Crna Gora
Ministarstvo javne uprave

Adresa: Rimski trg br. 45
81000 Podgorica, Crna Gora
tel:+382 20 482 131
fax:+382 20 241 790
www.mju.gov.me

Broj: 01-040/23-1844

IZVJEŠTAJ O SPROVEDENOJ JAVNOJ RASPRAVI

o Nacrtu zakona o informacionoj bezbjednosti

Ministarsto javne uprave uputilo je 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.

Vrijeme trajanja javne rasprave: Javni poziv za javnu raspravu objavljen je 01. marta 2023. godine, na internet stranici Ministarstva javne uprave https://www.gov.me/mju i portalu e-uprave www.euprava.me , u kom je navedeno da će javna rasprava trajati 20 dana od dana objavljivanja javnog poziva. Na ovaj način svi zainteresovani subjekti pozvani su da do i zaključno sa 20. martom 2023. godine, dostave svoje primjedbe, predloge i sugestije.

Način sprovođenja javne rasprave:

- Održavanje javnih konsultacija sa fokus grupama (dvije fokus grupe) sa ciljem kreiranja šireg inkluzivnog procesa koje su činili predstavnici ambasada u Crnoj Gori, predstavnici međunarodnih udruženja u Crnoj Gori, privrede, biznis i akademske zajednice i NVO sektora, u cilju prezentovanja koncepta Nacrta zakona o informacionoj bezbjednosti (09.03.2023. godine, održane dvije fokus grupe, u hotelu “Hilton” Podgorica);
- Održavanje sastanaka sa zainteresovanim subjektima, kao i putem drugih vidova komunikacije (e-mail korespodencija, putem telefona) u cilju pojašnjenja koncepta Nacrta zakona i pružanja dodatnih informacija;
- Održavanje Okruglog stola za svu zainteresovanu javnost (10.marta 2023. godine, održan okrugli sto u hotelu “Hilton” Podgorica);
- Dostavljanje primjedbi, predloga i sugestija tokom trajanja javne rasprave.

Ovlašćeni predstavnici ministarstva koji su učestvovali u javnoj raspravi:

- mr Marash Dukaj, ministar javne uprave,
- Dušan Polović, generalni direktor Direktorata za infrastrukturu, informacionu bezbjednost, digitalizaciju i e-servise,
- Dušan Krkotić, načelnik Direkcije za informacionu bezbjednost u Direktoratu za infrastrukturu, informacionu bezbjednost, digitalizaciju i e-servise,

- Jelena Knežević, načelnica Direkcije za normativu, elektronsku identifikaciju i elektronske usluge povjerenja, u Direktoratu za infrastrukturu, informacionu bezbjednost, digitalizaciju i e-servise.

Pored ovlašćenih predstavnika ministarstva tokom javne rasprave na fokus grupama i okruglom stolu prisustvovao je i Robert Mikač, ekspert iz Hrvatske koji je pružao stručnu podršku pri izradu Nacrta zakona, a koji je angažovan uz podršku Ženevskog centra za upravljanje sektorom bezbjednosti (DCAF) koji finansira Ministarstvo spoljnih poslova Velike Britanije (UK FCDO).

Podaci o broju i strukturi učesnika u javnoj raspravi:

U toku trajanja javne rasprave od ukupno devet učesnika dostavljeno je 96 primjedbi/ predloga/sugestija:

1. ICT Cortex (Coinis doo) Podgorica, Crna Gora, devet;
2. Branka Mićović, osam;
3. One Crna Gora doo, 13;
4. Ivan Vujović, 19;
5. Dragana Bulatović (ISO MONT doo), osam;
6. Crypted Security Integration, 11;
7. Američka privredna komora u Crnoj Gori (AmCham), 17;
8. Agencija za elektronske komunikacije i poštansku djelatnost, tri;
9. Branimir Bošnjak, osam.

Rezime dostavljenih primjedbi, predloga i sugestija, sa navedenim razlozima njihovog prihvatanja, odnosno neprihvatanja:

1. **ICT Cortex (Coinis doo) Podgorica, Crna Gora**

Primjedba/predlog/sugestija 1: Predloženo je da se u čl. 8, 9 i 10 Nacrta zakona odvoje pojmovi "mrežni i informacioni", u cilju prepoznavanja istih kao različitih segmenata jedne cjeline, uz obrazloženje da bi se na ovaj način obezbjedilo lakše definisanje potencijalnih prijetnji, incidenata i radnji, kao i da bi se na ovaj način kasnije mogli mnogo jasnije pojedinačno definisati pojmovi, postupci i procedure koje se tiču hardware-a (mreže) i informacija (software-a i samih podataka).

Predlog se ne prihvata.

Obrazloženje:

U odredbi člana 5 tačka 1 Nacrta zakona o informacionoj bezbjednosti dato je značenje izraza "mrežni i informacioni sistem", budući da se taj izraz koristi u preostalom tekstu Nacrta zakona.

Takođe, u skladu sa Programom pristupanja Crne Gore Evropskoj uniji (EU), Crna Gora je u obavezi da usklađuje propise sa pravnom tekovinom EU, te je shodno tome, Ministarstvo javne uprave u obavezi da prilikom izrade Nacrta zakona o informacionoj bezbjednosti transponuje Direktivu (EU) 2022/2555 EVROPSKOG PARLAMENTA I SAVJETA od 14. decembra 2022. godine, o mjerama za visoki zajednički nivo sajber bezbjednosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i o ukidanju Direktive (EU) 2016/1148 (NIS 2 Direktiva) i da kroz izradu Tabele usklađenosti (koja se dostavlja Ministarstvu evropskih poslova i Evropskoj komisiji na mišljenje) prikaže odredbe i tekst odredbe izvora prava Evropske unije (član, stav, tačka) koji se transponuje u odredbu i tekst odredbe nacrta/predloga propisa Crne Gore (član, stav, tačka).

Imajući u vidu navedeno izraz “mrežni i informacioni sistem” usklađen je sa članom 6 tačka 1 pomenute Direktive, te smatramo da je isti odgovarajući.

***Primjedba/predlog/sugestija 2*:** Predloženo je da se definiše mjesto/fizička lokacija skladištenja podataka, uz obrazloženje da se jasno definišu pravila i procedure koje se tiču same zaštite podataka, tj. minimalnog nivoa zaštite i enkripcije istih, bez obzira gdje se isti nalazili.

Predlog se ne prihvata.

Obrazloženje:

U poglavlju II Nacrta zakona, u odredbama čl. 6 do 11 propisane su mjere informacione bezbjednosti, uključujući i fizičku zaštitu.

U članu 11 stav 3 Nacrta zakona, propisano je da bliži način utvrđivanja mjera informacione bezbjednosti iz čl. 6 do 11 ovog zakona propisuje Vlade Crne Gore, što znači da će se podzakonskim aktom (Uredba) detaljnije urediti mjere informacione bezbjednosti, koje podrazumijevaju i fizičku zaštitu.

***Primjedba/predlog/sugestija 3*:** Predloženo je da se prepozna javnog-privatno partnerstvo kao ključno za sajber bezbednost, uz obrazloženje da se za slučaj nemogućnosti popunjavanja radnih mjesta u tjelima i organima predvidjenim ovim Zakonom savjetuje utvrdjivanje osnova za angažovanje kapaciteta privrednih subjekata i fizičkih lica sa potrebnim kompetencijama koji bi preuzeli obaveze predvidjene ovim Zakonom sa ciljem održavanja potrebnog nivoa sajber bezbjednosti.

Predlog se ne prihvata.

Obrazloženje:

Uređivanje javno-privatnog partnerstva ne može biti predmet ovog zakona, budući da se ta pitanja uređuju drugim posebnim zakonom (Zakon o javno-privatnom partnerstvu).

Primjedba/predlog/sugestija 4: Predloženo je da u članu 25 Nacrta zakona Savjet Agencije ima bar jednog člana stručne (cyber security) zajednice, uz obrazloženje da se razmotri i uvodjenje dodatnog člana iz kruga stručnjaka na polju sajber bezbjednosti akreditovanog sa minimum “ulaznim” sertifkatom (npr. CEF, CISA, i sl.) koji izdaje akreditaciona institucija priznata od strane EU ili ekvivalentnim iskustvom u IT sferi van državnih subjekata.

Predlog se ne nprihvata.

Obrazloženje:

Agencija za sajber bezbjednost će imati status državne agencije u skladu sa Zakonom o državnoj upravi "Službeni list CG", br. 78/28, 70/21 i 52/22, te samim tim organi državne agenije su savjet i direktor, koje imenuje i razrješava Vlada.

Budući da je odredbi člana 25 stav 2 Nacrta zakona propisano da Savjet ima pet članova, ministarstvo će na osnovu svih dostavljenih sugestija u odnosu na ovaj član procijeniti predstavnici kojih institucija mogu biti članovi Savjeta Agencije.Svakako da će Savjet činiti i predstavnici različitih institucija, uključujući i privredu, što je i bila namjera zakonopisca prilikom kreirana člana 25 Nacrta zakona.

Primjedba/predlog/sugestija 5: U članu 33 Nacrta zakona predloženo je da se u cilju akreditacije i obuka zaposlenih definišu kompetencije zaposlenih u Agenciji kao i akreditaciju/sertifikaciju istih kako bi se obezbjedio najviši moguči nivo sajber zaštite na državnom nivou. Akreditacije/sertifikati trebaju biti izdati po najnovijim programima i od strane akreditacionog tjela priznatog od strane EU.

Predlog se ne prihvata.

Obrazloženje:

Odredbama člana 33 Nacrta zakona definisana je primjena drugih propisa, ali se u Nacrtu zakona ne mogu uređivati uslovi koje zaposleni u Agenciji trebaju da ispune, kao i njihove kompetencije. Pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mjesta Agencije uređivaće se uslovi koje zaposleni trebaju da ispune.

***Primjedba/predlog/sugestija 6*:** U članu 36 Nacrta zakona je predloženo da se podzakonskim aktima, definiše tačna sadržina i standardi koji će biti primenjivani na sisteme, fizičku lokaciju, pouzdanost i upravljanje istim, uz obrazloženje da bi ovako opširno i dvosmisleno definisanje tehničkih uslova za obavljanje rada Agencije i CIRT-a trebalo maksimalno izbjeći í iste jasno definisati makar u djelu primenljivih standarda za fizičku lokaciju, telekomunikacije, EM zaštitu, upravljanje rizicima i sekundarnoj opremljenosti.

Predlog se ne prihvata.

Obrazloženje:

Članom 36 Nacrta zakona propisani su “neophodni” tehnički i drugi uslovi za Agenciju i Vladin CIRT, koje je potrebno ispuniti, a koji uslovi su transponovani iz člana 11 NIS2 Direktive. Svakako da će pored ovih uslova u skladu sa potrebama rada Agencije biti neophodni i drugi uslovi koji se u ovom momentu ne mogu predvidjeti.

***Primjedba/predlog/sugestija 7*:** Sugerisana je proaktivnost i aktivni monitoring infrastrukture na državnom nivou, uz obrazloženje da se umjesto pasivnog čekanja Agencije/CIRT-a predlaže aktivni pristup u kom bi bi se aktivno pratio status mrežne infrastrukture i ključnih informacionih sistema na nivou države Crne Gore u saradnji sa ključnim subjektima, na koji način bismo brže i bolje reagovali na sve potencijalne prijetnje po mrežne i informacione sisteme na teritoriji države i ne bi bilo potrebe da se čeka na dostavljanje informacije od strane ugroženog subjekta.

Predlog se prihvata.

Obrazloženje:

Predloženo će u skladu sa NIS 2 Direktivom biti propisano u Nacrtu zakona.

Primjedba/predlog/sugestija 8: Predloženo je da se u pogledu stručnog i inspekcijskog nadzora definisati potrebna znanja i vještine koje inspektor i stručni nadzonik mora da posjeduje kako bi adekvatno vršili poslove iz svog djelokruga rada.

Predlog se ne prihvata.

Obrazloženje:

Ovim zakonom ne mogu se uređivati znanja i vještine inspektora i stručnog nadzornika. Zakonom o inspekcijskom nadzoru uređuju se načela inspekcijskog nadzora, način i postupak vršenja inspekcijskog nadzora, obaveze i ovlašćenja inspektora i druga pitanja od značaja za vršenje inspekcijskog nadzora, dok se internim aktima (Pravilnik o unutrašnjoj organizaciji i sistematizaciji radnih mjesta) uređuju dodatni uslovi za inspektora i nadzornika.

Primjedba/predlog/sugestija 9: Predloženo je da se jasno i precizno definišu standardi koji će biti korišćeni, a ne samo okvirno navesti ISO 27001, koje se tiče samo menadžment aspekta sajber bezbjednosti. Sugerisano je da bi trebalo razmotriti uvodjenje i korišćenje svih relevantnih IOS/IEC JTC 1/SC27 ” standarda kao i implementaciju ITIL procedura bilo kroz sam Zakon bilo kroz podzakonska akta i/ili operativne procedure nadležnih organa. Takođe, ISO 27001 se ne tice samo menadžment aspekta sajber bezbjednosti već i implementacije

konkretnih mjera sajber bezjbednosti npr. u cilju sertifikacije za isti ISO 27002 daje detaljni prikaz mjera koje je neophodno implementirati.

Predlog se ne prihvata.

Obrazloženje:

Odredbom člana 20 stav 3 Nacrta zakona propisano je da su ključni subjekti dužni da primjenjuju međunarodni standard ISO/IEC 27001 za upravljanje informacionom bezbjednošću. Navedeno podrazumijeva obaveznu primjenu ovog standarda, što ne isključuje upotrebu i drugih standarda na nivou ključnih subjekata, u zavisnosti od potrebe i djelatnosti kojima se ti subjekti bave.

2. Branka Mićović

Primjedba/predlog/sugestija 1: Predloženo je da se u pogledu izraza mrežni i informacioni sistemi isti pojednostavi, odnosno da je svrsishodnije da se svede pod nazivom informacioni sistem koji podrazumijeva komunikacioni, računarski ili druge elektronski sisteme u kome se podaci obrađuju, čuvaju ili prenose.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 1 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 2: Predloženo je da se u članu 5 Nacrta zakona informaciona bezbjednost drugačije definiše imajući u vidu da se informaciona bezbjednost odnosi na sve informacije, kako u digitalnom formatu tako i papirnoj formi neophodno je u ovom objašnjenju to i precizirati, pa je predloženo da definicija glasi: informaciona bezbjednost podrazumijeva stanje povjerljivosti, cjelovitosti, dostupnosti i zaštite informacija, uključujući i sajber bezbjednost.

Predlog se ne prihvata.

Obrazloženje:

U odredbi člana 5 tačka 3 Nacrta zakona propisano je da je podatak svaka informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos internetom i elektronsku poštu. Smatramo da ovaka definicija kroz uključivanje elektronskog, optičkog ili sličnog sredstva uključuje elektronski ili digitalni oblik, kao i da je izraz “podatak” adekvatniji.

Primjedba/predlog/sugestija 3: Predloženo je da je u članu 5 Nacrta zakona umjesto sajber prijetnje neophodno definisati prijetnju kao opšti pojam u informacionoj bezbjednosti, a koja obuhvata i sajber prijetnje.

Predlog se ne prihvata.

Obrazloženje:

Ovaj zakon uređuje pitanje informacione bezbjednosti (koje uključuje i sajber bezbjednost), te samim tim smatratamo da uređivanje izraza “prijetnja” ne odgovara potrebama ovog zakona. Takođe definicija sajber prijetnje je u skladu sa NIS2 Direktivom preuzeta iz Uredbe 2019/1881 EU (Akt o sajber bezbjednosti).

Primjedba/predlog/sugestija 4: U čl. 11, 49 i 51 Nacrta zakona je predloženo da se riječi: “politiku analize rizika i bezbjednosti mrežnih i informacionih sistema;” zamijene i da glase:

“procedura analize rizika i bezbjednosti mrežnih i informacionih sistema;”, uz obrazloženje da je dokument kojim se definišu metodologije i način sprovođenja analize rizika i bezbjednosti mrežnih i informacionih sistema procedure.

Predlog se ne prihvata.

Obrazloženje:

Naziv “Politika analize rizika i bezbjednosti mrežnih i informacionih sistema”, kao jedna od mjera kojima se obezbjeđuje zaštita od sajber prijetnji i incidenata mrežnih i informacionih sistema, korisnika tih sistema i drugih lica na koje one utiču, je usklađen sa članom 21 tačka 2a) NIS2 Direktive, te smatramo da je riječ “politika” adekvatan i širok pojam, koji može uključivati i procedure.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore "Službeni list CG", br. 3/12, 31/15, 48/17 i 62/18, dodatno ćemo se konsultovati da li ovako definisane riječi “Politika analize rizika i bezbjednosti mrežnih i informacionih sistema” podrazumijevaju i procedure ili ograničavaju samo na postojanje predmetne politike.

Primjedba/predlog/sugestija 5: U članu 25 Nacrta zakona je predloženo da se prepozna još jedan član Savjeta koji bi bio iz reda privrednih društava koji spadaju u kategoriju Kritične infrastrukture, uz obrazloženje da će član iz reda privrednih društava koji pripadaju kritičnoj infrastrukturi doprinijeti boljem radu Agencije.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 4 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 6: U odnosu na član 29 Nacrta zakona predloženo je da isti glasi: “Za direktora može biti imenovano lice, koje pored opštih uslova za zasnivanje radnog odnosa u državnim organima ima visoku stručnu spremu, pet godina radnog iskustva u oblasti informacione bezbjednosti.” , uz obrazloženje da se primjedba odnosi na mali boj godina radnog iskustva u oblasti informacione bezbjednosti.

Predlog se prihvata.

Obrazloženje:

U odredbi člana 29 Nacrta zakona radno iskustvo za direktora Agencije će sa tri godine radnog iskustva u oblasti informacione bezbjendosti biti povećano na pet godina, u skladu sa datim predlogom. Kod određivanja radnog iskustva za poslove direktora Agencije, držali smo se analogije koja se primjenjuje u drugim organima državne uprave, kako ovim rješenjem, iako je riječ o lex specialis propisu, ne bismo odudarali od sistemskih rješenja. Uslovi za izbor direktora Agencije dati su na način da se može kvalifikovati širi krug kandidata, kako bi se u daljem toku procedure izbora došlo do najbljeg rješenja. Cijenimo da ovakav pristup doprinosi ohrabrivanju svih onih kandidata koji imaju potencijal i žele da preuzmu odgovornost za značajne poslove i nadležnosti Agencije.

Primjedba/predlog/sugestija 7: U članu 43 Nacrta zakona je predloženo da se definišu precizni kriterijume za klasifikaciju incidenta koji mogu biti niskog, srednjeg ili visokog nivoa, uz obrazloženje da u zakonu ne postoji precizna klasifikacija niti definisana precizna metodologija za procjenu nivoa incidenta.

Predlog se ne prihvata.

Obrazloženje:

Odredbom člana 38 Nacrta zakona propisani su kriterijumi za utvrđivanje incidenta sa značajnim uticajem na kontinuitet pružanja usluga. Nadalje odredbom člana 43 stav 3 Nacrta zakona propisano je sledeće: "Agencija, odnosno Vladin CIRT po prijemu obavještenja iz člana 40 ovog zakona o incidentu sa značajnim uticajem na kontinuitet pružanja usluga sprovodi analizu i prema nivou značaja i načinu reagovanja na incident vrši klasifikaciju incidenta koji može biti niskog, srednjeg ili visokog nivoa", dok je u stavu 11 istog člana propisano sledeće: „Bliži način određivanja nivoa incidenta iz stava 3 ovog član prema nivou značaja i način reagovanja na incidente, na predlog Agencije, uređuje Vlada." Navedeno podrazumijeva da će se podzakonskim katom (Uredba) propisati način određivanja nivoa incidenta.

***Primjedba/predlog/sugestija* 8:** U poglavlju VI. NADZOR predloženo je da se u članovima koji definišu nadzor nad sprovođenjem zakona neophodno definisati da inspektor i nadzornik moraju imati minimum tri seftifikat za eksternog auditora i to: ISO/IEC 27001, ISO 22301, ISO 31000.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 8 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

3. One Crna Gora doo

***Primjedba/predlog/sugestija* 1:** Predloženo je da se član 2 Nacrta zakona promijeni tako da glasi: ''Po ovom zakonu obavezni su da postupaju državni organi, organi državne uprave, organi jedinica lokalne samouprave, organi lokalne uprave, i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, pravna lica sa javnim ovlašćenjima (u daljem tekstu: organi), kao i druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemima, a koji se dijele na ključne i važne subjekte, u smislu ovog zakona.", uz obrazloženje da je predlog izmjene dat kako bi se jasno definisali termini ''organ'', ''ključni'' i ''važni'' subjekti, a sve u cilju da svaki subjekat nedvosmisleno može jasno da prepozna kategoriju kojoj pripada.

Predlog se ne prihvata.

Obrazloženje:

Odredbom člana 2 Nacrta zakona definisano je da su po ovom zakonu obavezni da postupaju državni organi, organi državne uprave, organi jedinica lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva, pravna lica sa javnim ovlašćenjima i druga pravna i fizičkih lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemima, (u daljem tekstu: organi) kao i ključni i važni subjekti, u smislu ovog zakona.

Mišljenja smo da ovako definisana odredba odgovara konceptu zakona budući da se određene odredbe odnose samo na ključne i važne subjekte, a ne i na organe.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore dodatno ćemo se konsultovati da li je ova odredba odgovarajuća.

Primjedba/predlog/sugestija 2: Predloženo je da član 5 stav 1, tač. 7 i 8 dopune na način da glase:

'' 7) sajber prijetnja je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na podatke i mrežne i informacione sisteme,

korisnike tih sistema i druge organe i lica, a koja je poznata vlasniku mrežnih I informacionih sistema''

''8) ozbiljna sajber prijetnja je sajber prijetnja za koju se na osnovu njenih tehničkih obilježja može pretpostaviti da može imati ozbiljan uticaj na mrežne i informacione sisteme nekog subjekta ili korisnika usluga subjekta uzrokovanjem značajne materijalne ili nematerijalne štete, a koja je poznata vlasniku mrežnih I informacionih sistema;'' , uz obrazloženje da je predlog dopune definicija dat jer ne može da se nametne obaveza nekom subjektu da reaguje ili postupa na neki način ukoliko ni sam nije upoznat sa konkretnom prijetnjom.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da su definicije odgovarajuće, iste su u skladu sa NIS2 Direktivom koja u ovom dijelu upućuje na Uredbu 2019/1881 EU (Akt o sajber bezbjednosti).

Primjedba/predlog/sugestija 3: Predloženo je da se član 25 stav 2 tač. 2 i 3 se izmijeni na način da glasi:

'' 2) dva člana koje predlažu Univerziteti u Crnoj Gori (državni ili privatni)''

3) dva člana koje predlaže privredna komora Crna Gore ili neko drugo udruženje privrednika u Crnoj Gori''.

Takođe je predloženo da se član 25 stav 2 tač. 4 i 5 brišu.

Predložene izmjene su date uz obrazloženje da Savjet treba da bude popunjen od strane članova koji na najbolji način mogu dati doprinos informacionoj bezbjednosti u Crnoj Gori, kao i da je sukob interesa da neko ko je zaposleni u Agenciji bude i član Savjeta koji nadgleda Agenciju.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 4 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora, kao i dodatno obrazloženje koje glasi:

Savjet Agencije projektovan je kao upravljačko i rukovodeće tijelo koje će usmjeravati rad i djelovanje Agencije. Posebno smo imali u vidu da se radi o novom, do sada nepoznatom organu sui generis karaktera, koji se tek konstituiše u našem pravnom i uopšte sistemu organa od društvenog i ekonomskog značaja.
Stoga je upravo prisustvo jednog člana iz reda zaposlenih okolnost koja već od samog konstituisanja doprinosi boljem upravljanju i kompetentnijem radu Savjeta. Ovo posebno kod činjenice da su svih ostalih 4 člana osobe van institucije kojima je neophodno informisanje i o tekućim procesima i to upravo od nekoga ko zna unutrasnje prilike u Agenciji, ko je proizvod transparentnog izbora od samih zaposlenih u Agenciji (procedura će biti uređena podzakonskim propisom), a opet svojim pojedinačnim uticajem i glasom ne može ni na jedan način ugroziti javni interes, odnosno biti u konfliktu interesa.
Pored toga, u praksi imamo veliki broj institucija iz sistema javne administracije, u kojima su predstavnici zaposlenih članovi organa upravljanja, pa to u praksi ne proizvodi negativne reperkusije: Institut za standardizaciju, Prirodnjački muzej, Centar za očuvanje i razvoj kulture manjina, itd.

Primjedba/predlog/sugestija 4: Predloženo je da se član 34 stav 2 Nacrta zakona dopuni na način da glasi: ''Savjet iz stava 1 ovog člana, čine predstavnici organa državne uprave nadležnog za unutrašnje poslove, organa državne uprave nadležnog za poslove odbrane, organa državne uprave nadležnog za poslove pravosuđa, organa državnog uprave nadležnog za vanjske poslove, organa uprave nadležnog za tajne podatke, Ministarstva,

Agencije i Agencije za nacionalnu bezbjednost, vlasnika mrežnih i informacionih sistema, a po potrebi i predstavnici drugih organa i institucija'', uz obrazloženje da je jako bitno da pored predstavnika državnih organau u radu ovako bitnog tijela budu uključeni i predstavnici privrede koji su vlasnici mrežnih i informacionih sistema (energetski sektor, banke, komunikacioni operatori i drugi).

Predlog se ne prihvata.

Obrazloženje:

Odredbom člana 34 stav 2 Nacrta zakona definisan je sastav Savjeta na način da podrazumijeva obavezan sastav od predstavnika navedenih organa, a takođe je navedeno da ga po potrebi čine i predstavnici drugih organa i institucija. Ovako definisan sastav Savjeta ostavlja prostor za uključivanje i predstavnika drugih organa, ukoliko za to bude potrebe.

***Primjedba/predlog/sugestija* 5:** Predloženo je da se član 37 stav 2 Nacrta zakona izmijeni na način da glasi: '' Ključni i važni subjekti osim organa državne uprave, dužni su da Agenciji jednom mjesečno dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga.'', uz obrazloženje da je predložena izmjena u skladu sa članom 2, a i u duhu teksta u okviru Člana 37, stav 3.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da je odredba člana 37 stav 2 Nacrta zakona odgovarajuća, jer se istom obuhvataju organi i ključni i važni subjekti, što je bila i namjera.

***Primjedba/predlog/sugestija* 6:** Predloženo je da se član 37 stav 6 Nacrta zakona izmijeni na način da glasi: ''Ključni i važni subjekti dužni su da obavijeste afektovane primaoce svojih usluga o svim ozbiljnim sajber prijetnjama i incidentima, a koji bi mogli negativno da utiču na pružanje njihovih usluga, kao i o svim mjerama koje bi ti primaoci usluga trebalo da preduzmu kao odgovor na sajber prijetnje i incidente.'', uz obrazloženje da je predlog izmjene dat sa ciljem da se preciznije definiše obaveza ključnih i važnih subjekata u pogledu potrebe komunikacije ka primaocima usluge.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da je odredba člana 37 stav 6 Nacrta zakona odgovarajuća, te da riječ: "afektovane" za koju je predloženo da se doda, nije primjenjiva.

***Primjedba/predlog/sugestija* 7:** Predloženo je da se član 37, stav 8 izmijeni na način da glasi: ''Izvještaje iz st. 2 i 3 ovog člana i obavještenja iz st. 4 do 7 ovog člana, Agencija i/ili Vladin CIRT označavaju sa odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.'', uz obrazloženje da je Predlog dopune dat iz razloga što pravna lica koja nisu državni organi nemaju pravo da označavaju dokumenta sa određenim stepenom tajnosti.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da je odredba člana 37 stav 8 odgovarajuća, budući da član 2 Zakona o tajnosti podataka ("Službeni list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13, 18/14, 48/15 i 74/20) glasi: „Po ovom zakonu dužni su da postupaju državni organi, organi državne uprave, organi jedinica lokalne samouprave i druga pravna lica koja vrše javna ovlašćenja (u daljem tekstu: organi), kao i pravna i fizička lica kad u vršenju zakonom utvrđenih poslova,

odnosno izvršavanju ugovorenog posla ostvare pristup ili postupaju sa tajnim podacima (u daljem tekstu: drugi subjekti).”

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore dodatno ćemo se konsultovatiu pogledu ove odredbe.

***Primjedba/predlog/sugestija* 8:** Predloženo je da se član 38, stav 1, tačka 3 dopuni na način da glasi: ‘’3) geografskoj raširenosti incidenta, ukoliko je primjenljivo;’’, uz obrazloženje da je predlog dopune dat iz razloga što konkretno za mobilne operatore pitanje geografske raširenosti se ne može jasno odrediti, zbog same prirode usluge.

Predlog se prihvata.

Obrazloženje:

U skladu sa datom sugestijom inoviraćemo odredbu člana 38 tačka 3 Nacrta zakona.

***Primjedba/predlog/sugestija* 9:** Predloženo je da se posle člana 39, stav 1, doda stav 2 koji će da glasi: ’’Način i forma dostavljanja obavještenja i izvještaja iz stave 1 ovog člana bliže će odrediti Ministarstvo, a uz konsultacije sa ključnim i važnim subjektima.’’, uz obrazloženje da je predlog dopune dat iz razloga što se smatra potrebnim da se precizno navede forma i način izvještavanja koja se očekuje od subjekata ka nadležnim organima, čime se izbjegava različito tumačenje i obaveze koje subjekti imaju.

Predlog se djelimično prihvata.

Obrazloženje:

Prihvata se dio predloga koji se odnosi na propisivanje načina i forme obavještavanja i izvještavanja, dok se ne prihvata dio koji glasi: “a uz konsultacije sa ključnim i važnim subjektima” budući da to nije u skladu sa pravno-tehničkim pravilima za izradu propisa.

***Primjedba/predlog/sugestija* 10:** Predloženo je da se član 43, stav 12 Nacrta zakona izmijeni na način da glasi: ‘’Obavještenja iz stavova 2, 3,4, 6, 8 ovog člana , kao i predlog akta Vladi iz stava 10 ovog člana, Agencija i/ili Vladin CIRT označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka’’, uz obrazloženje da pravna lica koja nisu državni organi nemaju pravo da označavaju dokumenta sa određenim stepenom tajnosti.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na Primjedbu/predlog/sugestiju 7.

***Primjedba/predlog/sugestija* 11:** Predloženo je da se član 49 stav 1 tačka 9 Nacrta zakona izmijeni na način da glasi: ‘’9) naloži da obavijeste afektovane primaoce svojih usluga o sajber prijetnjama i incidentima koji bi mogli negativno uticati na pružanje njihovih usluga, kao i o svim mjerama koje bi trebali preduzeti kao odgovor na sajber prijetnje i incidente.’’, uz obrazloženje da se preciznije definiše obaveza ključnih i važnih subjekata u pogledu potrebe komunikacije ka primaocima usluge.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 6.

***Primjedba/predlog/sugestija* 12:** Predloženo je da se član 49 stav 1 tačka 11 izmijeni na način da glasi: ‘’11) privremeno zabrani rad i pružanje usluga, do trenutka otklanjanja ozbiljne sajber prijetnje i incidenta, a koji mogu imati negativan uticaj na podatke i mrežne i informacione sisteme, korisnike tih sistema i druge ključne i važne subjekte i organe.’’, uz obrazloženje da se preciznije definiše pravo inspektora ali i da se ograniče moguće posljedice po ključne i važne subjekte.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da je član 49 stav 1 tačka 11 Nacrta zakona odgovarajući, jer inspektor u skladu sa posebnim zakonom (Zakonu o inspekcijskom nadzoru) nalaže trajanje predložene mjere.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore dodatno ćemo se konsultovati u pogledu ove odredbe.

***Primjedba/predlog/sugestija* 13:** Predloženo je da se član 51, stav 4 izmijeni na način da glasi: ‘’Agencija može, osim nadzornika, ovlastiti i druga zaposlena lica da na licu mjesta (uz prisustvo nadzornika), kod ključnih i važnih subjekata, izvrše kontrolu i uzimanje podataka neophodnih za izvršavanje poslova iz nadležnosti Agencije.’’, uz obrazloženje da se smatra neosnovanim da bilo koje lice iz Agencije, bez prisustva nadzornika vrši stručni nadzor nad subjektom.

Predlog se ne prihvata.

Obrazloženje:

Odredbom člana 47 stav 2 Nacrta zakona propisano je sledeće:”Stručni nadzor nad primjenom ovog zakona vrši Agencija, preko zaposlenog lica koje je ovlašćeno za vršenje nadzora (u daljem tekstu: nadzornik).“ Naziv nadzornik uveden radi korišćenja skraćenice u daljem tekstu zakona, a to je svakako zaposleno lice u Agenciji koje je ovlašćeno za vršenje nadzora, što znači da Agencija može imati više zaposlenih lica koja će biti ovlašćena za vršenje nadzora.

4. Ivan Vujović

***Primjedba/predlog/sugestija* 1:** U bitnom je konstatovano da je na osnovu dosadašnjeg iskustva jasno da je Crnoj Gori potrebna temeljna reorganizacija sektora sajber bezbjednosti, pri čemu je kvalitetan i efikasan institucionalni okvir osnov tog procesa, te da Agencija za informacionu bezbjednost treba da bude krovna institucija u ovim procesima, kao i da pduzimanje nadležnosti Agencije u odnosu na ministarstva i državnu upravu i dodjelu nadležnosti Vladinom CIRT-u nije efikasno rješenje. Takođe je između ostalog konstatovano da: Agencija treba da ima nadležnost da donosi politike, procedure i uputstva iz oblasti sajber bezbjednosti i da obavlja reviziju i kontrolu primjene tih politika i za ministarstva i državne organe. Pored toga, u praksi može doći do koalizije odnosno preklapanja nadležnosti između Agencije i Vladinog CIRT-a, što može prouzrokovati da nefunkcionalnost sistema zaštite od sajber napada i istraživanja uzroka napada. Takođe, nadležnosti sektorskih organa (član 14, 15, 16) treba dodijeliti Agenciji, s obzirom da sektorski organi vjerovatno neće imati kapaciteta da adekvatno odrede kriterijume i pragove za prepoznavanje ključnih subjekata. Pozicija nadležnog sektorskog organa treba da bude savjetodavna, odnosno da Agencija u postupku određivanja ključnih i važnih subjekata konsultuje nadležni sektorski organ, ali da aktivnosti iz člana 14 sprovodi Agencija. Radi efikasnosti procesa, nadležnosti ministarstva iz člana 17, 18 i 19 treba prebaciti na Agenciju. Na ovaj način bi se jasno odredila odgovornost u procesu određivanja kritičnih i važnih subjekata i značajno poboljšala efikasnost tog procesa. Takođe je i postavljeno pitanje čija

nadležnost su mreže i informacioni sistemi Predsjenika Crne Gore, Skupštine Crne Gore, sudova i tužilaštava?

Predlog se ne prihvata.

Obrazloženje:

U skladu sa Zakonom o elektronskoj upravi Služba Predsjednika Crne Gore, Skupštine Crne Gore, sudova i tužilaštava može koristiti informaciono-komunikacionu mrežu kojom upravlja Ministarstvo javne uprave, ukoliko ispuni tehničke i druge uslove propisane navedenim zakonom i pratećim podzakonskim aktima.
Mišljenja smo da su nadležnosti i uloge Agencije i Vladinog CIRT-a jasno postavljene. Nadležnost Agencije ne može biti donošenje politika za organe državne uprave i državne organe, budući da su nadležnosti ministarstva (među kojima je i donošenje politika) propisane posebnim propisima. Odredbama čl. 14, 15 i 16 Nacrta zakona propisane su obaveze nadležnih sektorskih organa koje se ne mogu "dodijeliti" Agenciji, budući nadležni sektorski organi u skladu sa posebnim propisima vrše nadzor nad određenim organima.

***Primjedba/predlog/sugestija* 2:** Postavljeno je pitanje zašto je napravljeno izuzeće u članu 12 Nacrta zakona gdje se kaže da su državni organi izuzeti od obaveze upravljanja sajber bezbjednosnim rizicima.

Odgovor:

Odredbom člana 12 Nacrta zakona propisano je sledeće: "Organi su dužni da primjenjuju mjere informacione bezbjednosti od čl. 6 do 10 ovog Zakona, osim mjera iz člana 8, stav 1, tačka 3 ovog zakona."

Smisao navedene odredbe je da organi koji tokom postupka prepoznavanja nijesu određeni kao ključni ili važni ne primjenjuju mjeru informacione bezbjednosti iz člana 8, stav 1, tačka 3 ovog zakona (upravljanje sajber bezbjednosnim rizicima), iz razloga što je pojam organi široko postavljen, uključuje veliki broj institucija, te smo mišljenja da one institucije (organi) koje nijesu prepoznati kao ključni ili važni subjekt, nijesu spremne za primjenu mjere informacione bezbjednosti - upravljanje sajber bezbjednosnim rizicima.

***Primjedba/predlog/sugestija* 3:** Postavljeno je pitanje da li se trgovci i proizvođači oružja svrstavaju u kritične ili važne subjekte s obzirom da nijesu eksplicitno navedeni?

Odgovor:

Zavisiće od nadležnih sektorskih organa da li ih prepoznaju kao ključne i važne subjekte.

***Primjedba/predlog/sugestija* 4:** Ukazano je da važnim subjektima treba smatrati i sve one subjekte koji posjeduju, obrađuju ili vode registre ili zbirke ličnih podataka na osnovu kojih se može utvrditi identiteta lica, pri čemu se kriterijumi za jasno određivanje koji su to subjekti mogu regulisati podzakonskim aktima, uz obrazloženje da Nacrtom zakona (član 53) jeste predviđeno da se podaci o ličnosti koriste i obrađuju u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti, ali smatram da i ovim zakonom trebaju biti prepoznati i obuhvaćeni subjekti koji posjeduju registre ili zbirke ličnih podataka.

Odgovor:

Kao u primjedbi/predlogu/sugestiji 3.

***Primjedba/predlog/sugestija* 5:** Predloženo je da se u članu 18 stav 2 Nacrta zakona treba propisati da su ključni i važni subjekti dužni da prijave promjenu podataka iz člana 16 odmah nakon nastanka promjene, a najmanje jednom godišnje.

Predlog se prihvata.

Obrazloženje:

U skladu sa datom sugestijom upodobićemo odredbu člana 18 stav 2 Nacrta zakona.

***Primjedba/predlog/sugestija* 6:** Predloženo je da u članu 20 Nacrta zakona treba propisati da lice određeno za praćenje primjene mjera informacione bezbjednosti mora imati položen ispit (ili pohađati obuku) koju će organizovati Agencija, uz obrazloženje da to pitanje treba bliže urediti podzakonskim aktom.

Predlog se ne prihvata

Obrazloženje:

U Nacrtu zakona ne mogu se definisati uslovi za zaposlena lica kod ključnih subjekata, već to može biti predmet internog akta ključnog subjekta (Pravilnik o unutrašnjoj organizaciji i sistematizaciji radnih mjesta). Takođe u članu 23 tačka 13 Nacrta zakona propisan je da Agencija vrši edukaciju organa, nadležnih sektorskih organa i ključnih i važnih subjekata kroz savjetovanja i obuke u cilju jačanja informacione bezbjednosti.

***Primjedba/predlog/sugestija* 7:** Predloženo je da u članu 20 stav 3 Nacrta zakona treba izbjeći pominjanje konkretnog standarda, već to urediti kroz podzakonski akt, uz obrazloženje da ISO 27001 jeste opšte prihvaćen standard ali se vremenom može ukazati potreba da se mreže i informacioni sistemi usaglase sa nekim drugim standardom, pri čemu bi se onda izbjegla složenija procedura izmjene zakona, te da će sektorski kriterijumi za postizanje zadvoljavajućeg stepena informacione bezbjednosti vjerovatno biti zahtjevniji, kao npr. za bankarski ili zdravstveni sektor i možda zahtijevati prilagođavanje nekom drugom ili još nekom standardu.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 9 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

***Primjedba/predlog/sugestija* 8:** Predloženo je da se u članu 23 propiše da Agencija vrši reviziju, testira, provjerava i analizira nivo zaštite informacionih sistema ključnih i važnih subjekata, uz obrazloženje da Agencija mora imati nadležnosti i da obavlja provjeru, testira i analizu implementirane zaštite mreža i informacionih sistema subjekata kojima je nadležna.

Predlog se prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 7 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

***Primjedba/predlog/sugestija* 9:** Predloženo je da se Zakonom treba propisati da su ključni i važni subjekti i organi dužni da jednom godišnje Agenciji podnose izvjestaj o stanju bezbjednosti svojih mreža i informacionih sistema, uz pojašnje da bi Izvještaj trebao da sadrži opis sistema, informacije o eventualnoj pojavi incidenata, informacije implementiranim mjerama informacione bezbjednosti, i slično.

Predlog se prihvata.

Obrazloženje:

Predlog će biti inkorporiran u Nacrt zakona, na odgovarajući način.

***Primjedba/predlog/sugestija* 10:** Predloženo je da članom 26 treba osigurati kontinuitet poslovanja i mogućnost donošenja odluka u slučajevima između isteka mandata članu (članovima) Savjeta Agencije do izbora novih.

Predlog se ne prihvata.

Obrazloženje:

Odredbom člana 63 Nacrta zakona propisano je da Savjet za informacionu bezbjednost koji se obrazovan u skladu sa Zakonom o informacionoj bezbjednosti ("Službeni list CG" br. 14/10, 40/16 i 74/20) nastavlja sa radom do obrazovanja Savjeta za informacionu bezbjednost u skladu sa ovim zakonom, iz kog razloga nije potrebna izmjena člana 26 Nacrta zakona na predloženi način.

***Primjedba/predlog/sugestija* 11:** Predloženo je da u članu 27 Nacrta zakona nadležnosti oko usvajanja programa osnovne obuke za stručno usavršavanje zaposlenih u Agenciji treba da ima Direktor, a ne Savjet, uz obrazloženje da su ovo su uglavnom operativne odluke, pri čemu Savjet ima mogućnost da kroz finansijski plan i plan rada posredno utiče i na planiranje i sprovođenje obuka.

Predlog se ne prihvata.

Obrazloženje:

Budući da je Savjet Agencije organ upravljanja, mišljenja smo da je odredba člana 27 Nacrta zakona odgovarajuća, te da Savjet usvaja, odnosno donosi ono što direktor predlaže, u konkretnom slučaju direktor Agencije u skladu sa članom 30 tačka 8 predlaže program osnovne obuke za stručno usavršavanje zaposlenih u Agenciji dok isti Savjet usvaja, u skladu sa odredbom člana 27 tačka 5 Nacrta zakona.

***Primjedba/predlog/sugestija* 12:** Ukazano je da bi u članu 29 Nacrta zakona trebalo propisati da direktor ima i nekog rukovodećeg iskustva, ne samo iskustva u oblasti informacione bezbjednosti, kao i da je potrebno propisati i minimalnu stručnu spremu za poziciju direktora.

Predlog se ne prihvata.

Obrazloženje:

Odredba člana 29 Nacrta zakona je postavljena na način da to bude u skladu sa Zakonom o državnim službenicima i namještenicima "Službeni list CG", br. 2/18, 34/19, 8/21, u kom Zakonu je propisano između ostalog da lice koje vrši poslove iz kategorije visoki rukovodni kadar mora imati VII1 nivo kvalifikacije obrazovanja i najmanje dvije godine radnog iskustva na poslovima rukovođenja ili pet godina radnog iskustva.

***Primjedba/predlog/sugestija* 13:** Konstatovano je da u članu 33 stav 3 da nije odgovarajuća formulacija za zakonski tekst, uz obrazloženje da se eksplicitno pominjanje i vezivanje nadležnosti, prava i obaveza za ime nekog organa se uglavnom izbjegava.

Predlog se ne prihvata.

Obrazloženje:

Budući da se ovim zakonom stvaraju uslovi za osnivanje nove institucije – Agencije za sajber bezbjednost, te da ista nije prepoznata u Zakonu o zaradama zaposlenih u javnom sektoru, mišljenja smo da je u Nacrtu zakona potrebno eksplicitno navesti.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore dodatno ćemo se konsultovati da li je ova odredba odgovarajuća.

***Primjedba/predlog/sugestija* 14:** Sugerisano je da u članu 33 stav 4 nije potreban s obzirom na prava i obaveze koje direktoru proistuču iz zakona kao starješini organa, uz obrazloženje da se neka specifična nadležnost za direktora može regulisati Statutom Agencije.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na Primjedba/predlog/sugestija 13.

***Primjedba/predlog/sugestija* 15:** Predloženo je da članom 33 Nacrta zakona treba propisati da se zarade zaposlenih utvrđuju kao i za zaposlene u nezavisnim ili regulatornim tijelima, u skladu sa zakonom kojim se definišu zarade u javnom sektoru (državnih službenika i namještenika), kao i propisati da Savjet utvrđuje uslove, način ostvarivanja i visinu specijalnog dodatka na zaradu zaposlenih.

Predlog se ne prihvata.

Obrazloženje:

Agencija za sajber bezbjednost će imati status državne agencije u skladu sa Zakonom o državnoj upravi, a ne status regulatorne agencije, iz kog razloga smatramo da nije moguće drugačije definisanje odredbe člana 33 Nacrta zakona u dijelu zarada zaposlenih u Agenciji.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore dodatno ćemo se konsultovati da li je ova odredba odgovarajuća.

***Primjedba/predlog/sugestija* 16:** Predloženo je da se u članu 36 doda da je potrebno imati i savremnu i odgovarajuću tehničku opremu (hardver i softver) za obavljanje definisanih zadataka.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 6 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

***Primjedba/predlog/sugestija* 17:** Predloženo je da je potrebno predviđeti da Agencija za obavljanje svojih nadležnosti može angažovati i eksternog stručnjaka.

Predlog se ne prihvata.

Obrazloženje:

Smatramo da u Nacrtu zakona nije potrebno propisati da Agencija za obavljanje svojih nadležnosti može angažovati i eksternog stručnjaka, to se svakako podrazumijeva. U odredbi člana 43 stav 9 Nacrta zakona svakako je propisano da Agencija i Vladin CIRT u rješavanju incidenata sa značajnim uticajem na kontinuitet pružanja usluga visokog nivoa koji je doveo do značajnog oštećenja, poremećaja i negativnih uticaja na podatke i mrežne i informacione sisteme, korisnike tih sistema i druge ključne i važne subjekte i organe, mogu koristiti ekspertsku i stručnu pomoć nacionalnih i međunarodnih institucija i organizacija.

***Primjedba/predlog/sugestija* 18:** Predloženo je da se u članu 43 stav 1 treba propiše da Agencija, na osnovu sopstvene procjene, može da se uključi u rješavanje i "ovih incidenata". Ovo će možda nekada biti potrebno, kako bi se spriječilo nastajanje incidenta većih razmjera.

Predlog se ne prihvata.

Obrazloženje:

Smatramo da kod incidenata koji nemaju značajan uticaj na kontinuitet pružanja usluga, učešće Agencije odnosno Vladinog CIRT-a nije potrebno, ali smo u cilju praćenja takvih incidenata u odredbi člana 37 st. 2 i 3 Nacrta zakona propisali obavezu dostavljanja izvještaja o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga, jednom mjesečno Agenciji, odnosno Vladinom CIRT-u.

***Primjedba/predlog/sugestija* 19:** Ukazano je da je razdvajanje nadležnosti nadzora i inspektora je nepotrebno i vrlo neefikasno rješenje, uz obrazloženje između ostalog da razdvajane nadležnosti nadzornika i inspektora već postoji za oblast elektronskih komunikacija i pokazalo se kao vrlo neefikasno rješenje, sa dosta problema u primjeni, kao u da nadzornik neće imati ovlašćenja da piše prekršajni nalog subjektu nadzora, s obzirom da dosadašnju sudsku praksu, pa je samim tim upitna svrha postojanje takve pozicije.

Predlog se ne prihvata.

Obrazloženje:

Budući da organ državne uprave nadležan za inspekcijske poslove nema inspektora za oblast informacione bezbjednosti, već samo inspektora za oblast informacionog društva (široko postavljena nadležnost za sve propise iz oblasti informacionog društva) ovim rješenjem nastojali smo da kroz uloge stručnog nadzora i inspektora omogućimo efikasniju primjenu ovog zakona i nadzor nad istim.

5. **Dragana Bulatović (ISO MONT doo)**

***Primjedba/predlog/sugestija* 1:** Predloženo je da se u članu 13 stav 3 tačka 4 Nacrta zakona, poslije riječi: "distribucija" dodaju riječi: "prodaja", a u tački 5 poslije riječi: "proizvodnja" dodaju riječi: "i distribucija". Takođe, u odnosu na stav 4 istog člana predloženo je da bi subjekte trebalo obavezati da redovno rade analizu rizika sa aspekta informacione bezbjednosti, uz obrazloženje da se putem ocjene rizika identifikuju prijetnje po informacionu imovinu, ocjenjuju ranjivosti i vjerovatnoća njihovog ostvarivanja i utvrđuju se nivo uticaja kako bi se u konačnom dobio nivo rizika.

Predlog se ne prihvata.

Obrazloženje:

Odredba člana 13 stav 3 tačka 4 Nacrta zakona usklađena je sa NIS 2 Direktivom, te smo mišljenja da nije potrebno dodavati predložene riječi.

***Primjedba/predlog/sugestija* 2:** Predloženo je da se u članu 23 tačka 18 Nacrta zakona dodaju standardi 27032, 27005, 27017, 27018, 27701, kao i da se razmotri i o standardu ISO 22301 Sistemi menadžmenta kontinuiteta poslovanja.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 9 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 3: Predloženo je da se u članu 11 stav 2 tačka 1 Nacrta zakona riječi: "politiku analize rizika i bezbjednosti mrežnih i informacionih sistema;" zamijene riječima: "Dokumentovana informacija u kojoj je opisana metodologija za ocjenu i analizu rizika sa aspekta informaicone bezbjednosti", uz obrazloženje da bi time bili obuhvaćeni termini i politika i procedura.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 4 podnositeljke Branke Mićović.

Primjedba/predlog/sugestija 4: Predloženo je da član 5 tačka 11 Nacrta zakona drugačije glasi, i to: "11) ranjivost je slabost, osjetljivost ili nedostatak nekog resursa, sistema, procesa ili kontrole koja može biti eksploatisana (iskorišćena) od strane jedne ili više prijetnji;", uz obrazloženje da bi na taj način bile uključene i ostale prijetnje koje mogu da iskoriste ranjivost neke informacione imovine.

Predlog se ne prihvata.

Obrazloženje:

Nakon sagledavanja pojma ranjivosti utvrđeno je da se isti ne pominje tokom ostalog teksta Nacrta zakona, te samim tim nije potreban ni u izrazima, već će isti biti brisan.

Primjedba/predlog/sugestija 5: Predloženo je da se u članu 25 Nacrta zakona kao član Savjeta Agencije doda i neki člana iz privrednih društava koji pripadaju ključnim i važnim subjektima.

Takođe, predloženo je da se ovom članu dodaju i termini informaciona imovina pod kojom se podrazumijeva sve što ima vrijednost za subjekat, a ona se odnosi na: Informacije, Softvere, Hardvere, Servise, Ljude i njihove kvalifikacije, vještine i iskustva i Nematerijalnu imovinu, kao što je reputacija ili imidž subjekta i prijetnja koja je svaki događaj, situacija ili akcija koja može da ugrozi informacionu bezbjednost subjekta. Takođe je predloženo da se uvede I temin prijetnja na način da glasi: "prijetnja je svaki događaj, situacija ili akcija koja može da ugrozi imformacionu bezbjednost subjekta".

Predlog se ne prihvata.

Obrazloženje:

U odnosu na predlog koji se odnosi na člana Savjeta Agencije odgovor je kao na primjedbu/predlog/sugestiju 4 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

U odnosu na predlog koji se tiče uvođenja termina "informaciona imovina" smatramo da isti nije potreban i ne odgovara konceptu ovog zakona.

U odnosu na predlog za uvođenje termina "prijetnja" odgovor kao na primjedbu/predlog/sugestiju 3 podnositeljke Branke Mićović.

Primjedba/predlog/sugestija 6: U odnosu na član 29 Nacrta zakona kojim se uređuje pitanje direktora Agencije, sugerisano je da je bitno da da direktor ima iskustva na rukovodećim pozicijama u oblasti informacione bezbjednosti i da takođe poznaje zahtjeve

standarda ISO/IEC 27001, što će dokazati dostavljanjem međunarodno priznatog sertifikata za Lead auditora.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 12 Ivana Vujovića.

Primjedba/predlog/sugestija 7: U odnosu na poglavlje VI. Kojim se uređuje nadzor predloženo je da se definiše da inspektori moraju da imaju sertifikate za Lead auditora za standarda ISO/IEC 27001, ISO/IEC 27005 I ISO 22301 i najmanje 3 godine iskustva u oblasti audita sa aspekta informacione bezbjednosti kako bi mogli na adekvatan način da vrše monitoring and primjenom ovog zakona.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 8 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 8: U odnosu na član 11 Nacrta zakona ukazano je da kompletan član treba da se odnosi na rizike sa aspekta informacione bezbjednosti u koje su uključeni i sajber rizici, odnosno da se obuhvatanjem svih rizika informacione imovine na vrijeme detektuju i sajber rizici kako bi se sa istima moglo upravljati.

Predlog se ne prihvata.

Obrazloženje:

Član 11 Nacrta zakona usklađen je sa NIS2 Direktivom čime je definisano da se upravljanje sajber bezbjednosnim rizicima odnosi na primjenu mjera kojima se obezbjeđuje zaštita od sajber prijetnji i incidenata mrežnih i informacionih sistema, korisnika tih sistema i drugih lica na koje one utiču.

6. Crypted Security Integration

Primjedba/predlog/sugestija 1: Predloženo je u bitnom da se tekst Nacrta zakona izmijeni u pogledu izbora termina, a u cilju izbjegavanja mogućnosti nepreciznog ili dvosmislenog tumačenja, uz obrazloženje da termini poput „visok nivo informacione bezbjednosti“, „ozbiljan uticaj“ i slični termini, otvaraju mogućnost slobodnog i proizvoljnog tumačenja, što posljedično može dovesti do umanjenja svrsishodnosti Zakona, kao i da je navedene termine potrebno zamijeniti mjerljivim vrijednostima, ili, alternativno, ustanoviti nacionalni okvir mjerljivih vrijednosti i referencirati tako ustanovljen okvir.

Predlog se ne prihvata.

Obrazloženje:

Termini korišćeni u Nacrtu zakona usklađeni su sa NIS2 Direktivom.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore, dodatno ćemo se konsultovati oko riječi „visok nivo informacione bezbjednosti“.

Primjedba/predlog/sugestija 2: Sugerisano je da postupci za određivanje ključnih i važnih subjekata opisani u Nacrtu zakona i ako do određene mjere jasni i detaljni, ipak ostavljaju prostor za slobodno tumačenje pojma pripadnosti segmentu ključnih i važnih subjekata, uz obrazloženje da treba jasno definisati pripadnost segmentu ključnih i važnih subjekata, ili definisati jasna i nedvosmislena mjerila za prepoznavanje i određivanje ključnih i važnih subjekata.

Predlog se ne prihvata.

Obrazloženje:

Odredbom člana 14 stav 1 Nacrta zakona propisane su obaveze nadležnog sektorskog organa u postupku prepoznavanja ključnih i važnih subjekata, koje između ostalog podrazumijevaju i utvrđivanje sektorskih kriterijuma i kriterijumskih pragova za prepoznavanje ključnih i važnih subjekata, u saradnji sa određenim podsektorom.
Odredbom člana 14 stav 2 definisano je da nadležni sektorski organ određuje sektorske kriterijume uzimajući u obzir karakteristike tih sektora, vrstu i značaj usluga koje taj sektor, odnosno podsektor pruža, dok je odredbom člana 14 stav 3 definisano da kriterijumske pragove određuje na osnovu procjene uticaja sajber prijetnje i incidenta na pružanje usluga, posebno uzimajući u obzir gubitke, ekonomske posljedice, uticaj na nacionalnu bezbjednost, uticaj na javnost i drugo.

Takođe, odredbom člana 15 Nacrta zakona propisani su opšti kriterijumi za prepoznavanje ključnih i važnih subjekata.

Budući da je djelatnost svakog sektora, odnosno podsektora različita zavisno od usluga koje pružaju, te da se ovim zakonom ne mogu definisati jednoobrazni sektorski kriterijumi i kriterijumski pragovi, već samo opšti kriterijumi, mišljenja smo da smo smo kroz propisivanje odredbi člana 14 st. 2 i 3 ostavili jasan osnov za određivanje sektorskih kriterijuma i kriterijumskih pragova.

Primjedba/predlog/sugestija 3: Predloženo je drugačije definisanje izraza u članu 5 Nacrta zakona, uz ukazivanje na potrebu definisanja digitalnog podatka, uz obrazloženje da se isti upotrebljava, a da nije definisan u Nacrtu zakona.

U odnosu na definiciju informaciona bezbjednost ukazano je da se ovakva definicija ne uklapa ni u tradicionalni, ni u savremeni okvir kojim se definišu osnovni stubovi na kojima počiva definicija informacione bezbjednosti, dok je za definiciju izraza sektor navedeno da je u potpunosti nejasna i kao takva, neprihvatljiva.

U odnosu na definiciju kriptovana zaštita ukazano je da je isti u potpunosti nepostojeći i kao takav neprihvatljiv, uz obrazloženje da se radi o kriptofrafskoj zaštiti.

Predlog se djelimično prihvata.

Obrazloženje:

U odnosu na definisanje izraza u članu 5 Nacrta zakona odgovor je kao na primjedbu/predlog/sugestiju 2 podnositeljke Branke Mićović. Što se tiče definicije sektor mišljenja smo da je odgovarajuća, ali ćemo istu sagledati tokom usaglašavanja teksta Nacrta zakona u skladu sa Poslovnikom Vlade Crne Gore, sa relevantnim institucijama.

U odnosu na ukazivanje izraza „kriptovana zaštita" prihvatamo sugestiju da isti bude "kriptografska zaštita".

Primjedba/predlog/sugestija 4: U bitnom je sugerisano da listu regulativa i akata koja se nalazi u članu 11 Nacrta zakona treba izmijeniti u listu mjera kojima će se obezbijediti postizanje i održanje neophodnog nivoa informacione i mrežne bezbjednosti, uz obrazloženje

da takve mjere treba da uključe oblasti kao što su upravljanje konfiguracijama i izmjenama, izradu i pohranjivanje rezervnih kopija podataka, mjere za pouzdanu identifikaciju, mjere za primjenu prava pristupa i slično.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 2 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora. Takođe, član 11 Nacrta zakona usklađen je sa NIS2 Direktivom, te isti smatramo odgovarajućim.

Primjedba/predlog/sugestija 5: Predloženo je u bitnom da se u okviru nacionalnog okvira informacione bezbjednosti sastav, prava i obaveze, kao i hijerarhijska i funkcionalna povezanost Agencije za sajber bezbjednost, Savjeta Agencija za sajber bezbjednost, i Savjeta za informacionu bezbjednost izdvoje u zasebne regulatorne akte, bilo kao Zakon o obrazovanju organa informacione bezbjednosti, bilo kao Uredba o obrazovanju organa informacione bezbjednosti, kako bi se do detalja opisale nadležnosti, obaveze, prava, interno i eksterno funkcionisanje, kao i interna i eksterna komunikaciju, uz obrazloženje da to bude u skladu sa aktuelnom domaćom i međunarodnom regulativom, i potrebama savremenog nacionalnog okvira informacione bezbjednosti.

Takođe je ukazano da je potrebno razdvojiti upravnu, operativnu i kontrolnu ulogu, navodeći kao primjer organe za nadzor i inspektorat koji su u nadležnosti Ministarstva, a koji istovremeno vrše poslove nadzora i kontrole tijela koja su dio Ministarstva. Isto tako ukazano je da nije definisano na koji način će se vršiti stručni nadzor nad primjenom informacione bezbjednosti propisane međunarodnim standardom ISO/IEC 27001.

U odnosu na članove Savjeta za informacionu bezbjednost sugerisano je da članovi Savjeta moraju zadovoljavati kriterijume koji moraju sadržati u sebi i odrednice vezane za informacionu bezbjednost (kao što su npr. obavljanje profesionalnih zadataka u prethodnom profesionalnom angažovanju na poslovima informacione bezbjednosti, posjedovanje globalno priznatih i prepoznatih sertifikata iz oblasti informacione bezbjednosti u adekvatnom trajanju i slično).

Predlog se ne prihvata.

Obrazloženje:

U skladu sa važećom zakonskom regulativom u Crnoj Gori mišljenja smo da obrazovanje i nadležnosti Agencije za sajber bezbjednost, Savjeta Agencija za sajber bezbjednost i Savjeta za informacionu bezbjednost ne mogu biti uređene drugim posebnim aktima, već je upravo ovaj zakon osnov za njihovo uspostavljanje. Što se tiče Savjeta za informacionu bezbjednost posebnim aktom o obrazovanju će se uraditi zadaci, način rada, i druga pitanja od značaja za rad Savjeta, što je propisano u članu 34 stav 6 Nacrta zakona. Takođe, nižim pravnim aktim koje će donositi Agencije će se urediti kako način rada Savjeta Agencije, tako i ostala bitna pitanja za rad Agencije.

Jedan od načina vršenja stručni nadzor nad primjenom informacione bezbjednosti propisane međunarodnim standardom ISO/IEC 27001 vrši se na način tako sto ce vlasnik dostaviti na uvid sertifiakt ISO 27001 dobijen od akreditovane organizacije za izdavanje istih.

Što se tiče stručnog i inspekcijskog nadzora, inspekcijski nadzor nije u nadležnosti ministarstva već u organu uprave (Uprava za inspekcijske poslove), te smo ovim rješenjem nastojali da kroz uloge stručnog nadzora i inspektora omogućimo efikasniju primjenu ovog zakona i nadzor nad istim.

Savjet za informacionu bezbjednost nije organ upravljanja, već savjetodavno tijelo privremenog karaktera, te smo mišljenja da se uslovi za članove Savjeta ne mogu propisivati.

Primjedba/predlog/sugestija 6: Predloženo je da se u članu 12 Nacrta zakona definiše pojam organa, uz obrazloženje da u članu 12 ne postoji prethodno jasna odrednica organa, kao da se definiše pojam akta, budući u članu 34 Nacrta zakona pominje "Akt o obrazovanju Savjeta iz stava 5 ovog člana", uz ukazivanje da stav 5 člana 34 specificira pravo na naknadu za rad predsjedniku, članovima i sekretaru Savjeta za informacionu bezbjednost.

Predlog se ne prihvata.

Obrazloženje:

U skladu sa pravno-tehničkim pravilima izrade propisa pojam organi definisan je u odredbi člana 2 Nacrta zakona, gdje se prvi put uvodi taj pojam.

U odnosu na ukazivanje na član 34 Nacrta zakona gdje se pominje "Akt o obrazovanju Savjeta iz stava 5 ovog člana" misli se na Savjet za informacionu bezbjednost koji se pominje u stavu 5 ovog člana.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore, sagledaćemo da li je definisano u skladu sa pravno-tehničkim pravilima izrade propisa.

Primjedba/predlog/sugestija 7: Sugerisano je da u odnosu na međunarodni standard ISO/IEC 27001, koji se pominje na više mjesta u tekstu Nacrta zakona nije jasno specificirano koja verzija standarda se primjenjuje, niti je naveden razlog primjene navedenog standarda, uz obrazloženje da je pomenuti ISO standard nesumnjivo jedan od referentnih globalnih standarda informacione bezbjednosti, čija primjena istog se podržava ali da je neophodno obrazložiti razlog prihvatanja navedenog standarda kao dijela Zakona, kao i specificirati verziju standarda koja će se primijeniti.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 9 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 8: U odnosu na poglavje VII. Koje se odnosi na kaznene odredbe sugerisno je da su predviđene kazne izuzetno niske, i da se njima neće postići svrha kažnjavanja.

Predlog se ne prihvata.

Obrazloženje:

Zakon o prekršajima ("Službeni list CG", br. 1/11, 6/11, 39/11, 32/14 i 51/17) između ostalog propisuje između ostalog propisuje raspon i iznos u kom se novčana kazna može propisati, te je ovaj zakon u dijelu novčanih kazni neophodno uskladiti sa Zakonom o prekršajima.

Napomena: Organ državne uprave u čijoj je nadležnosti Zakon o prekršajima daje mišljenje na tekst Nacrta zakona o informacionoj bezbjednosti, u dijelu kaznenih odredbi, u skladu sa Poslovnikom Vlade Crne Gore.

Primjedba/predlog/sugestija 9: U članu 59 Nacrta zakona predloženo je da se propisani rok za sertifikaciju u skladu sa standardom ISO/IEC 27001 smanji na 18 mjeseci (maksimalan rok), uz obrazloženje da je propisan rok od 30 mjeseci previše dugačak.

Predlog se ne prihvata.

Obrazloženje:

Nacrt zakona o informacionoj bezbjendosti razmatran je i na sjednici Savjeta za informacionu bezbjednost, te se jedna od preporuka članova Savjeta odnosila na produžetak roka na 30

mjeseci. Mišljenja smo da svi potencijalni ključni subjekti nijesu spremni za kraći rok od 30 mjeseci.

Primjedba/predlog/sugestija 10: Predloženo je da se u Nacrtu zakona urede precizne mjere kojima će se postići i održavati neophodan nivo informacione bezbjednosti, budući da se u ovakvom tekstu Nacrta zakona u potpunosti izostavljaju oblasti kojima se propisuju obaveze iz oblasti edukacije, podizanja svijesti, zaštite javnog interesa i zaštite od hibridnih prijetnji.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 4.

Primjedba/predlog/sugestija 11: Predloženo je da se izraditi predlog rebalansa republičkog budžeta kojim će biti obuhvaćene sve aktivnosti koje proističu iz ovog Zakona.

Predlog se ne prihvata.

Obrazloženje:

U nadležnosti Ministarstva javne uprave nije izrada predloga Budžeta, a tekst Nacrta zakona će shodno Poslovniku Vlade Crne Gore, svakako biti dostavljen na mišljenje organu državne uprave nadležnom za psolove finansija.

7. Američka privredna komora u Crnoj Gori (AmCham)

Primjedba/predlog/sugestija 1: Predloženo je da se član 2 Nacrta zakona izmijeni na način da glasi: *"*Prema odredbama ovoga zakona obavezni su da postupaju državni organi, organi državne uprave, organi jedinica lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, pravna lica sa javnim ovlašćenjima (u daljem tekstu: organi), kao i druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemima, a koji se dijele na ključne i važne subjekte, u smislu ovog zakona.", uz obrazloženje da bi se na ovaj način jasno definisali termini "organ", "ključni" i "važni" subjekti, a sve u cilju da svaki subjekat nedvosmisleno može jasno da prepozna kategoriju kojoj pripada.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 1 podnosioca One Crna Gora doo.

Primjedba/predlog/sugestija 2: Predloženo je da se član 5 stav 1 tač. 7 i 8 dopune na način da glase:

"7) sajber prijetnja je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na podatke i mrežne i informacione sisteme, korisnike tih sistema i druge organe i lica, a koja je poznata vlasniku mrežnih i informacionih sistema;".

"8) ozbiljna sajber prijetnja je sajber prijetnja za koju se na osnovu njenih tehničkih obilježja može pretpostaviti da može imati ozbiljan uticaj na mrežne i informacione sisteme nekog subjekta ili korisnika usluga subjekta uzrokovanjem značajne materijalne ili nematerijalne štete, a koja je poznata vlasniku mrežnih i informacionih sistema;".

Pojašnjeno je da bi se na ovaj način dodatno pojasnili izrazi sajber prijetnje i ozbiljne sajber prijetnje kako se ne bi nametala obaveza subjektu da reaguje ili postupa na neki način ukoliko ni sam nije upoznat sa postojanjem konkretne prijetnje.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 2 podnosioca One Crna Gora doo.

Primjedba/predlog/sugestija 3: Predloženo je da se član 20 izmijeni tako da jasno i nedvosmisleno ukazuje na obavezu sertifikacije ključnih subjekata, a u skladu sa članom 59 koji propisuje rok za primjenu ove obaveze od 30 mjeseci od dana stupanja na snagu Zakona.

Predlog se prihvata.

Obrazloženje:

Odredba člana 20 će biti usklađena sa datim predlogom.

Primjedba/predlog/sugestija 4: Predloženo je da se u okviru člana 23, u djelokrug rada Agencije decidno uvrsti i podizanje svijesti o sajber bezbjednosti organa, nadležnih sektorskih organa i ključnih i važnih subjekata, ali i šire javnosti kroz kampanje usmjerene na podizanje svijesti o opštim principima sajber bezbjednosti (sajber higijena).

Takođe je ukazano da bi s obzirom da je u tački 7 predviđeno da Agencija postupa po prijavljenim incidentima ključnih i važnih subjekata, osim organa državne uprave, trebalo jasno propisati ko postupa po prijavljenim incidentima organa državne uprave, jer je to u Nacrtu zakona ostalo nedorečeno.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da je predloženo u odredbi člana 23 uključeno kroz tač. 12 Nacrta zakona, u kojima je navedeno da Agencija vrši edukaciju organa, nadležnih sektorskih organa i ključnih i važnih subjekata kroz savjetovanja i obuke u cilju jačanja informacione bezbjednosti, čime se ne ograničava ni podizanje svijesti o sajber bezbejdnosti.

Primjedba/predlog/sugestija 5: Predloženo je da se u članu 25 Nacrta zakona izmijeni sastav Savjeta Agencije na način da privreda i akademija budu više zastupljeni u ovom tijelu, i to kroz dva člana koje bi predlagala udruženja privrednika, kao i dva člana koje bi predlagali univerziteti u Crnoj Gori (državni ili privatni).

Takođe je ukazano da član ovoga tijela ne treba da bude neko ko je zaposlen u Agenciji, zbog postojanja sukoba interesa.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 3 podnosioca One Crna Gora.

Primjedba/predlog/sugestija 6: U odnosu na član 29 stav 2 ukazano je da treba preispitati posebne uslove koji se traže za direktora Agencije, uz pojašnjenje da propisani uslovi “tri godine radnog iskustva u oblasti infromacione bezbjednosti ili sedam godina radnog iskustva u državnim organima ili deset godina radnog iskustva” ne zahtijevaju preveliku stručnost kako bi se obavljala odgovorna funkcija kakvu podrazumijeva funkcija direktora Agencije.

Predlog je da se propišu restriktivniji uslovi po pitanju radnog iskustva kako na obavljanju specifičnih poslova, tako i na rukovodećim pozicijama, kako bi se osiguralo da funkciju direktora Agencije pokriva lice značajnih profesionalnih kompetencija, visokorukovodnog kadra.

<u>Predlog se djelimično prihvata.</u>

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 6 Branke Mićović u odnosu na sugestiju u dijelu godina radnog iskustva u oblasti infromacione bezbjednosti, dok je u dijelu uslova kada je u pitanju rukovodeće iskustvo odgovor kao na primjedbu/predlog/sugestiju 12 Ivana Vujovića.

Primjedba/predlog/sugestija 7: Predloženo je da se član 34 stav 2 dopuni na način da glasi: *"*Savjet iz stava 1 ovog člana, čine predstavnici organa državne uprave nadležnog za unutrašnje poslove, organa državne uprave nadležnog za poslove odbrane, organa državne uprave nadležnog za poslove pravosuđa, organa državnog uprave nadležnog za vanjske poslove, organa uprave nadležnog za tajne podatke, Ministarstva, Agencije i Agencije za nacionalnu bezbjednost, vlasnika mrežnih i informacionih sistema, a po potrebi i predstavnici drugih organa i institucija.".

Takođe je predloženo da se ostavi prostor Savjetu za informacionu bezbjednost da, po potrebi, može osnivati stručne radne grupe radi sveobuhvatnijeg pristupa prikupljanju potrebnih informacija u cilju predlaganja aktivnosti Agenciji i Ministarstvu na uspostavljanju sistema zaštite od sajber prijetnji i incidenata, kao i razmatranja stručnih pitanja u oblasti informacione bezbjednosti, kao i da stručne radne grupe, u skladu sa konkretnom potrebom, mogu da čine predstavnici privatnog i civilnog sektora i akademije.

Pojašnjeno je da bi na ovaj način u radu ovako bitnog tijela budu uključeni i predstavnici privrede koji su vlasnici mrežnih i informacionih sistema (energetski sektor, banke, komunikacioni operatori i drugi), a što bi bio jedan od pokazatelja unapređenja javnog i privatnog partnerstva koje je predviđeno Strategijom sajber bezbjednosti 2022-2026 koju je Vlada Crne Gore usvojila u decembru 2021. godine.

<u>Predlog se ne prihvata</u>.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 4 podnosioca One Crna Gora. U odnosu na predlog da se Savjetu za informacionu bezbjednost ostavi da, po potrebi, može osnivati stručne radne grupe, odredbom člana 34 stav 6 Nacrta zakona propisano je da se aktom o obrazovanju Savjeta utvrđuju se zadaci, način rada, i druga pitanja od značaja za rad Savjeta, što podrazumijeva i obrazovanje stručnih grupa.

Primjedba/predlog/sugestija 8: U okviru člana 35 sugerisano je da Vladin CIRT u Zakonu ili nije definisan kako treba, ili nije pozicioniran kako treba. Naime, Vladin CIRT je u članu 35 Zakona – Nadležnosti Ministarstva, pozicioniran kao posebna organizaciona jedinica Ministarstva, što ne korespondira sa njegovim nazivom "Vladin CIRT". Neophodno je razgraničiti sve nadležnosti, pozicionirati nadležne organe u okviru Vlade i uspostaviti jasnu hijerarhiju kod rješavanja incidenata, imajući u vidu da kada se desi incident, treba reagovati promptno.

Ukazano je da treba jasnije urediti ko i kada djeluje u slučaju incidenta, da li jedan ili drugi organ ili skupa, te ko, u krajnjem, donosi odluku da u konkretnom kriznom slučaju postupa Agencija odnosno Vladin CIRT ili Agencija i Vladin CIRT.

<u>Predlog se ne prihvata</u>.

Obrazloženje:

Mišljenja smo da su nadležnosti Agencije za sajber bezbjednost i Vladinog CIRT-a jasno definisane kroz odredbe čl. 23, 35, a posebno u slučaju postupanja po prijavljenim incidentima čl. 37 do 45 Nacrta zakona (poglavlje V. Upravljanje sajber bezbjednošću). Takođe, Vladin CIRT je skraćenica, budući da se koristi u ostalom tekstu zakona.

Primjedba/predlog/sugestija 9: Predlaženo da se u članu 36 stav 1 tačka 6 uvrsti i odrednica da Agencija i Vladin CIRT moraju imati dovoljan broj zaposlenih koji su adekvatno obučeni za sprovođenje svih ovlašćenja predviđenih zakonom, uključujući i vršenje uloge nadzornika.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 5 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 10: Predlaženo je da se član 37 stav 2 izmijeni na način da glasi: "Ključni i važni subjekti osim organa državne uprave, dužni su da Agenciji jednom mjesečno dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga.", uz obrazloženje da je predložena izmjena stava 2 u skladu sa članom 2, a i u duhu odredbi člana 37 stav 3.

Dalje je predlaženo da se stav 6 izmijeni na način da glasi: "Ključni i važni subjekti dužni su da obavijeste afektovane primaoce svojih usluga o svim ozbiljnim sajber prijetnjama i incidentima, a koji bi mogli negativno da utiču na pružanje njihovih usluga, kao i o svim mjerama koje bi ti primaoci usluga trebalo da preduzmu kao odgovor na sajber prijetnje i incidente.", uz obrazloženje da je predlog izmjene stava 6 dat sa ciljem da preciznije definiše obaveza ključnih i važnih subjekata u pogledu potrebe komunikacije ka primaocima usluge.

Predloženo je da se stav 8 izmijeni na način da glasi: "Izvještaje iz st. 2 i 3 ovog člana i obavještenja iz st. 4 do 7 ovog člana, Agencija i/ili Vladin CIRT označavaju sa odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.", uz obrazloženje da je predlog dopune stava 8 dat iz razloga što pravna lica koja nisu državni organi nemaju pravo da označavaju dokumenta sa određenim stepenom tajnosti.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 5, 6, 7 i 8 One Crna Gora doo.

Primjedba/predlog/sugestija 11: Predloženo je da se član 38 stav 1 tačka 3 dopuni na način da glasi: *"3) geografskoj raširenosti incidenta, ukoliko je primjenljivo;".* Recimo za mobilne operatore pitanje geografske raširenosti se ne može jasno odrediti zbog same prirode usluge.

Takođe, predloženo je da se u kriterijume za incidente sa značajnim uticajem na kontinuitet pružanja usluga iz stava 1 uvrsti dodatna tačka koja se odnosi na uticaj na druge sektore, imajući u vidu među-sektorsku povezanost u određenim domenima sajber bezbjednosti, kao i neophodnost upravljanja rizicima u okviru lanca snabdijevanja.

Predlog se prihvata.

Obrazloženje:

Predloženo će biti inkorporirano u Nacrt zakona.

Primjedba/predlog/sugestija 12: Predloženo da se u članu 39 doda stav 2 kojim bi se propisala forma (obrazac) za dostavljanje obavještenja o incidentu kako bi se vrsta i obim informacija standardizovala i kako bi se obezbijedilo prikupljanje dovoljne količine relevantnih informacija u svakoj od faza razvoja incidenta: *"Bliži način i formu dostavljanja obavještenja i izvještaja iz stava 1 ovog člana uređuje Ministarstvo".*

Predlog se prihvata.

Obrazloženje:

Propisaćemo osnov za donošenje podzakonskog akta.

Primjedba/predlog/sugestija 13: Sugerisano je da u okviru člana 43 nije jasan odnos Agencije i Vladinog CIRTA-a, uz pojašnjenje da Agencija za sajber bezbjednost, koja se osniva ovim zakonom, postavljena je kao krovni, Vladin organ za informacionu bezbjednost, a ima i ulogu koordinacije među nadležnim organima i saradnje sa svim subjektima koji su nadležni po ovom zakonu. Ukazano je da u navedenom članu Agencija i Vladin CIRT rješavaju incidente i preduzimaju aktivnosti uporedo, odnosno ili jedan ili drugi (jer u ovom članu imamo odrednice: Agencija odnosno Vladin CIRT, Agencija i Vladin CIRT), što pravi zabunu, i nadležnost Vladinog CIRT-a u dijelu zakona stavlja u nivo nadležnosti Agencije, što ne bi trebalo da je slučaj. Sugerisano je da je potrebno jasno razgraničiti i utvrditi njihove nadležnosti.

Predloženo je da se član 43 stav 12 izmijeni na način da glasi: "Obavještenja iz stavova 2, 3, 4, 6 i 8 ovog člana, kao i predlog akta Vladi iz stava 10 ovog člana, Agencija i/ili Vladin CIRT označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka", uz obrazloženje da pravna lica koja nisu državni organi nemaju pravo da označavaju dokumenta sa određenim stepenom tajnosti.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 10.

Primjedba/predlog/sugestija 14: Predloženo je da se član 49 stav 1 tačka 9 izmijeni na način da glasi: "9) naloži da obavijeste afektovane primaoce svojih usluga o sajber prijetnjama i incidentima koji bi mogli negativno uticati na pružanje njihovih usluga, kao i o svim mjerama koje bi trebali preduzeti kao odgovor na sajber prijetnje i incidente;", uz obrazloženje da se na ovaj način preciznije definiše obaveza ključnih i važnih subjekata u pogledu potrebe komunikacije ka primaocima usluge.

Predloženo je da se član 49 stav 1 tačka 11 izmijeni na način da glasi: "11) privremeno zabrani rad i pružanje usluga, do trenutka otklanjanja ozbiljne sajber prijetnje i incidenta, a koji mogu imati negativan uticaj na podatke i mrežne i informacione sisteme, korisnike tih sistema i druge ključne i važne subjekte i organe.", uz obrazloženje da se na ovaj način preciznije definiše pravo inspektora, ali i da se ograniče moguće posljedice po ključne i važne subjekte.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 11 I 12 One Crna Gora doo.

Primjedba/predlog/sugestija 15: Predloženo je da se član 51 stav 4 izmijeni na način da glasi: *"Agencija može, osim nadzornika,* ovlastiti i druga zaposlena lica da na licu mjesta (uz prisustvo nadzornika), kod ključnih i važnih subjekata, izvrše kontrolu i uzimanje podataka neophodnih za izvršavanje poslova iz nadležnosti Agencije.", uz obrazloženje da je predlog izmjene je dat iz razloga što smatramo neosnovanim da bilo koje lice iz Agencije, bez prisustva nadzornika, može vršiti stručni nadzor nad subjektom.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 13 One Crna Gora doo.

Primjedba/predlog/sugestija 16: Predloženo je da se u okviru kaznenih odredbi u čl. 54, 55 i 56 treba izmijeniti stav 2 tako da jasno ukazuje da će se novčana kazna izreći odgovornom fizičkom licu u pravnom licu.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da je definisana norma odgovarajuća.

Napomena: Organ državne uprave u čijoj je nadležnosti Zakon o prekršajima daje mišljenje na tekst Nacrta zakona o informacionoj bezbjednosti, u dijelu kaznenih odredbi, u skladu sa Poslovnikom Vlade Crne Gore.

Primjedba/predlog/sugestija 17: U okviru člana 62 predloženo je da se umjesto striktno datumski definisanog roka stav 1 preformuliše tako da ukazuje na vremenski period u odnosu na datum usvajanja Zakona (npr. XX mjeseci od dana stupanja na snagu ovog zakona).

Predlog se ne prihvata.

Obrazloženje:

Smatramo da je potrebno znati tačan datum početka rada Agencije.

8. Agencija za elektronske komunikacije i poštansku djelatnost

Primjedba/predlog/sugestija 1: Predloženo je da se u članu 5 stav 1 tačka 1 alineja 1 izmjeni i glasi:

“elektronsku komunikacionu mrežu kako je definisana zakonom kojim se definiše oblast elektronskih komunikacija”, uz obrazloženje da je elektronska komunikaciona mreža jdefinisana Zakonom o elektronskim komunikacija, koji je krovni zakon za oblast elektronskih komunikacija i logično je da postoji samo ta definicija.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da predloženi način definisanja nije pravno-tehnički, ali ćemo definiciju elektronske komunikacione mreže dodatno sagledati kako bi ista bila usklađena sa propisom kojim se uređuje oblast elektronskih komunikacija.

Primjedba/predlog/sugestija 2: Predloženo je da se član 13 stav 2 tačka 8 izmjeni tako da se dodaju subjekti koji mogu biti ključni subjekti, a koji su navedeni u Prilogu 1. NIS2 direktive, pod rednim brojem 8. Digitalna infrastruktura, iz razloga da se tačno navedu subjekti koji mogu spadati u kategoriju ključnih subjekata, da bi se izbjeglo bilo kakvo tumačenje. Sugerisano je da se razmisli i da se ovo primjeni i na cijelu listu datih sektora, da se odrede subjekti koji mogu biti ključni.

Predlog se ne prihvata.

Obrazloženje:

Mišljenja smo da dodavanje priloga Nacrtu zakona u kom bi se navela vrsta subjekata nije pravno-tehnički prihvatljivo, što ćemo dodatno sagledati sa nadležnim organom koji shodno Poslovniku Vlade Crne Gore daje mišljenje na Nacrt zakona. Ukoliko bude pravno-tehnički moguće uredićemo i taj dio.

Primjedba/predlog/sugestija 3: Sugerisano je da je član 43 stav 8 je u koliziji sa članom 23, stav 1, tačka 7, uz obrazloženje da se u članu 23 stav 1 tačka 7 se navodi da Agencija postupa po prijavama ključnih i važnih subjekata, osim organa državne uprave, a onda u članu 43, stav 8, se navodi da zajedno Agencija i Vladin CIRT rješavaju incidente visokog

nivoa, te da bi trebalo još jednom preispitati nadležnosti Ministarstva, Vladinog CIRT-a i Agencije i njihovu međusobnu saradnju.

Predlog se ne prihvata.

Obrazloženje:

Smisao odredbe člana 43 stav 8 Nacrta zakona je zajedničko postupanje Agencije i Vladinog CIRT-a kada se radi o incidentu sa značajnim uticajem na kontinuitet pružanja usluga visokog nivoa, što je izuzetak od odredbe člana 23 stav 1 tačka 7 Nacrta zakona.

Napomena: Tokom usaglašavanja teksta ovog zakona sa relevantnim institucijama, u skladu sa Poslovnikom Vlade Crne Gore dodatno ćemo se konsultovati da li je ova odredba odgovarajuća.

9. Branimir Bošnjak

Primjedba/predlog/sugestija 1: Sugerisano je da je u članu 2 Nacrta zakona zbog korišćenja zareza i više puta veznika "i" koji se po pravilu mora nalaziti jedino na kraju nabrajanja ostaje nejasno ko su obveznici primjene ovog zakona.

Predlog se prihvata.

Obrazloženje:

Biće pravno-tehnički uslađeno.

Primjedba/predlog/sugestija 2: Predloženo je da se u članu 5 Nacrta zakona umjesto termina "mrežni i informacioni sistem", koristi termin „informacioni sistem", uz obrazloženje da korišćenje termina "mrežni i informacioni sistem" kao složenice nepotrebno dovodi do komplikacija u razumijevanju daljeg teksta zakona jer sadržaj rečenice umetanjem ovog termina često postaje teže razumljiv.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 1 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 3: Sugerisano je da u članu 5 Nacrta zakona termin sajber kriza nije objašnjen na pravi način, uz obrazloženje da se iz ovako definisanog termina ne može zaključiti da je riječ o događaju u domenu IT-a već možemo pomisliti da se radi o nekim drugim nepogodama (poplave, zemljotresi, rat, pandemija…).

Predlog se prihvata.

Obrazloženje:

U skladu sa datim predlogom termin će biti preciznije definisan.

Primjedba/predlog/sugestija 4: U odnosu na član 9 Nacrta zakona primjedba je u smislu da se vidi nespretno uvođenje termina "mrežni i informacioni sistemi" koje daje teško razumljiv sadržaj rečenici.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 1 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

Primjedba/predlog/sugestija 5: U odnosu na član 13 Nacrta zakona sugerisano je da uvođenje pod tačkom 11 kao sektora “svemir” nema nekog smisla, uz pojašnjenje da svemir obuhvata sve oko nas i da ne možemo tako definsati sektor.

Predlog se ne prihvata.

Obrazloženje:

Sektori su sklađeni sa NIS 2 Direktivom, pa samim tim i svemir.

Primjedba/predlog/sugestija 6: U odnosu na član 17 sugerisano je da naslov člana 17 koristi termin “kritični” a prethodno se pominjao termin “ključni”.

Predlog se prihvata.

Obrazloženje:

Tehički propust, biće korigovano.

Primjedba/predlog/sugestija 7: U odnosu na član 29 koji definiše ko može biti direktor Agencije sugerisano je da treba biti istaknuto iskustvo iz oblasti informatike ili informatičke bezbjednosti, kako bi se radilo o kompetentnosti i stručnosti u ovoj oblasti.

Predlog se prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 6 Branke Mićović.

Primjedba/predlog/sugestija 8: U odnosu poglavlje VI. Nadzor sugerisano je da inspektor i nadzornik moraju imati određene sertifikate za obavljanje ovih poslova.

Predlog se ne prihvata.

Obrazloženje:

Odgovor kao na primjedbu/predlog/sugestiju 8 podnosioca ICT Cortex (Coinis doo) Podgorica, Crna Gora.

M**jesto i datum sačinjavanja Izvještaja**: Podgorica, 04. 04. 2023. godine.

Naziv organizacione jedinice koja je odgovorna za pripremu Nacrta zakona: Direktorat za infrastrukturu, informacionu bezbjednost, digitalizaciju i e-servise.

mr Marash Dukaj
M I N I S T A R

Marash Dukaj
Digitally signed by Marash Dukaj
Date: 2023.04.04 14:05:04 +02'00'