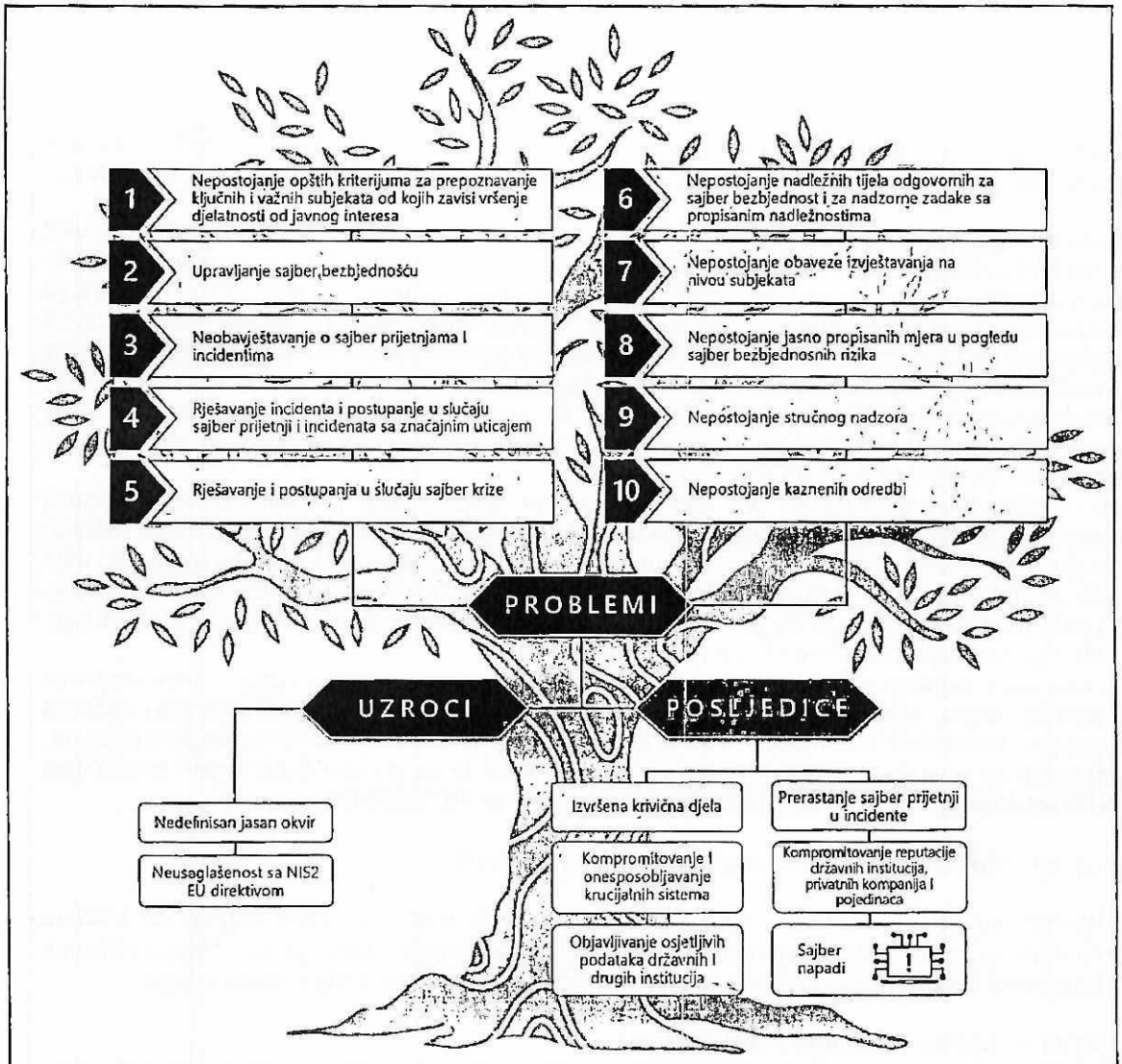
Nedefinisan jasan okvir, koji omogućava organizaciju i koordinaciju u slučajevima rješavanja sajber prijetnji, sajber incidenata sa značajnim uticajem i sajber krize.

Neusaglašenost sa Direktivom (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2).

Koje su posljedice problema?

Posljedice problema su: krivična djela izvršena u ovom domenu, objavljivanje osjetljivih podatka državnih i drugih institucija, kompromitovanje i onesposobljavanje krucijalnih mrežnih i informacionih sistema na kojima su bazirani poslovni i društveni procesi, kompromitovanje reputacije kako državnih i privatnih institucija, tako i pojedinaca.

Prerastanje sajber prijetnji u incidente sa visokim značajnim negativnim učinkom, može dovesti do znatnog oštećenja, poremećaja i negativnih uticaja na podatke i mrežne i informacione sisteme.



Primjer:

Sajber napad na Vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu organa od 20. avgusta 2022. godine.

Detaljnom analizom[1] utvrđeno je djelovanje ransomware malicioznog koda i detektovani su DDoS i Botnet napadi visokog nivoa sofisticiranosti. U cilju predostrožnosti i sprječavanja daljih posljedica napada, izvršeno je isključivanje servera na kojima su smješteni informacioni sistemi organa, sa informaciono-komunikacione mreže organa. Nastali sajber napad onemogućio je nesmetan rad i funkcionisanje javne uprave, te se sa elektronskog poslovanja moralo preći na

[1] Informacija o preduzetim aktivnostima povodom saniranja posljedica izazvanih sajber napadima na Vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu organa (Informacija o preduzetim aktivnostima povodom saniranja posljedica izazvanih sajber napadima na vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu organa (www.gov.me)

tradicionalni način poslovanja. Ugrožen je veliki broj informacionih sistema, od kojih je zavisio kontinuitet pružanja usluga i ostvarena značajna šteta, koja je iziskivala oporovak u više faza.

Oporavak od sajber napada, je bio dugotrajan proces u kome su pored domaćih, podršku pružili i međunarodni partneri. Ekspertski tim iz Sjedinjenih Američkih Država pružio je stručnu (konsultativnu) podršku u prevazilaženju novonastale situacije i planiranju i stvaranju mehanizama za adekvatniju sajber zaštitu u slučaju novog sajber napada visokog nivoa sofisticiranosti. Od strane eksperata iz Republike Francuske, odnosno Nacionalne agencije za bezbjednost informacionih sistema (ANSSI), Ministarstvu je pružena podrška na ponovnom uspostavljanju pojedinih informacionih sistema. Sa partnerima iz Velike Britanije razmijenjena su iskustva u vezi aktuelnih sajber napada i planirani su zajednički projekti za unapređenje informacione bezbjednosti u Crnoj Gori.
Nacionalna infrastruktura je sve izloženija sajber rizicima koji proističu iz integrisanosti informaciono komunikacionih tehnologija sa poslovima koji se obavljaju preko infrastrukture. Rastuća zavisnost od informaciono komunikacionih tehnologija stvorila je slabe tačke, što daje prilike sajber kriminalu da raznim hakerskim alatima ugrozi funkcionisanje vitalne infrastrukture. Tokom analize utvrđeno je da je kriptovano ukupno 17 informacionih sistema u 10 institucija, dok je sajber napad direktno uticao na 150 računara.
U cilju preduzimanja mjera i aktivnosti za otklanjanje posljedica sajber napada i sprječavanje nastanka novih, organi su, u koordinaciji sa Ministarstvom javne uprave, intezivno radili na oporavku korisničkih računara. Izvršena je reinstalacija svih računara u mreži organa državne, pri čemu su postojeći podaci arhivirani i izuzeti, kako bi se izvršilo skeniranje i mogućnost ponovne infekcije prethodno reinstalitanih uređaja svela na minimum.

Koji su subjekti oštećeni, na koji način i u kojoj mjeri?

Oštećeni su brojni subjekti - kako institucije, privreda tako i građani. Napad na Vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu doveo je do onemogućavanja elektronske komunikacije među institucijama i prema korisnicima elektronskih usluga.

Načini na koji su oštećene institucije su:
Onemogućavanje rada informacionih sistema na kojima se zasnivaju biznis procesi, kao i procesi od nacionalne bitnosti (npr. nacionalni telekomunikacioni sistemi, sl).
Onemogućavanje pružanja elektronskih usluga građanima, privredi i organima državne uprave.
Onemogućavanje obavljanja svakodnevnih aktivnosti koje se zasnivaju na informaciono komunikacionim tehnologijama, a koje su dio jedinstvenog informacionog sistema kojim upravlja Ministarstvo javne uprave.
Narušavanje ugleda objavljivaljem lažnih informacija ili krađom informacija.

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

Opcija „status quo" bi dovela do još veće eskalacije problema koji su nabrojani. Naime, bez jasno propisanog okvira za bezbjednost mrežnih i informacionih sistema, sa definisanim tijelima za sprovođenje i unapređenje mjera informacione bezbjednosti, propisanog vršenja nadzora nad primjenom tih mjera, kao i bez uspostavljenog sistema za rano otkrivanje i odbranu od sajber prijetnji i incidenata, povećava se opasnost od potencijalnih napada u sajber prostoru. Nastali sajber napadi mogu pruzrokovati značajnu štetu uslijed prekida električne energije, nedostatka vode, nemogućnost javnog transporta i drugo.

2. Ciljevi

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

Koji ciljevi se postižu predloženim propisom?

Glavni cilj ovog zakona je: izgradnja informacionih i sajber bezbjedonosnih kapaciteta na nivou države Crne Gore, ublažavanje prijetnji mrežnim i informacionim sistemima koji se upotrebljavaju za pružanje osnovnih usluga u ključnim sektorima i osiguravanje kontinuiteta takvih usluga u slučaju incidenata, čime se doprinosi sigurnosti i efikasnijem funkcionisanju privrede i društva.

Predloženi propis se priprema u skladu sa Programom rada Vlade za 2023. godinu, u okviru oblasti 5. Digitalna transformacija pod ciljem 5.2 Jačanje Vladine informatičke infrastrukture, kao aktivost pod br. ND 130, a čiji rok završetka je planiran za III kvartal 2023. godine.

Donošenjem ovog propisa stvara se zakonski osnov za realizacilju sledećih ciljeva:

- Usklađivanje sa pravnom tekovinom EU kroz transponovanje Direktive (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2). Kroz Program pristupanja Crne Gore Evropskoj uniji 2023 – 2024. u okviru usluga informatičkog društva planirana je izrada ovog propisa.
- Izgradnja sajber bezbjednosnih kapaciteta na nivou Crne Gore, poput Agencije za sajber bezbjednost i CIRTa državne uprave;
- Identifikovanje ključnih i važnih subjekata od kojih zavisi vršenje djelatnosti od javnog interesa;
- Stvaranje održivog sistema za efikasno otkrivanje i odbranu od sajber prijetnji i incidenata visokog nivoa.
- Ublažavanje i sprječavanje prijetnji mrežnih i informacionih sistemima koji se koriste za pružanje osnovnih usluga u ključnim i važnim sektorima
- Jačanje povjerenja korisnika u smislu zaštite njihovih podataka.

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).**
- **Obrazložiti preferiranu opciju?**

Prilikom pripreme Predloga zakona razmatrana je "status quo", neregulatorna i regulatorna opcija.
Status quo opcija: Ova opcija omogućava nastavak postojećih praksi i procedura, to bi značilo da se u slučaju zadržavanja "status quo" opcije ne bi se postigao zadovoljavajući nivo informacione bezbjednosti mrežnih i informacionih sistema. Zadržavanjem "Status quo" opcije

izalazi se iz regulatornih tokova EU, koji imaju za cilj da nizom propisa podignu nivo informacione bezbjednosti na području Unije, jedan od njih je i Direktiva NIS 2.

Neregulatorna opcija: Ova opcija nije prihvatljiva budući da država Crna Gora u procesu usaglašavanja sa evropskom pravnom tekovinom, ima obavezu usaglašavanja propisa sa pravnom tekovinom EU, u ovom slučaju sa Direktivom NIS 2, koja je usvojena 14. decembra 2022. godine, te razmatranje neregulatorne opcije nije prihvatljivo.

Regulatorna opcija: Preferirana opcija je donošenje ovog propisa čime će se stvoriti zakonski osnov za izgradnju informacionih i sajber kapaciteta na nivou države, ublažavanje prijetnji mrežnim i informacionim sistemima i osiguravanje kontinuiteta usluga u slučaju prijetnji i incidenata. Takođe doprinijeće se uklanjanju razlika u pogledu informacionu i sajber bezbjednosti na nivou EU i države Crne Gore kao kandidata za ulazak u EU.

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.**

Na koga će i kako će najvjerovatnije uticati rješenja u propisu - nabrojati pozitivne i negativne uticaje, direktne i indirektne.

Donošenje ovog propisa će pozitivno uticati na rad državnih organa, organa državne uprave, organa jedinica lokalne samouprave, organa lokalne uprave, i službi obrazovanih u skladu sa zakonom kojim se uređuje lokalna samouprava, pravnih lica koja vrše javna ovlašćenja (organi), privrednih društava i drugih pravnih i fizičkih lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemom (drugi subjekti), kao i na građane Crne Gore.

Takođe, pozitivan uticaj će se odraziti i na investicioni ambijent u Crnoj Gori, čime se stvaraju bolji uslovi za razvoj investicija. uz sigurnije i bezbjednije funkcionisanje informacionih sistema na kojima su zasnovani kritični i biznis procesi.

Rješenja u ovom zakonu doprineće boljoj povezanosti svih relevantnih aktera u oblasti informacione bezbjednosti, budući da se ovim zakonom predviđa uspostavljanje Zbirnog registra ključnih i važnih subjekata koji pružaju usluge od opšteg interesa za Crnu Goru . Na taj način Ministarstvo javne uprave kao organ nadležan za informacionu bezbjednost i Agencija za sajber bezbjednost, čije osnivanje se predviđa ovim zakonom, uspostaviće intenzivniju saradnju sa svim ključnim i važnim subjektima, naročito u slučaju kada se dešava sajber prijetnja, incident ili kriza.

Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim i srednjim preduzećima)?

Budući da primjena mjera informacione bezbjednosti podrazumijeva primjenu tehničkih i organizacionih mjera, organi su u obavezi da svoje mrežne i informacione sisteme unaprijede u skladu sa propisanim mjerama za čiju primjenu su potrebna finansijska ulaganja. Ukoliko su oni već uspostavili sistem upravljanja informacionom bezbednošću u skladu sa međunarodnim standardima i dobrom praksom u ovoj oblasti, ne očekuje se da primjena zakona izazove značajne troškove. Međutim, organi koji su u skladu sa zakonom prepoznati kao ključni i važni subjekti, a koji do sada nijesu uspostavili odgovarajući sistem upravljanja informacionom bezbjednošću imaće određene troškove za ispunjenje zakonskih obaveza koji se ogledaju u eventualnom dodatnom tehnološkom opremanju, obuci zaposlenih, angažovanju novih stručnjaka i slično.

Precizni iznosi dodatnih troškova za navedene organe variraju , budući da isti zavise od više faktora koji mogu da budu veoma različiti u različitim organima. Naime, koliko će finansijskih sredstava za primjenu zakona izdvojiti zavisi od njihove veličine, odnosno broja zaposlenih, tehnološke opremljenosti (posjedovanje računarske opreme, informacionog sistema), obučenosti zaposlenih za korišćenje informacionih tehnologija u domenu informacione bezbjednosti, i drugih faktora od kojih funkcionisanje informacione bezbjednosti zavisi. Shodno navedenom, nije moguće dati ni tačne, ni okvirne iznose po organu.

Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti?

Primjena mjera informacione bezbjednosti je od posebnog značaja i zahtijeva finansijska ulaganja, ali i smanjuje i sprječava finansijske izdatke koje mogu nastati kao posledica sajber incidenata sa značajnim uticajem na mrežne i informacione sisteme.
U većini slučajeva, onemogućavanje obavljanja svakodnevnih aktivnosti koje se zasnivaju na upotrebi mrežnih i informacionih sistema, izaziva veće finasijske izdatke od samih ulaganja u sprovođenje mjera zaštite.
Neispunjavanje mjera informacione bezbjednosti od strane ključnih i važnih subjekta koji su prepoznati u sektorima energetike, transporta, finansija, sanbdijevanja vodom i dr. može značajno da ugrozi normalno funkcionisanje društva.
Opasnost od potencijalnih napada može da se odrazi na bezbjednost i javno zdravlje građana, ekonomiju, životnu sredinu i dr.
Narušavanje reputacije objavljivanjem lažnih informacija ili krađom održava se na poslovni uspjeh i poslovanje organa.

Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija?

Primjena ovog propisa podržava stvaranje novih privrednih subjekata koji će pružati usluge informacione bezbjednosti i sajber zaštite.

Uključiti procjenu administrativnih opterećenja i biznis barijera.

Odredbama člana 18 ovog zakona propisano je sledeće:
Organi i drugi subjekti koji su u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona. Ključni i važni subjekti određuju se Odlukom Vlade, nakon sprovedenog postupka prepoznavanja od strane nadležnih organa u skladu sa ovim zakonom.

Organi i drugi subjekti koji nijesu u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 15 ovog zakona.
Organi i drugi subjekti dužni su da odrede zaposleno lice za praćenje primjene mjera informacione bezbjednosti u skladu sa st. 1 i 2 ovog člana.
Radi sprovođenja mjera informacione bezbjednosti, organi i drugi subjekti koji su u sladu sa ovim zakonom određeni kao ključni subjekti moraju da ispunjavaju uslove u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001.
O ispunjenosti uslova iz stava 4 ovog člana ključnim subjektima akreditovano pravno lice izdaje certifikat.
Ključni subjekti dužni su da od akreditovanog pravnog lica zahtijevaju periodičnu provjeru ispunjenosti uslova u skladu sa standardom iz stava 4 ovog člana.

Budući da se propisom pored primjene mejra informacione bezbjednosti na propisani način u članu 18 ovog zakona, zahtijeva određivanje zaposlenog lica za praćenje mjera informacione bezbjednosti od strane organa i drugih subjekata, kao i primjena važećeg crnogorskog standarda za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 od strane ključnih subjekata, u tom smislu troškovi organa i drugih subjekata koji nemaju stručno lice za praćenje primjene mjera, kao i troškovi ključnih usbjekata koji nemaju implementiran navedeni standard bi bili povezani sa troškovima zapošljavanja stručnog lica i uspostavljanja navedenog standarda.

Međutim kroz dosadašnju saradnju, objavljene godišnje izvještaje o radu institucija smatra se da u cilju digitalne transformacije društva veći broj organa i drugih subjekata ima zaposleno lice za praćenje primjene mjera informacione bezbjednosti, kao i da određeni broj ključnih i važnih subjekata već ispunjava uslove propisane ovim zakonom, uključujući i primjenu važećeg crnogorskog standarda za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 od strane ključnih subjekata.

Najveći sajber napad u Crnoj Gori dogodio se 20. avgusta 2022. godine.

- Tokom napada obustavljena je svaka međusobna elektronska komunikacija organa, kao i komunikacija sa privredom i građanima preko 5. 500 službenih e-mail adresa.

- Informacioni sistem socijalnog staranja ISSS (tzv. Socijalni karton) je jedan od ključnih informacionih sistema bez kojeg praktično nije moguće sprovesti postupke podnošenja zahtjeva utvrđivanja prava na materijalna davanja i socijalne usluge, izdavanje pojedinačnih rješenja, mjesečne revizije postojećih korisnika, obračun i isplatu. Kroz ISSS mjesečno se obračuna i uputi na isplatu oko 200.000, 00 pojedinačnih isplata ka građanima u ukupnom iznosu od oko 200 miliona eura za 2023. godinu.
  Onemogućavanje rada ovog informacionog sistema uslijed sajber napada bi ugrozilo egzistenciju velikog broja građana Crne Gore. Takođe, ISSS je interoperabilan za devet razliičitih institucija sa kojima se razmjenjuju podaci .

- Elektronski sistem javnih nabavki nije bio u funkciji, te su se javne nabavke odložile za nekoliko mjeseci, što se posebno odrazilo na nabavku ljekova.

- Prestao je da radi Portala eUprava, te su građanima, pravnim licima, kao i cjelokupnoj upravi par mjeseci bile nedostupne 383 elektronske usluge. Iz tih razloga za 2.743 visokoškolaca prolongiran je Program stručnog osposobljavanja lica sa stečenim

visokim obrazovanjem za 2022-2023. za mjesec dana kao i podnošenja zahtjeva za dodjelu studentskog kredita za 3.900 studenata.

- Zapošljavanje preko sistema za elektro testiranje kandidata odloženo je za dva mjeseca.

- Portal elektronskih sjednica Vlade koji podržava elektronska zasijedanje Vlade i Vladinih komisija nije bio u funkciji tako da je 10 sjednica održano uz upotrebu papirne dokumentacije.

- Portal Vlade GOV.ME preko kojeg se objavljuju informacije u skladu sa Zakonom o slobodnom pristupu informacija i ažuriraju ostale informacije koje su važne za rad organa državne uprave, nije bio u funkciji oko mjesec dana.

- Sistem za elektronsko upravljanje dokumentima (eDMS) nije bio u funkciji tri mjeseca. Samim tim komunikacija se obavljala isključivo u papirnoj formi.

Osim ovog sajber napada, za vrijeme napada koji se dogodio 2016. godine oboreni su sajtovi državnih institucija, a i 2017. bili su ugroženi servisi Vlade i državnih institucija.

Sajber napadima su izložene sve države u region i šire, primjera radi susjedne države Albanija i Srbija bile su skorije mete snažnih sajber napada.
Albanija - Javni onlajn servisi Albanije bili su blokirani u julu 2022. nakon sajber napada.
Hakeri su pokušali da onesposobe ključne sisteme Metod koji su koristili identičan je napadima viđenim u međunarodnom sajber prostoru", poput izvedenih u Ukrajini, Nemačkoj, Litvaniji, Malti, Holandiji i Belgiji.
Srbija - Hakeri su preko sajta javno-komunalnog preduzeća Informatika blokirali informatički sistem Novog Sada u martu 2020. godine.
U zamjenu za kod kojim bi se, navodno, otključale blokirane baze podataka zatražili su otkup od 50 bitkoina (400.000 eura). Kako je grad odbio da plati ucjenu, ostao je bez velikog broja podataka. Tokom napada nijesu mogle da se izdaju građevinske dozvole, nije radila objedinjena naplata, prestao je da radi sistem video nadzora, internet je prestao da radi u upravama.

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 proisteći 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.**

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

Članom 53 ovog zakona propisano je da se sredstva za rad Agencije za sajber bezbjednost obezbjeđuju u Budžetu Crne, kao da odobrena sredstva za funkcionisanje i rad Agencije ne mogu biti manja od 0,2% tekućeg budžeta Crne Gore. Takođe Članom 54 stav 2 ovog zakona, propisano je da zaposleni u Agenciji imaju mjesečni dodatak na zaradu u iznosu od 45%, što je od izuzetnog značaja imajući u vidu nadležnosti Agencije, kao I poslove koje će zaposleni raditi, a posebno pri činjenici da broj kadrova u Crnoj Gori u ovoj oblasti nije zadovoljavajući, te da ih treba dodatno motivisati i spriječiti odliv takvih kadrova na rad van Grne Gore. Trenutno na tržištu rada ne postoje kadrovi sa ovim znanjima i postoji velika potražnja od strane država Zapadne Evrope ka angažovanju lica sa ovakvim specifičnim znanjima. Ujedno je i potražnja od strane privatnog sektora takođe izražena i u tom smislu je neophodno obezbijediti mjesečni dodatak u navedenom iznosu. Za popunjavanje radnih mjesta u agenciji neophodno je poznavanje rada na kompleksnim platformama i posebno iskustvo u radu sa mrežnim uređajima. Ujedno, zaposleni u Agenciji će imati potrebu za pristupu i obradi tajnih podataka, a to se odnosi na kompletan kadar.

Za implementaciju ovog propisa potrebno je obezbijediti finansijska sredstva iz Budžeta Crne Gore, prije svega za ispunjenje tehničkih i drugih uslova za rad Agencije i CIRT-a državne uprave,a to je da:

1) posjeduju sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju;
2) posjeduju prostorije za rad i informacione sisteme, smještene na sigurnim lokacijama;
3) posjeduju adekvatan sistem za prijavljivanje i upravljanje incidentima;
4) obezbjeđuju povjerljivost i pouzdanost procesa rada;
5) posjeduju redundantne sisteme i rezervne radne prostorije kako bi se obezbjedio kontinuitet rada;
6) imaju dovoljan broj zaposlenih kako bi se obezbijedio kontinuitet rada 24 časa.

U tom smislu troškovi povećanja kapaciteta Ministarstva javne uprave (CIRT državne uprave) bi bili okvirno sledeći:

- sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju predviđaju nabavku satelitskog linka za internet i telefonsku komunikaciju - **30 000 eura,**
- opremanje prostorija za rad i informacione sisteme, smještene na sigurnim lokacijama, u smislu obezbjeđivanja prostorija za rad CIRT-a – **50 000 eura,**
- adekvatan sistem za prijavljivanje i upravljanje incidentima **– 30 000 eura,**
- redundantne sisteme i rezervne radne prostorije kako bi se obezbjedio kontinuitet rada, na način da u slučaju kompromitacije ili fizičke nedostupnosti primarne lokacije, bezbjedonosni sistemi nad mrežom državnih organa I Vladinom infrastruktrom mogu biti promptno aktivirani sa druge lokacije – **300 000 eura,**

- dovoljan broj zaposlenih kako bi se obezbijedio kontinuitet rada 24 časa , odnosi se na uvećanje roja izvršilaca za tri, kao i za obezbjeđivanje naknade za rad GSOC-a za 24/7 nadzor i monitoring koji čine Direkcija Vladin CIRT i Direkcija za infrastrukturu,**120 000 eura**

Troškovi u vezi ispunjenja tehničkih i drugih uslova Agencije za sajber bezbijednosti bili bi sledeći:

- sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju predviđaju nabavku satelitskog linka za internet i telefonsku komunikaciju - **30 000 eura,**
- prostorije za rad i informacione sisteme, smještene na sigurnim lokacijama , u skladu sa Zaključkima Vlade koristiće prostorije poslovne zgrade Respa u dnilovgradu, ali je neophodno opremanje server sale sa infrastrukturnom i mrežnom opremom, kao i posebne mjere fizičke zaštitte(dojava požara, gašenje požara, video nadzor), obezbijediti agregatsko napajanje i obezbjediti redudansu svih sistema 1 **500 000 eura,**
- nabavka softverskih alata za forenziku , analitiku, bezbjedonosnih alata – 300.000
- adekvatan sistem za prijavljivanje i upravljanje incidentima – **30 000 eura,**
- redundantne sisteme i rezervne radne prostorije kako bi se obezbjedio kontinuitet rada, obezbijediće se prostorija u Disaster recovery u Bijelom polju, ali je neophodno obezbujediti opremu za redudantne sisteme – **200 000 eura.**
- dovoljan broj zaposlenih(sedam) u sektoru za nadzor i odgovor na incidente kako bi se obezbijedio kontinuitet rada 24/7 časa –**30 000 eura.**

Planirani broj zaposlenih u Agenciji za sajber bezbejdnost je 39.

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

Radi realizacije Predloga zakona, predviđeno je donošenja sledećih podzakonskih akata iz kojih neće proisteći dodatne finansijske obaveze:

- Uredbe o bližem način utvrđivanja mjera informacione bezbjednosti,
- Uredbe o bližem načinu određivanja nivoa incidenta prema nivou značaja i način reagovanja na incidente,
- Pravilnik o izgledu i sadržaju obrasca za dostavljanje obavještenja o incident.

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

Ulaskom u 2023. sajber bezbjednost je i dalje na vrhu liste briga kako državne uprave tako i privrede. Ovo nije iznenađenje ako imamo u vidu da je u prvoj polovini 2022. godine bilo je 2,8 milijardi malver napada širom svijeta i 236,1 miliona ransomver napada, kao i da je procijenjeno da je na globalnom nivou 2022. godine, pokrenuto šest milijardi fišing napada.
U novoj anketi IEEE (Institut inženjera elektrotehnike i elektronike- najveće svjetsko stručno udruženje za unaprjeđivanje tehnologije) anketirano je 350 glavnih tehnoloških službenika, direktora za informacione tehnologije i IT direktora, 51% ispitanika je navelo ranjivost oblaka kao najveću zabrinutost (u odnosu na 35% u 2022.), a 43% je navelo ranjivost centara podataka kao najveću zabrinutost (sa 27% u 2022.)[2].

[2] Izvor: https://www.techrepublic.com/article/top-cybersecurity-threats/

Implementacijom predloga zakona neće se ostvariti direktan prihod u budžetu, ali njegovom primjenom doprinosi se smanjenju negativnog finansijskog uticaja koje bi potencijalne sajber prijetnje, incidenti ili sajber krize mogle da izazovu.

Finansijsku procjenu štete, koja je prouzrokovana sajber napadima teško je izraziti. Cijena sajber napada zavisi od više faktora. Ukoliko se radi o klasičnom sajber kriminalu u cilju otkupa ukradenih podataka ne postoji pravilo koliko će se za otkup potraživati. Osim toga napadnuti subjekt koji je odgovoran za čuvanje prikupljenih podataka moraće da snosi i zakonske kazne. Korisnici usluga gube povjerenje u pružaoce usluga koji su bili meta napada.
Posljedice sajber napada mogu biti dalekosežne, kako u finansijskom tako i političkom smislu. Kontinuiranim ulaganjem u informacionu bezbjednost troškovi se znatno umanjuju i jača povjerenje korisnika.

Od sajber pretnji nisu zabrinute samo velike kompanijama koje vrijede milijardu dolara i više. Naime, mala i srednja preduzeća su sve češće žrtve sajber pretnji jer sa slabijom primjenom mjera informacione bezbjednosti imaju tendenciju da budu ranjivija. Prema Izveštaju Verizon Data Breach Investigations za 2021.[3]
1 od 5 žrtava bila su mala i srednja preduzeća — sa srednjom cijenom gubitaka od 21.659 dolara.

Prekid poslovanja izazvan sajber napadima može prouzrokovati ogromne gubitke u neostvarenom profitu. Gubitak povjerenja korisnika često zna da bude nepovratan. Zato čak 57% evropskih malih i srednjih preduzeća strahuje da bi sajber napad mogao veoma lako da ih dovede do bankrotstva (Izvor: EU Agencija za sajber bezbjednost- ENISA).

Zbog nedostatka adekvatnih struktura i mehanizama zaštite, kao i bezbjednosne politike, razvijene zemlje, ali i zemlje u razvoju, podjednako su na meti napada.
Napadima na energetski sistem Sjedinjenih Američkih Država oko 50 miliona ljudi ostalo je bez električne energije.

U toku 2014. godine, samo u jednom danu 50 norveških naftnih kompanija je napadnuto sajber napadima različitih intenziteta. Cjelokupna naftna industrija ove skandinavske države bila je žrtva masovnog napada. U napadima je došlo do hakovanja i krađe podataka bušenja, istraživanja i inženjeringa.

Njemačka željezara je bila meta napada krajem 2014. godine. Hakeri su uspješno preuzeli kontrolu nad programom čija je funkcija bila gašenje visoke peći. Ovo je jedan od primjera gde je sajber napad izazvao direktnu fizičku štetu.

Nedostatak ulaganja u bezbjednosna rješenja su globalni problemi, kojem su sve više izložena mala i srednja preduzeća dok velike koorporacije, nakon neugodnih iskustava koja su rezultirala velikim materijalnim štetama sve više ulažu u informacionu bezbjednost kroz primjenu mjera i poštovanje najsavremenijih standarda. Osim toga, kako se ne bi došlo u situaciju da, zahvaljujući sopstvenim bezbjednosnim propustima, sajber napad bude uspješan neophodno je kontinuirano raditi na razvoju bezbjednosne kulture.

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

[3] Izvor: https://www.forbes.com/advisor/business/common-cyber-security-threats/

Prilikom obračuna finansijskih izdataka/prihoda uzete su u obzir tri početne osnove:

- Odredbe Nacrta zakona o informacionoj bezbjednosti Crne Gore koje regulišu djelokrug rada Agencije i obaveze primjene propisa;
- Preporuke Microsofta o organizacionoj strukturi agencije za sajber bezbjednost („Building an effective national cybersecurity agency")
- Analiza različitih struktura agencija za sajber bezbjednost i posledica sajber napada na osnovu javno dostupnih izvora koji su navedeni u prethodnom tekstu.

Da li su postojale sugestije Ministarstva finansija na nacrt/predlog propisa?
Naknadno.
Da li su dobijene primjedbe uključene u tekst propisa? Obrazložiti.
Naknadno.

6. Konsultacije zainteresovanih strana

- **Naznačiti da li je korišćena eksterna ekspertska podrška i ako da, kako.**
- **Naznačiti koje su grupe zainteresovanih strana konsultovane, u kojoj fazi RIA procesa i kako (javne ili ciljane konsultacije).**
- **Naznačiti glavne rezultate konsultacija, i koji su predlozi i sugestije zainteresovanih strana prihvaćeni odnosno nijesu prihvaćeni. Obrazložiti.**

Naznačiti da li je korišćena eksterna ekspertska podrška i ako da, kako.

Tokom izrade ovog zakona korišćena je ekspertska podrška od strane eksperta iz Hrvatske, koji je angažovan uz podršku Ženevskog centra za upravljanje sektorom bezbjednosti (DCAF) koji finansira Ministarstvo spoljnih poslova Velike Britanije (UK FCDO).

Naznačiti koje su grupe zainteresovanih strana konsultovane, u kojoj fazi RIA procesa i kako (javne ili ciljane konsultacije).

Za potrebe izrade ovog propisa, kao i izrade RIA obrasca u početnoj fazi bio je formiran radni tim koji su činili predstavnici Ministarstva. U pripremnoj fazi izrade Nacrt zakona, prije raspisivanja javnog poziva za javnu raspravu, Nacrt zakona u dvodnevnom trajanju prezentovan je Savjetu za informacionu bezbjednost, koji čine predstavnici institucija za koje je informaciona bezbjednost od posebnog značaja, radi dobijanja inputa i smjernica.

Takođe, u skladu sa Uredbom o izboru predstavnika nevladinih organizacija u radna tijela organa državne uprave i sprovođenju javne rasprave u pripremi zakona i strategija („Službeni list CG", broj: 41/18), 10. novembra 2022. godine, raspisan je javni poziv za zainteresovanoj javnosti da se uključe u početnu fazu pripreme Nacrta zakona na internet stranici **http://www.mju.gov.me/ministarstvo** i portalu e-uprave **https://www.euprava.me/** , i u roku od 25 dana dostave svoje sugestje i predloge, o čemu je sačijen Izvještaj o obavljenom konsultovanju zainteresovane javnosti, u propisanom roku.

Isto tako, shodno navedenoj uredbi, 01. marta 2023. godine, raspisan je i javni poziv građanima, privrednim društvima, preduzetnicima, nezavisnim i regulatornim tijelima, pravnim i fizičkim licima koja vrše javna ovlašćenja, državnim organima, organima državne uprave, organima lokalne samouprave, organima lokalne uprave, nevladinim organizacijama i drugim organima i organizacijama (zainteresovani subjekti) da se uključe u javnu raspravu i daju svoj doprinos u razmatranju Nacrta zakona o informacionoj bezbjednosti i dostave svoje predloge,

sugestije i primjedbe, a koja javna rasprava je trajala 20 dana od dana objavljivanja javnog poziva na internet stranici Ministarstva javne uprave **https://www.gov.me/mju** i portalu e-uprave **www.euprava.me** . Na javnoj raspravi pored Nacrta zakona, objavljen je bio i Izvještaj o sprovedenoj analizi procjene uticaja propisa (RIA obrazac), međutim na isti nije bilo nikakvih sugestija ni primjedbi.
Tokom trajanja javne rasprave, pored redovnih javnih konsultacija (okruglog stola), sa ciljem kreiranja šireg inkluzivnog procesa, Ministarstvo javne uprave, organizovalo je i konsultacije sa "fokus grupama" koje su činile predstavnici ambasada, predstavnici privrede, akademske zajednice, NVO sektora i predstavnici međunarodnih udruženja u Crnoj Gori.

U toku trajanja javne rasprave od ukupno devet učesnika dostavljeno je 96 primjedbi/ predloga/sugestija, od čega je prihvaćeno 13 primjedbi/predloga/sugestija, dva su djelimično prihvaćena, a 77 primjedbi/ predloga/sugestija nije prihvaćeno, dok su ostali komentari (četiti) bili u vidu pitanja na koje je dat odgovor. O sprovedenoj javnoj raspravi sačinjen je Izvještaj o sprovedenoj javnoj raspravi u propisanom roku, koji je takođe javno objavljen na navedenim linkovima.

Tokom sprovedenog postupka javnog konusultovanja svi zainteresovani subjekti imali su priliku da se uključe u proces javne rasprave, kako putem dostavljenih komentara, primjedbi i sugestija u skladu sa javnim pozivom, tako i putem održavanja okruglo stola, o čemu je zainteresovana javnost mogla da se informiše na zvaničnoj stranici Ministarstva.

Sve informacije o sprovedenoj javnoj raspravi i obavještenjima objavljene su na zvaničnoj internet stranici Ministarstva na linku nacrt zakona o informacionoj bezbjednosti - Pretraga - GOV.ME (www.gov.me)

7: Monitoring i evaluacija

- **Koje su potencijalne prepreke za implementaciju propisa?**
- **Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?**
- **Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?**
- **Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?**

Koje su potencijalne prepreke za implementaciju propisa?

Kao potencijalne prepreke za implementaciju propisa izdvajaju se prije svega:
Potrebno je obezbijediti značajana finansijska sredstva za nesmetan rad tijela koja sačinjavaju okvir informacione bezbjednosti Crne Gore (Agencija za sajber bezbjednost i CIRT državne uprave).
Nedostatak službenika osposobljenih na odgovarajući način, prije svega za poslove rješavanja incidenata, stručnog i inspekcijskog nadzora, koji bi trebalo da posjeduju vještine potrebne za obavljenje tih zadataka u smislu utvrđivanje nedostataka hardvera, softvera, kriptovanja, mreža i sl.
Nerazumijevanje značaja primjene mjera informacione bezbjednosti od strane obveznika zakona u smislu podizanja svijesti zaposlenih u obalasti sajber bezbjednosti i integrisanja tehnologija kojima se jača informaciona bezbjednost.

Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?

U saradnji sa Agencijom za sajber bezbijednostMinistarstvo javne uprave izradiće Nacionalni plan za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu, u kojem će se utvrditi način upravljanja sajber prijetnjama, incidentima i sajber krizama.

Zaštitu 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, kao i stručni nadzor nad primjenom mjera informacione bezbjednosti kod tih organa i drugih subjekata vršiće Agencija za sajber bezbjednost. Ovo tijelo će se baviti informacionom bezbjednošću svih organa i drugih subjekata u smislu ovog zakona, osim organa državne uprave, za koje je zadužen CIRT državne uprave.

Takođe, važnu ulogu ima i Savjet za informacionu bezbijednost, radi praćenja razvoja informacione bezbjednosti, a naročito sajber bezbjednosti u cilju obezbjeđivanja bezbjednog sajber prostora Crne Gore.

Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?

Indikatori su:

1. Broj organa i drugih subjekata u smislu ovog zakona, a naročito ključnih i važnih subjekata koji primjenjuju mjere informacione bezbjednosti, a praćenje indikatora vršiće se preko stručnog i inspekcijskog nadzora koji e vršiti nadzornik, odnosno inspektor za usluge informacionog društva.

Naime, ovim zakonom definisani su kriterijumi za određivanje ključnih i važnih subjekata, kao i mjereinformacione bezbjednosti u cilju postizanja najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema.
Stručnim i inspekcijskim nadzorom utvrdiće se da li je postignut adekvatan nivo bezbjednosti.

Budući da u važećim Zakonom o informacionoj bezbjednosti nije opširnije razrađen nadzor, u prilog tome govori činjenica da nijesu postojale kaznene odredbe, novim zakonskim rješenjem je, kroz propisivanje stručnog i inspekcijskog nadzora, naglašen značaj praćenja i primjene mjera informacione bezbjednosti.

Stručnim nadzorom će se posebno utvrditi da li se primjenuju propisane mjere informacione bezbjednosti, posebno one koje se odnose na rad ključnih i važnih subjekata u smislu da li su donijeli propisane akte o sajber bezbjednosnim rizicima, odnosno da li je uspostavljen adekvatan nivo bezbijednosti sistema.

2. Broj prijavljenih sajber prijetnji i incidenata

Ovim zakonom propisana je obaveza izvještavanja o sajber prijetnjama i incidentima. Na osnovu broja prijavljenih sajber prijetnji i incidenata moći će se pratiti stanje u ovoj oblasti u smislu koliko je sajber prijetnji prijavljeno, koliko je preraslo u incidente, koliko je incidenata prijavljeno i kog su nivoa.

3. Uspostavljen Zbirni registar ključnih i važnih subjekata.

Po prvi put će se uspostaviti Zbirni registar ključnih i važnih subjekata, koji će voditi Ministarstvo javne uprave.

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

Monitoring i evaulaciju primjene propisa vršiće Ministarstvo javne uprave i Agencija za sajber bezbjednost, preko godišnjih izvještaja, kao i godišnjeg izvještaja o radu Savjeta za informacionu bezbjednost.
Jedan od načina praćenja evaluacije su i izvještaji organa i drugih subjekata o sajber prijetnjama i incidentima koji su obavezni da postupaju po ovom zakonu.

Datum i mjesto
10.07.2023. godine

Starješina
MINISTAR
mr Maraša Dukaj