CRNA GORA
MINISTARSTVO UNUTRAŠNJIH POSLOVA
Odjeljenje za zaštitu podataka o ličnosti
i slobodan pristup informacijama
39 Broj: UPI – 007/19-4464/3
Podgorica, 24.10.2019.godine

Ministarstvo unutrašnjih poslova - Odjeljenje za zaštitu podataka o ličnosti i slobodan pristup informacijama, na osnovu člana 30 Zakona o slobodnom pristupu informacijama („Službeni list CG", broj: 44/12 i 30/17) i člana 18 Zakona o upravnom postupku („Službeni list CG", br.56/14, 20/15, 40/16 i 37/17) rješavajući zahtjev za pristup informacijama Instituta Alternativa, donosi

RJEŠENJE

1. Odobrava se pristup informaciji u posjedu Ministarstva unutrašnjih poslova-informacija o kopiji izrađenog Predloga zakona o kritičnoj infrastrukturi i ostalo.

2. Odobrenje iz tačke 1 dispozitiva, izvršiće se na način dostavljanjem kopije informacije.

OBRAZLOŽENJE

Institut Alternativa, podnio je zahtjev za pristup informacijama-informacija o kopiji izrađenog Predloga zakona o kritičnoj infrastrukturi i ostalo.

Ministarstvo unutrašnjih poslova je nadležan organ shodno važećim zakonima, te se tražene informacije nalaze u posjedu ovog organa.

Razmatrajući zahtjev Instituta Alternativa, organ je zaključio da je zahtjev opravdan, te da se istom treba udovoljiti.

Na osnovu izloženog, odlučeno je kao u dispozitivu rješenja.

Upustvo o pravnoj zaštiti:

Protiv ovog rješenja dopuštena je žalba Agenciji za zaštitu ličnih podataka i slobodan pristup informacijama, u roku od 15 dana, od dana prijema ovog rješenja. Žalba se predaje ovom organu ili šalje putem pošte.

Rješenje je oslobođeno plaćanja takse, shodno članu 33 Zakona o slobodnom pristupu informacijama („Službeni list CG", broj: 44/12).

Ovlašćeni službenik za
vođenje postupka
Ana Kostić
Ana Kostić

Crna Gora
Ministarstvo unutrašnjih poslova

Adresa: Bulevar Sv. Petra Cetinjskog 22,
81000 Podgorica, Crna Gora
tel: +382 20 241 590
fax: +382 20 246 779
www.mup.gov.me

Direktorat za strateško-razvojne poslove

02 Br: UP1-007/19-4464/2

15. oktobar 2019.

Za: **ODJELJENJE ZA ZAŠTITU PODATAKA O LIČNOSTI I SLOBODAN PRISTUP INFORMACIJAMA**

- Načelnici, g-đi Zori Čizmović

Predmet: Zahtjev za slobodan pristup informacijama

Uvažena g-đo Čizmović,

U vezi sa dopisom NVO "Institut alternativa" broj UP1-007/19-4464/2 kojim je podnijet zahtjev za pristup određenim dokumentima i informacijama o sprovođenju aktivnosti u trećem kvartalu 2019. godine, iz domena nadležnosti Direktorata za strateško razvojne poslove obavještavamo sljedeće:

- u toku je izrada obaveznog Programa upravljanja ljudskim resursima koja se vrši u saradnji sa međunarodnim partnerima. Planirano je da Program bude izrađen 24. 10. 2019. godine, nakon čega ćemo biti u mogućnosti da pošaljemo kopiju;

- obuke na temu "Upravljanje ljudskim resursima" za rukovodioce Uprave policije realizovaće se nakon donošenja gore pomenutog programa.

Takođe, s obzirom da je traženo i dostavljanje kopije izrađenog Predloga zakona o kritičnoj infrastrukturi, to vam istu u prilogu dostavljamo.

S poštovanjem,

GENERALNI DIREKTOR,

mr Safet Korać

Safet Korać

Prilog: - Predlog zakon o kritičnoj infrastrukturi

PREDLOG

ZAKON O ODREĐIVANJU I ZAŠTITI KRITIČNE INFRASTRUKTURE*

I. OSNOVNE ODREDBE

Predmet
Član 1

Kritična infrastruktura određuje se i štiti na način i pod uslovima propisanim ovim zakonom, međunarodnim ugovorima i standardima Evropske unije.

Kritična infrastruktura
Član 2

Kritična infrastruktura obuhvata sisteme, mreže, objekte, odnosno njihove djelove koji se nalaze na teritoriji Crne Gore, čiji prekid funkcionisanja,odnosno prekid isporuka roba ili usluga preko tih sistema, mreža, objekata, odnosno njihovih djelova može imati ozbiljne posljedice po nacionalnu bezbijednost, zdravlje i život ljudi, imovinu, životnu sredinu, bezbjednost građana, ekonomsku stabilnost, odnosno vršenje djelatnosti od javnog interesa.

Zaštita kritične infrastrukture
Član 3

Zaštita kritične infrastrukture predstavlja skup aktivnosti i mjera koje imaju za cilj da spriječe nastanak poremećaja u radu, oštećenje ili uništenje kritične infrastrukture u slučaju prijetnje, obezbijede funkcionisanje kritične infrastrukture u slučaju poremećaja u radu ili oštećenja i spriječe nastanak posljedica poremećaja u radu, odnosno oštećenja ili uništenja kritične infrastrukture.

Upotreba rodno osjetljivog jezika
Član 4

Izrazi koji se u ovom zakonu koriste za fizička lica u muškom rodu podrazumijevaju iste izraze u ženskom rodu.

Značenje izraza
Član 5

Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

1) operatori kritične infrastrukture su državni organi, organi državne uprave, organi lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva i druga pravna lica koji koriste, odnosno upravljaju sistemima, mrežama, objektima, odnosno njihovim djelovima koji su određeni kao kritična infrastruktura;

2) analiza rizika podrazumijeva razmatranje mogućih opasnosti i prijetnji radi procjene mogućih posljedica poremećaja u radu ili mogućeg prekida funkcionisanja kritične infrastrukture, njenog oštećenja, odnosno uništenja;

3) kritična informatička infrastruktura obuhvata informacione sisteme kojima upravljaju operatori kritične infrastrukture, čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa;

4) osjetljive informacije o zaštiti kritične infrastrukture su informacije o kritičnoj infrastrukturi koje bi se, kad bi bile otkrivene, mogle upotrijebiti za planiranje i preduzimanje aktivnosti kojima će se izazvati poremećaj u radu ili prekid funkcionisanja kritične infrastrukture, odnosno njeno oštećenje ili uništenje;

5) Evropska kritična infrastruktura podrazumijeva kritičnu infrastrukturu koja se nalazi na teritoriji države članice Evropske unije, čiji bi poremećaj u radu, prekid funkcionisanja, oštećenje ili uništenje imalo značajne posljedice za najmanje dvije države članice.

II. ODREĐIVANJE KRITIČNE INFRASTRUKTURE

Kriterijumi za određivanje kritične infrastrukture
Član 6

Kritična infrastruktura određuje se na osnovu kriterijuma koji se odnose na procjenu mogućih posljedica poremećaja u radu ili mogućeg prekida funkcionisanja kritične infrastrukture u oblasti energetike, saobraćaja, snabdijevanja vodom, zdravstva, finansija, elektronskih komunikacija i informaciono-komunikacionih tehnologija, zaštite životne sredine, funkcionisanja državnih organa, kao i u drugim oblastima od javnog interesa (u daljem tekstu: kriterijumi za određivanje kritične infrastrukture).

Kriterijumi za određivanje kritične infrastrukture mogu biti sektorski i međusektorski.

Sektorski kriterijumi za određivanje kritične infrastrukture
Član 7

Sektorski kriterijumi za određivanje kritične infrastrukture utvrđuju se na osnovu analiza rizika koje za svaki sektor kritične infrastrukture sačinjavaju ministarstva nadležna za određene sektore, uzimajući u obzir karakteristike tih sektora.

Sektorske kriterijume za određivanje kritične infrastrukture propisuje Vlada Crne Gore (u daljem tekstu: Vlada).

Akt iz stava 2 ovog člana označava se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

Međusektorski kriterijumi za određivanje kritične infrastrukture
Član 8

Međusektorski kriterijumi za određivanje kritične infrastrukture utvrđuju se na osnovu analize rizika koja se odnosi na sve sektore kritične infrastrukture.

Međusektorski kriterijumi iz stava 1 ovog člana su:

- mogući broj poginulih ili povrijeđenih zbog ozbiljnih poremećaja u radu ili prekida funkcionisanja kritične infrastrukture;

- ekonomske posljedice, mogući ekonomski gubici i/ili pogoršanje kvaliteta proizvoda ili usluga, kao i moguće posljedice po okolinu zbog ozbiljnih poremećaja u radu ili prekida funkcionisanja kritične infrastrukture;

- uticaj na javnost, odnosno moguće posljedice poremećaja u radu ili prekida funkcionisanja kritične infrastrukture na povjerenje javnosti i redovne životne aktivnosti.

Sistem, mreža, objekat, odnosno njihov dio može se odrediti kao kritična infrastruktura ako ispunjava najmanje jedan kriterijum iz stava 2 ovog člana.

Sektori kritične infrastrukture

Član 9

Sektori kritične infrastrukture su oblasti u kojima se vrši identifikacija i određivanje kritične infrastrukture, i to energetika, saobraćaj, snabdijevanje vodom, zdravstvo, finansije, elektronske komunikacije, informaciono-komunikacionetehnologije, zaštita životne sredine, funkcionisanje državnih organa, kao i druge oblasti od javnog interesa.

Obaveza operatora kritične infrastrukture

Član 10

Ministarstva nadležna za sektore za koje su utvrđeni sektorski kriterijumi za određivanje kritične infrastrukture operatorima kritične infrastrukutre daju podatke o sektorskim kriterijumima propisanim aktom iz člana 7 stav 2 ovog zakona za te sektore.

Operatori kritične infrastrukture, na osnovu međusektorskih i sektorskih kriterijuma za određivanje kritične infrastrukture, procjenjuju koji sistemi, mreže, objekti, odnosno njihovi djelovi koje oni koriste, odnosno kojima upravljaju predstavljaju kritičnu infrastrukturu u određenom sektoru kritične infrastrukture, o čemu dostavljaju obavještenje ministarstvu nadležnom za taj sektor.

Obavještenje iz stava 2 ovog člana sadrži detaljan opis i tehničku specifikaciju sistema, mreža, objekata, odnosno njihovih djelova koji predstavljaju kritičnu infrastrukturu i druge podatke za koje se procijeni da mogu biti od značaja za određivanje kritične infrastrukture, kao i razloge zbog kojih operator kritične infrastrukture smatra da ti sistemi, mreže, objekti, odnosno njihovi djelovi predstavljaju kritičnu infrastrukturu.

Određivanje kritične infrastrukture

Član 11

Ministarstva nadležna za određene sektore utvrđuju da li sistemi, mreže, objekti, odnosno njihovi djelovi iz člana 10 stav 2 ovog zakona ispunjavaju kriterijume iz čl. 7 i 8 ovog zakona i sačinjavaju predloge za određivanje kritične infrastrukture za te sektore, koje dostavljaju organu državne uprave nadležnom za unutrašnje poslove (u daljem tekstu: Ministarstvo).

Objedinjene predloge iz stava 1 ovog člana Ministarstvo dostavlja Vladi.

Na osnovu objedinjenih predloga iz stava 2 ovog člana, Vlada određuje kritičnu infrastrukturu.

Obavještenje iz člana 10 stav 3 ovog zakona, predlozi iz st. 1 i 2 i akt iz stava 3 ovog člana označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

Promjene u kritičnoj infrastrukturi

Član 12

Operator kritične infrastrukture dužan je da, najmanje jednom godišnje, ministarstvu nadležnom za određeni sektor dostavi obavještenje o stanju, odnosno promjenama u sistemima, mrežama, objektima, odnosno njihovim djelovima koje koristi, odnosno kojima upravlja, a koji su određeni kao kritična infrastruktura.

Na osnovu obavještenja iz stava 1 ovog člana, ministarstvo nadležno za određeni sektor utvrđuje da li je potrebno izvršiti izmjene, odnosno dopune u pogledu određivanja kritične infrastrukture u tom sektoru.

Ako utvrdi da je potrebno izvršiti izmjene, odnosno dopune iz stava 2 ovog člana, ministarstvo nadležno za određeni sektor sačinjava predlog izmjena, odnosno dopuna za određivanje kritične infrastrukture koji dostavlja Ministarstvu.

Predlog iz stava 3 ovog člana Ministarstvo dostavlja Vladi, radi izmjena, odnosno dopuna akta iz člana 11 stav 3 ovog zakona.

Obavještenje iz stava 1 ovog člana i predlog iz stava 3 ovog člana označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

III. ZAŠTITA KRITIČNE INFRASTRUKTURE

Način zaštite kritične infrastrukture

Član 13

Zaštita kritične infrastrukture vrši se primjenom fizičke i tehničke zaštite, na način i pod uslovima propisanim za zaštitu objekata i prostora u kojima se vrše djelatnosti od javnog interesa, djelatnosti koje predstavljaju povećanu opasnost za život i zdravlje ljudi, kao i objekti čijim oštećenjem ili uništenjem bi mogle nastupiti teže posljedice po život i zdravlje većeg broja ljudi, u skladu sa zakonom kojim se uređuje zaštita lica i imovine koju ne obezbjeđuje država, ako ovim zakonom nije drukčije propisano.

Izuzetno od stava 1 ovog člana, način zaštite kritične informatičke infrastrukture, kao i način zaštite kritične infrastrukture koju koriste, odnosno kojom upravljaju organ državne uprave nadležan za poslove odbrane, organ uprave nadležan za policijske poslove, Vojska Crne Gore i Agencija za nacionalnu bezbjednost Crne Gore vrši se u skladu sa posebnim zakonom.

Bezbjednosni plan

Član 14

Operatori kritične infrastrukture, osim operatora koji koriste, odnosno upravljaju informacionim sistemima i drugih operatora iz člana 13 stav 2 ovog zakona, dužni su da izrade

bezbjednosni plan za zaštitu kritične infrastrukture koju koriste, odnosno kojom upravljaju (u daljem tekstu: bezbjednosni plan) i na taj plan pribave saglasnost Ministarstva, u roku od jedne godine od donošenja akta iz člana 11 stav 3 ovog zakona, kojim su sistemi, mreže, objekti, odnosno djelovi objekata koje oni koriste, odnosno kojima upravljaju određeni kao kritična infrastruktura.

Bezbjednosni plan sadrži naročito:

1) opis sistema, mreža, objekata, odnosno njihovih djelova koji predstavljaju kritičnu infrastrukturu;

2) analizu rizika; i

3) aktivnosti i mjere koje imaju za cilj da spriječe nastanak poremećaja u radu, oštećenja ili uništenja kritične infrastrukture u slučaju prijetnje, obezbijede funkcionisanje kritične infrastrukture u slučaju poremećaja u radu ili oštećenja i spriječe nastanak posljedica poremećaja u radu, odnosno oštećenje ili uništenje kritične infrastrukture, i to:

- trajne mjere bezbjednosti (tehničke, organizacione, komunikacione mjere i mjere ranog upozoravanja i jačanja svijesti) koje se kontinuirano preduzimaju; i

- mjere bezbjednosti koje se preduzimajuu zavisnosti od nivoa rizika i prijetnji za funkcionisanje kritične infrastrukture.

Bliži sadržaj bezbjednosnog plana propisuje Ministarstvo.

Bezbjednosni plan i akt iz stava 3 ovog člana označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

Plan zaštite kao bezbjednosni plan

Član 15

Ako operator kritične infrastrukture ima plan zaštite sistema, mreža, objekata, odnosno njihovih djelova koje koristi, odnosno kojima upravlja, a koji su određeni kao kritična infrastruktura, izrađen u skladu sa zakonom kojim se uređuje zaštita lica i imovine koju ne obezbjeđuje država, odnosno zakonom kojim se uređuje bezbjednosna zaštita brodova i luka ili drugim posebnim zakonom, taj plan se smatra bezbjednosnim planom ako komisija iz člana 16 ovog zakona utvrdi da ispunjava uslove u pogledu zaštite kritične infrastrukture u skladu sa ovim zakonom.

Saglasnost na bezbjednosni plan

Član 16

Radi davanja saglasnosti na bezbjednosne planove i utvrđivanja da li planovi zaštite iz člana 15 ovog zakona ispunjavaju uslove u pogledu zaštite kritične infrastrukture, Ministarstvo obrazuje komisiju.

Ako bezbjednosni plan ne ispunjava uslove u skladu sa članom 14 ovog zakona, komisija iz stava 1 ovog člana operatoru kritične infrastrukture daje uputstva, odnosno preporuke na koji način je potrebno izmijeniti, odnosno dopuniti taj plan.

Komisija iz stava 1 ovog člana dužna je da, prije davanja saglasnosti na plan zaštite iz člana 15 ovog zakona, u saradnji sa predstavnicima ministarstva nadležnog za određeni sektor, utvrdi da li taj plan ispunjava uslove u pogledu zaštite kritične infrastrukture.

Ako komisija iz stava 1 ovog člana utvrdi da plan zaštiteiz člana 15 ovog zakona ne ispunjava uslove u pogledu zaštite kritične infrastrukture postupiće na način iz stava 2 ovog člana.

Operatori kritične infrastrukture dužni su da postupe po uputstvima, odnosno preporukama iz st. 2 i 4 ovog člana, u roku od 90 dana.

Ako dođe do promjene okolnosti u funkcionisanju sistema, mreža, objekata, odnosno njihovih djelova koje koristi, odnosno kojima upravlja, a koji su određeni kao kritična infrastruktura, operator kritične infrastrukture je dužan da izvrši reviziju bezbjednosnog plana, odnosno plana zaštite iz člana 15 ovog zakona.

Izrada bezbjednosnog plana

Član 17

Bezbjednosni plan izrađuje lice zaposleno kod operatora kritične infrastrukture koje ima:

- VII1 nivo kvalifikacije obrazovanja i najmanje pet godina radnog iskustva na poslovima zaštite kritične infrastrukture ili poslovima zaštite u smislu zakona kojim se uređuje zaštita lica i imovine koju ne obezbjeđuje država; i
- uvjerenje o položenom stručnom ispitu za zaštitu kritične infrastrukture.

Ako operator kritične infrastrukture nema zaposleno lice koje ispunjava uslove iz stava 1 ovog člana, izradu bezbjednosnog plana može ugovorom povjeriti privrednom društvu, drugom pravnom licu ili preduzetniku koje obavlja djelatnost zaštite u skladu sa zakonom kojim se uređuje zaštita lica i imovine koju ne obezbjeđuje država i ima zaposleno lice koje ispunjava uslove iz stava 1 ovog člana.

Koordinator

Član 18

Operatori kritične infrastrukture, osim operatora koji koriste, odnosno upravljaju informacionim sistemima i drugih operatora iz člana 13 stav 2 ovog zakona, dužni su da iz reda zaposlenih odrede lice za zaštitu kritične infrastrukture (u daljem tekstu: koordinator), u roku od šest mjeseci od dana donošenja akta iz člana 11 stav 3 ovog zakona, kojim su sistemi, mreže, objekti, odnosno njihovi djelovi koje oni koriste, odnosno kojima upravljaju određeni kao kritična infrastruktura.

Koordinator može biti lice koje:

1) ima prebivalište, odnosno odobren boravak u Crnoj Gori;
2) ima VII1 nivo kvalifikacije obrazovanja;
3) ima opštu zdravstvenu sposobnost;
4) nije pravosnažno osuđeno za krivično djelo za koje se goni po službenoj dužnosti, odnosno za takvo krivično djelo protiv njega nije pokrenut krivični postupak;
5) je stručno osposobljeno za zaštitu kritične infrastrukture; i
6) ima položen stručni ispit za zaštitu kritične infrastrukture.

Zdravstvena sposobnost iz stava 1 tačka 3 ovog člana dokazuje se uvjerenjem koje izdaje nadležna zdravstvena ustanova, u skladu sa zakonom.

Uvjerenje iz stava 3 ovog člana sadrži ocjenu o zdravstvenoj sposobnosti lica za zaštitu kritične infrastrukture i ne smije da sadrži podatke o njegovom zdravstvenom stanju.

Operatori kritične infrastrukture dužni su da, najkasnije u roku od 15 dana od dana određivanja koordinatora, Ministarstvu dostave podatke o koordinatoru, kao i da o svakoj promjeni tih podataka obavijeste Ministarstvo, u roku od pet dana od dana nastale promjene.

Poslovi koordinatora
Član 19

Koordinator:

1) prati propise i međunarodne ugovore iz oblasti zaštite kritične infrastrukture;

2) prati primjenu bezbjednosnog plana, odnosno plana zaštite iz člana 15 ovog zakona;

3) posreduje u komunikaciji između operatora kritične infrastrukture i ministarstva nadležnog za određeni sektor u vezi sa zaštitom kritične infrastrukture;

4) priprema i sprovodi obuke zaposlenih kod operatora kritične infrastrukture u vezi zaštite kritične infrastrukture i vodi evidenciju o njihovim obukama;

5) savjetuje zaposlene kod operatora kritične infrastrukture u vezi zaštite kritične infrastrukture; i

6) vrši i druge poslove u skladu sa ovim zakonom.

Osposobljavanje i polaganje stručnog ispita za zaštitu kritične infrastrukture
Član 20

Osposobljavanje iz člana 18 stav 2 tačka 5 ovog zakona vrši organizator obrazovanja odraslih koji ima licencu izdatu u skladu sa propisima kojima se uređuje obrazovanje odraslih.

Osposobljavanje iz člana 18 stav 2 tačka 5 ovog zakona sprovodi se po programu obrazovanja, u skladu sa propisima kojima se uređuje obrazovanje odraslih.

Stručni ispit iz člana 18 stav 2 tačka 6 ovog zakona polaže se pred komisijom za polaganje stručnog ispita za zaštitu kritične infrastrukture, koju obrazuje ministar unutrašnjih poslova.

O položenom stručnom ispitu za zaštitu kritične infrastrukture Ministarstvo izdaje uvjerenje.

Članovima komisije za zaštitu kritične infrastrukture pripada naknada za rad, koju utvrđuje ministar unutrašnjih poslova rješenjem, a koja se isplaćuje iz budžeta Crne Gore.

Troškove polaganja stručnog ispita za zaštitu kritične infrastrukture snosi operator kritične infrastrukture, odnosno privredno društvo, drugo pravno lice, odnosno preduzetnik iz člana 17 stav 2 ovog zakona.

Program i način polaganja stručnog ispita za zaštitu kritične infrastrukture, sastav komisije za polaganje stručnog ispita za zaštitu kritične infrastrukture i visinu naknade za radtekomisije, obrazac uvjerenja iz stava 4 ovog člana, kao i visinu troškova polaganja stručnog ispita propisuje Ministarstvo.

Koordinaciono tijelo za zaštitu kritične infrastrukture

Član 21

U slučaju nastanka poremećaja u radu, odnosno oštećenja ili uništenja kritične infrastrukture rukovođenje i koordinaciju sprovođenja mjera i aktivnosti u skladu sa ovim zakonom, preduzima koordinacioni tim obrazovan u skladu sa zakonom kojim seuređuje zaštita i spašavanje.

U radu koordinacionog tima iz stava 1 ovog člana, po pozivu, mogu učestvovati starješine i predstavnici drugih organa državne uprave nadležnih za određene sektore kritične infrastrukture, kao i stručnjaci iz oblasti zaštite kritične infrastrukture.

Postupanje sa tajnim podacima i osjetljivim informacijama

Član 22

Operatori kritične infrastrukture, koordinatori i drugi subjekti, u vršenju svojih poslova i prilikom učestvovanja u razmjeni podataka u vezi sa kritičnom infrastrukturom, dužni su da sa tajnim podacima koji se odnose na kritičnu infrastrukturu postupaju u skladu sa zakonom kojim se uređuje tajnost podataka.

Operatori kritične infrastrukture, koordinatori i drugi subjekti iz stava 1 ovog člana dužni su da osjetljive informacije koriste isključivo u svrhu zaštite kritične infrastrukture propisane ovim zakonom.

Postupanje sa podacima o ličnosti

Član 23

Operatori kritične infrastrukture, koordinatori, i drugi subjekti, prilikom postupanja sa podacima o ličnosti u vezi sa kritičnom infrastrukturom, dužni su da postupaju u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

IV. EVROPSKA KRITIČNA INFRASTRUKTURA

Određivanje evropske kritične infrastrukture

Član 24

Evropska kritična infrastruktura može se odrediti u sektorima koje utvrđuje organ Evropske komisije nadležan za zaštitu kritične infrastrukture.

Evropsku kritičnu infrastrukturu na teritoriji Crne Gore određuje Vlada, na predlog Ministarstva, a na zahtjev i uz saglasnost zainteresovanih država članica Evropske unije.

O određivanju evropske kritične infrastrukture na teritoriji Crne Gore Ministarstvo obavještava zainteresovane države članice Evropske unije.

Ako bi poremećaj u radu, prekid funkcionisanja, oštećenje, odnosno uništenje kritične infrastrukture koja se nalazi na teritoriji druge države članice Evropske unije imalo značajne posljedice za Crnu Goru, Ministarstvo predlaže određivanje evropske kritične infrastrukture organu Evropske komisije nadležnom za zaštitu kritične infrastrukture.

Zaštita evropske kritične infrastrukture

Član 25

Evropska kritična infrastruktura na teritoriji Crne Gore štiti se u skladu sa ovim zakonom, ako propisima Evropske unije nije drukčije propisano.

Izvještavanje o evropskoj kritičnoj infrastrukturi

Član 26

Vlada, na predlog Ministarstva, usvaja godišnji izvještaj o evropskoj kritičnoj infrastrukturi po sektorima i broju zainteresovanih država na koje određena kritična infrastruktura ima uticaj.

Izvještaj iz stava 1 ovog člana Ministarstvo dostavlja organu Evropske komisije nadležnom za zaštitu kritične infrastrukture.

Vlada Crne Gore, svake dvije godine, dostavlja organu Evropske komisije nadležnom za zaštitu kritične infrastrukture pregled podataka o vrstama opasnosti, prijetnji i slabosti utvrđenih u svakom sektoru u kojem je u Crnoj Gori određena evropska kritična infrastruktura.

Izvještaj iz stava 1 ovog člana i podaci iz stava 3 ovog člana, označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

Razmjena informacija o evropskoj kritičnoj infrastrukturi

Član 27

Kontakt tačka za razmjenu informacija i koordinaciju aktivnosti u vezi sa evropskom kritičnom infrastrukturom sa drugim državama članicama i organima Evropske unije je Ministarstvo.

Postupanje sa tajnim podacima i osjetljivim informacijama

Član 28

Operatori evropske kritične infrastrukture, koordinatori i drugi subjekti, u vršenju svojih poslova i prilikom učestvovanja u razmjeni podataka u vezi sa evropskom kritičnom infrastrukturom, dužni su da sa tajnim podacima koji se odnose na evropsku kritičnu infrastrukturu postupaju u skladu sa zakonom kojim se uređuje tajnost podataka i međunarodnim ugovorima o razmjeni tajnih podataka.

Operatori evropske kritične infrastrukture, koordinatori i drugi subjekti iz stava 1 ovog člana dužni su da osjetljive informacije u vezi sa evropskom kritičnom infrastrukturom koriste isključivo u svrhu zaštite evropske kritične infrastrukture.

Odredbe iz st. 1 i 2 ovog člana odnose se i na nepisane podatke koji se razmjenjuju tokom sastanaka u vezi sa zaštitom evropske kritične infrastrukture.

Postupanje sa podacima o ličnosti
Član 29

Operatori evropske kritične infrastrukture, koordinatori, i drugi subjekti, prilikom postupanja sa podacima o ličnosti u vezi sa evropskom kritičnom infrastrukturom, dužni su da postupaju u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti i međunarodnim ugovorima o razmjeni podataka o ličnosti.

V. EVIDENCIJE

Evidencije koje vodi Ministarstvo
Član 30

Ministarstvo vodi evidencije o:

1) položenom stručnom ispitu za zaštitu kritične infrastrukture, koja sadrži sljedeće podatke:

- redni broj,
- ime, prezime, jedinstveni matični broj, pol, datum, mjesto i državu rođenja i prebivalište lica koje je položilo stručni ispit,
- datum polaganja stručnog ispita,
- uspjeh na polaganju stručnog ispita, i
- broj uvjerenja o položenom stručnom ispitui datum izdavanja;

2) saglasnostima na bezbjednosne planove, koja sadrži sljedeće podatke:

- redni broj,
- naziv, sjedište i adresu operatora kritične infrastrukture koji je izradio bezbjednosni plan,
- broj i datum davanja saglasnosti na bezbjednosni plan,
- broj bezbjednosnog plana na koji je data saglasnost;

3) koordinatorima, koja sadrži sljedeće podatke:

- redni broj,
- ime i prezime koordinatora,
- naziv, sjedište i adresu operatora kritične infrastrukture koji je odredio koordinatora,
- datum određivanja koordinatora.

Evidencije koje vodi operator kritične infrastrukture
Član 31

Operator kritične infrastrukture vodi evidenciju o:

1) kritičnoj infrastrukturi, koja sadrži sljedeće podatke:

- redni broj,
- broj i nazive sistema, mreža, objekata ili njihovih djelova koji čine kritičnu infrastrukturu,
- mjesta na kojim se kritična infrastruktura nalazi,
- podatak da operator kritične infrastrukture nije dužan da izradi bezbjednosni plan u skladu sa članom 14 ovog zakona;

2) bezbjednosnim planovima, odnosno planovima zaštite iz člana 15 ovog zakona, koja sadrži sljedeće podatke:

- redni broj,
- datum upućivanja bezbjednosnog plana Ministarstvu na saglasnost i datum dobijanja saglasnosti,
- broj bezbjednosnog plana, odnosno plana zaštite iz člana 15 ovog zakona;

3) koordinatoru, koja sadrži sljedeće podatke:

- redni broj,
- ime, prezime, jedinstveni matični broj, datum, mjesto, državu rođenja i prebivalište koordinatora, i
- datum određivanja koordinatora.

Način vođenja evidencija

Član 32

Evidencije iz čl. 30 i 31 ovog zakona vode se u pisanoj i elektronskoj formi.

Tajni podaci koji se unose u evidencije iz čl. 30 i 31 ovog zakona obrađuju se i štite u skladu sa zakonom kojim se uređuje tajnost podataka, a podaci o ličnosti koji se unose u te evidencije obrađuju se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

VI. NADZOR

Član 33

Nadzor nad sprovođenjem ovog zakona i propisa donesenih na osnovu ovog zakona vrši Ministarstvo.

Inspekcijski nadzor, u skladu sa ovim zakonom i zakonom kojim se uređuje inspekcijski nadzor, vrši inspektor za zaštitu kritične infrastrukture.

VII. KAZNENE ODREDBE

Član 34

Novčanom kaznom u iznosu od 2.000 do 15.000 eura kazniće se pravno lice,ako:

1) najmanje jednom godišnje ne dostavi ministarstvu nadležnom za određeni sektor kritične infrastrukture obavještenje o stanju, odnosno o promjenama u sistemima, mrežama, objektima, odnosno njihovim djelovima koje koristi, odnosno kojim upravlja, a koji su određeni kao kritična infrastruktura (član 12 stav 1);

2) ne izradi bezbjednosni plan i ne pribavi saglasnost Ministarstva na taj bezbjednosni plan u roku od jedne godine od donošenja akta iz člana 11 stav 3 ovog zakona (član 14 stav 1);

3) ne postupi po uputstvima, odnosno preporukama komisije iz člana 16 ovog zakona u roku od 90 dana (član 16 stav 5);

4) u slučaju da dođe do promjene okolnosti u funkcionisanju sistema, mreža, objekata, odnosno njihovih djelova koje koristi, odnosno kojima upravlja, a koji su određeni kao kritična infratsruktura, ne izvrši reviziju bezbjednosnog plana (član 16 stav 6);

5) ne odredi koordinatora iz reda zaposlenih u roku od šest mjeseci oddana donošenja akta iz člana 11 stav 3 ovog zakona, kojim su sistemi, mreže, objekti, odnosno njihovi djelovi, koje oni koriste, odnosno kojima upravljaju određeni kao kritična infrastruktura (član 18 stav 1);

6) zaposli lice koje ne ispunjava uslove za koordinatora u skladu sa ovim zakonom (član 18 stav 2);

7) Ministarstvu ne dostavi podatke o koordinatoru najkasnije u roku od 15 dana od dana određivanja koordinatora i ne obavijesti ga o svakoj promjeni tih podataka u roku od 5 dana od dana nastale promjene (član 18 stav 5);

8) ne koristi osjetljive informacije isključivo u svrhu zaštite kritične infrastrukture propisane ovim zakonom (član 22 stav 2).

Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 200 do 1000 eura.

Član 35

Novčanom kaznom od 200 do 1.000 eura kazniće se za prekršaj odgovorno lice u nadležnom državnom organu, organu državne uprave, organu lokalne samouprave, organu lokalne uprave, ako:

1) najmanje jednom godišnje ne dostavi ministarstvu nadležnom za određeni sektor kritične infrastrukture obavještenje o stanju, odnosno o promjenama u sistemima, mrežama, objektima, odnosno njihovim djelovima koje koristi, odnosno kojim upravlja, a koji su određeni kao kritična infrastruktura (član 12 stav 1);

2) ne izradi bezbjednosni plan i ne pribavi saglasnost Ministarstva na taj bezbjednosni plan u roku od jedne godine od dana donošenja akta iz člana 11 stav 3 ovog zakona (član 14 stav 1);

3) ne postupi po uputstvima, odnosno preporukama komisije iz člana 16 ovog zakona u roku od 90 dana (član 16 stav 5);

4) u slučaju da dođe do promjene okolnosti u funkcionisanju sistema, mreža, objekata, odnosno njihovih djelova koje koristi, odnosno kojima upravlja, a koji su određeni kao kritična infratsruktura, ne izvrši reviziju bezbjednosnog plana (član 16 stav 6);

5) ne odredi koordinatora iz reda zaposlenih u roku od šest mjeseci od dana donošenja akta iz člana 11 stav 5 ovog zakona, kojim su sistemi, mreže, objekti, odnosno njihovi djelovi, koje oni koriste, odnosno kojima upravljaju određeni kao kritična infrastruktura (član 18 stav 1);

6) zaposli lice koje ne ispunjava uslove za koordinatora u skladu sa ovim zakonom (član 18 stav 2);

7) Ministarstvu ne dostavi podatke o koordinatoru najkasnije u roku od 15 dana od dana određivanja koordinatora i ne obavijesti ga o svakoj promjeni tih podataka u roku od 5 dana od dana nastale promjene (član 18 stav 5);

8) ne koristi osjetljive informacije isključivo u svrhu zaštite kritične infrastrukture propisane ovim zakonom (član 22 stav 2).

VIII. PRELAZNE I ZAVRŠNE ODREDBE

Rok za donošenje podzakonskih akata
Član 36

Propisi za sprovođenje ovog zakona donijeće se u roku od jedne godine od dana stupanja na snagu ovog zakona.

Član 37

Operatori kritične infrastrukture dužni su da, u roku od šest mjeseci od donošenja akta iz člana 7 stav 2 ovog zakona, ministarstvima nadležnim za određene sektore dostave obavještenja iz člana 10 stav 2 ovog zakona.

Primjena odredaba o evropskoj kritičnoj infrastrukturi
Član 38

Odredbe poglavlja IV ovog zakona primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.

Stupanje na snagu
Član 39

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u „Službenom listu Crne Gore''.

*U ovaj zakon prenijete su odredbe Direktive Savjeta 2008/114/EZ od 8. decembra 2008. o utvrđivanju i označavanju Evropske kritične infrastrukture i procjeni potrebe poboljšanja njene zaštite.

OBRAZLOŽENJE

I. USTAVNI OSNOV ZA DONOŠENJE ZAKONA

Ustavni osnov za donošenje ovog zakona sadržan je u odredbi člana 16 stav 1 tačka 5 Ustava Crne Gore („Službeni list Crne Gore", br. 1/07) kojom je propisano da se zakonom u skladu sa Ustavom, uređuju i druga pitanja od interesa za Crnu Goru.

II. RAZLOZI ZA DONOŠENJE ZAKONA

Izrada Zakona o određivanju i zaštiti kritične infrastrukture predviđena je Programom pristupanja Crne Gore Evropskoj uniji 2019-2020. Prilikom izrade ovog zakona izvršeno je usaglašavanje sa Direktivom Savjeta 2008/114/EZ od 8. decembra 2008. o utvrđivanju i označavanju Evropske kritične infrastrukture i procjeni potrebe poboljšanja njene zaštite.

III.USAGLAŠENOST SA PRAVNOM TEKOVINOM EVROPSKE UNIJE I POVRĐENIM MEĐUNARODNIM KONVENCIJAMA

Ne postoje odredbe primarnih izvora prava Evropske unije sa kojim je potrebno izvršiti usaglašavanje. Kada su u pitanju sekundarni izvori prava Evropske unije zakonodavac je ovaj zakon usaglašavao sa odredbama Direktive Savjeta 2008/114/EZ od 8. decembra 2008. o utvrđivanju i označavanju Evropske kritične infrastrukture i procjeni potrebe poboljšanja njene zaštite.

IV. OBJAŠNJENJE OSNOVNIH PRAVNIH INSTITUTA

Crnogorski pravni sistem do sada nije poznavao propis koji uređuje oblast kritične infrastrukture, prema tome predmetni Predlog zakona je prvi kojim je ista uređena.

Predlogom zakona uređuje se identifikacija, određivanje i zaštita kritične infrastrukture Crne Gore, kao i nadležnosti, odgovornosti, i druga pitanja od zanačaja za kritičnu infrastrukturu. Takođe, kao posebno poglavlje Predloga zakona predviđena je evropska kritična infrastruktura, tj.kritična infrastruktura Evropske unije, čije odredbe će se primjenjivati po ulasku Crne Gore u Evropsku uniju, što je i definisano u prelaznim odredbama.

Kao što je već rečeno, ovaj zakon je prvi koji uređuje oblast kritične infrastrukture, te su termini koji definišu predmetnu oblast propisani čl. 2, 3 i 5 Predloga zakona.

Kritična infrastruktura specifična je prevashodno iz razloga što obuhvata više resora, te je prilikom određivanja iste, potrebno voditi računa o tome da se obuhvati svaka oblast društva na koju se ona odnosi. Navedene oblasti nazvane su sektorima kritične infrastrukture koji su definisani u članu 9 Predloga zakona.

Određivanje kritične infrastrukture propisano je u članu 10 Predloga zakona, gdje je na detaljan način uređen postupak izvještavanja i dostavljanja predloga za određivanje kritične infrastrukture između operatora, ministarstava nadležnih za određeni sektor i Ministarstva unutrašnjih poslova, koje u krajnjem objedinjene predloge za određivanje kritične infrastrukture dostavlja Vladi, koja svojim aktom koji je određen stepenom tajnosti određuje kritičnu infrastrukturu.

Nadalje, za upravljanje kritičnom infrastrukturom zaduženi su operatori kritične infrastrukture, a to mogu biti državni organi, organi državne uprave, organi lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva i druga pravna lica koji upravljaju sistemima, mrežama, objektima ili njhovim djelovima koji su određeni kao kritična infrastruktura. Svaki operator dužan je da iz reda zaposlenih najkasnije šest mjeseci po određivanju kritične infratrastrukture odredi koordinatora kritične infrastrukture, što je propisano u članu 17 Predloga zakona. Takođe, za koordinator su propisani uslovi koje mora da ispunjava, među kojima je, između ostalih, i položen stručni ispit za zaštitu kritične infrastrukture. U skladu sa navedenim, u članu 19 Predloga zakona definisano je i osposobljavanje i polaganje pomenutog stručnog ispita.

Propisano je da će se zaštita kritične infrastrukture vršiti primjenom fizičke i tehničke zaštite shodno Zakonu o zaštiti lica i imovine, gdje već postoje privredna društva, druga pravna lica i preduzetnici koji vrše poslove zaštite. Takođe, istim Zakonom je omogućeno da ministarstva, organi državne uprave, lokalne samouprave i službe koje obrazuje država mogu da obrazuju svoju unutrašnju službu zaštite.

Iz zaštite kritične infrastrukture izuzeti su Ministarstvo odbrane, Vojska CG, Agencija za nacionalnu bezbjednost, Uprava policije, kao i kritična informatička infrastruktura jer se oni štite po posebnim zakonima (Zakon o odbrani, Zakon o Vojsci, Zakon o Agenciji za nacionalnu bezbjednost, Zakon o unutrašnjim poslovima i Zakon o informacionoj bezbjednosti). Takođe, navedeni organi nijesu dužni da odrede koordinatora za zaštitu kritične infrastrukture, kao ni da izrađuju bezbjednosni plan shodno ovom Zakonu. Ovu mogućnost izuzeća omogućava i Direktiva sa kojom je Predlog zakona usaglašavan.

Prilikom upravljanja kritičnom infrastrukturom operatori vode računa o bezbjednosnom planu. Naime, Bezbjednosni plan uređen je članom 13 Predloga zakona, a koji predviđa obavezu operatora da najkasnije godinu dana po određivanju kritične infrastrukture izradi bezbjednosni plan i na isti pribavi saglasnost Ministarstva unutrašnjih poslova. S obzirom da na osnovu Zakona o zaštiti lica i imovine, Zakona o zaštiti luka i brodova i drugih posebnih zakona, već postoje planovi zaštite koji se odnose na oblasti koje uređuju pomenuti zakoni, predviđeno je u članu 15 da se taj plan može smatrati bezbjednosnim planom u smislu ovog Zakona, ako Komisija Ministarstva unutrašnjih poslova utvrdi da navedeni planovi ispunjavaju uslove u pogledu zaštite kritične infrastrukture. Postupak saglasnosti na bezbjednosni plan uređen je u članu 16 Predloga zakona, dok članom 17 je predviđeno ko može da izradi bezbjednosni plan.

Članom 21 Predloga zakona je propisano da u slučaju nastanka poremećaja u radu, odnosno oštećenja ili uništenja kritične infrastrukture rukovođenje i koordinaciju sprovođenja mjera i aktivnosti u skladu sa ovim zakonom, preduzima koordinacioni tim obrazovan u skladu sa Zakonom o zaštiti i spašavanju.

Kao što je to gore navedeno, posebno poglavlje (poglavlje IV) Predloga zakona zauzima kritična infrastruktura Evropske unije. Kritična infrastruktura Evropske unije podrazumijeva kritičnu infrastrukturu koja se nalazi na teritoriji države članice Evropske unije, čije bi poremećaj u radu, prekid funkcionisanja, oštećenje, odnosno uništenje imalo značajne posljedice na najmanje dvije države članice. Ovim poglavljem definisani su određivanje, zaštita, izvještavanje, razmjena informacija o ovoj kritičnoj infrastrukturi, kao i postupanje sa tajnim i lični podacima i osjetljivim informacijama.

Poglavljima V, VI i VII i VIII propisano je vođenje evidencija, nadzor na sprovođenjem ovog zakona, kaznene odredbe i prelazne i završne odredbe.

V. PROCJENA FINANSIJSKIH SREDSTAVA ZA SPROVOĐENJE ZAKONA

Predlog zakona predviđen je za III kvartal 2019.godine, međutim primjena ovog zakona neće biti moguća dok se ne donese podzakonski akt iz člana 7 Predloga zakona, na osnovu kojeg su operatori dužni da u roku od godinu dana od donošenja pomenutog akta, a nakon završenog postupka određivanja Ministarstvu dostave prijedloge kritične infrastrukture u svom sektoru. Prema tome za 2019.godinu nije potrebno planirati sredstva za sprovođenje ovog zakona, ali su operatori kritične infrastrukture (državni organi, organi državne uprave, organi lokalne samouprave, organi lokalne uprave, službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva i druga pravna lica koja upravljaju kritičnom infrastrukturom) dužni da planiraju sredstva za 2020. godinu, kada je i planirano donošenje navedenog akta Vlade.