



CRNA GORA  
SKUPŠTINA CRNE GORE

PRIMLJENO:	6. 11.	20 19	GOD.
KLASIFIKACIONI BROJ:	24-5/19-1		
VEZA:			
EPA:	849 XXVI		
SKRAĆENICA:			PRILOG:

Crna Gora  
VLADA CRNE GORE  
Broj: 07-5656  
Podgorica, 28. oktobra 2019. godine

PREDSJEDNIKU SKUPŠTINE CRNE GORE

PODGORICA

Vlada Crne Gore, na sjednici od 17. oktobra 2019. godine, utvrdila je **PREDLOG ZAKONA O ODREĐIVANJU I ZAŠTITI KRITIČNE INFRASTRUKTURE**, koji Vam u prilogu dostavljamo radi stavljanja u proceduru Skupštine Crne Gore.

Za predstavnike Vlade koji će učestvovati u radu Skupštine i njenih radnih tijela, prilikom razmatranja Predloga ovog zakona, određeni su **MEVLUDIN NUHODŽIĆ**, ministar unutrašnjih poslova i **SAFET KORAĆ**, generalni direktor Direktorata za strateško - razvojne poslove u Ministarstvu unutrašnjih poslova.

PREDSJEDNIK  
Duško Marković, s. r.

**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 bezbjednost, 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 i otpornost 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 konvencionalnih, odnosno hibridnih 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.

Pri određivanju procjene rizika i potrebnog nivoa zaštite kritične infrastrukture mora se uzeti u obzir i uticaj pojedinog sektora kritične infrastrukture na kritične infrastrukture drugih sektora, kako bi se obezbijedila razmjena podataka potrebnih za izradu analize rizika.

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 nacionalnu bezbjednost;
- 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 infrastrukture daju podatke o sektorskim kriterijumima propisanim aktom iz člana 7 stav 3 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 preduzimaju u 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 i jačanje otpornosti 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 zaštite iz 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.

Operatori su dužni da jednom u pet godina, odnosno 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, izvrše 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:

- VIII nivo kvalifikacije obrazovanja i najmanje pet godina radnog iskustva na poslovima zaštite kritične infrastrukture u sektoru kritične infrastrukture za koju se bezbjednosni plan izrađuje 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 VIII 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 i reviziju 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, preuzima 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.

### **Izveštavanje 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 ispitu i 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,  
- datum izvršene revizije 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.

Inspeksijski nadzor, u skladu sa ovim zakonom i zakonom kojim se uređuje inspeksijski 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) jednom u pet godina, odnosno 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 infrastruktura, 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 upravljaju, 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 infrastruktura, 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 donijeeće 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 3 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 značaja 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 njihovim djelovima koji su određeni kao kritična infrastruktura. Svaki operator dužan je da iz reda zaposlenih najkasnije šest mjeseci po određivanju kritične infrastrukture odredi koordinatora kritične infrastrukture, što je propisano u članu 18 Predloga zakona. Takođe, za koordinatora 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 20 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 14 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, preuzima koordinacioni tim obrazovan u skladu sa Zakonom o zaštiti i spašavanju.

Kao što je to gore navedeno, posebno poglavlje (poglavljje 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 infrastrukturuom) dužni da planiraju sredstva za 2020. godinu, kada je i planirano donošenje navedenog akta Vlade.



Crna Gora

**Organ državne uprave nadležan za oblast na koju se propis odnosi/donosilac akta**

**Ministarstvo unutrašnjih poslova Crne Gore**

<b>Naziv propisa</b>	<b>Predlog zakona o određivanju i zaštiti kritične infrastrukture</b>	
<b>Klasifikacija propisa po oblastima i podoblastima uređivanja</b>	<b>oblast</b>	<b>podoblast</b>
	IV. UNUTRAŠNJI POSLOVI	2. Unutrašnja bezbjednost
<b>Klasifikacija po pregovaračkim poglavljima Evropske Unije</b>	<b>poglavlje</b>	<b>potpoglavlje</b>
	24 Pravosuđe, sloboda i bezbjednost	24.30.10 Policajska saradnja [19.30.10]
<b>Ključni termini - eurovok deskriptori</b>		

## IZVJEŠTAJ O SPROVEDENOJ ANALIZI PROCJENE UTICAJA PROPISA

**PREDLAGAČ PROPISA**

Ministarstvo unutrašnjih poslova

**NAZIV PROPISA**

Predlog zakona o određivanju i zaštiti kritične infrastrukture

### 1. Definisanje problema

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

- Izrada ovog Zakona 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.

- 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 značaja za kritičnu infrastrukturu. Takođe, kao posebno poglavlje Predloga zakona predviđena je Kritična infrastruktura Evropske unije, s obzirom da će se odredbe ovog poglavlja primjenjivati po ulasku Crne Gore u Evropsku uniju, što je i definisano u prelaznim odredbama.

- Identifikacija kritične infrastrukture vrši se na osnovu kriterijuma koje određuje Vlada Crne Gore. Vlada takođe određuje i sektore kritične infrastrukture na prijedlog Ministarstva unutrašnjih poslova. Sektorski kriterijumi za identifikaciju kritične infrastrukture, uređiće se kroz podzakonski akt Vlade, koji ujedno predstavlja i polaznu tačku za zaštitu kritične infrastrukture.

### 2. Ciljevi

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

- Cilj koji se želi postići predloženim propisom jeste stvaranje normativnog okvira u oblasti kritične infrastrukture koja do sada u Crnoj Gori nije bila regulisana ni na jedan način.

### 3. Opcije

- Koje su moguće opcije za ispunjavanje ciljeva i rješavanje problema? (uvijek treba razmatrati "status quo" opciju i preporučljivo je uključiti i neregulatornu opciju, osim ako postoji obaveza donošenja predloženog propisa).
- Obrazložiti preferiranu opciju?
- Ne postoje druge opcije imajući u vidu da je predmetni Predlog zakona prvi propis kojim se uređuje ova oblast u Crnoj Gori.

### 4. Analiza uticaja

- Na koga će i kako će najvjerovatnije uticati rješenja u propisu - nabrojati pozitivne i

**negativne uticaje, direktne i indirektne.**

- **Koje troškove će primjena propisa izazvati građanima i privredi (naročito malim i srednjim preduzećima).**
- **Da li pozitivne posljedice donošenja propisa opravdavaju troškove koje će on stvoriti.**
- **Da li se propisom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija.**
- **Uključiti procjenu administrativnih opterećenja i biznis barijera.**

- Primjena propisa neće izazivati troškove građanima.
- Predlog zakona će izazvati troškove privrednim subjektima i to u zavisnosti od kritične infrastrukture koja se na osnovu gore pomenutog podzakonskog akta Vlade identifikuje, s obzirom da kritična infrastruktura obuhvata sljedeće sektore: energetika, saobraćaj, snabdijevanje vodom, zdravstvo, finansije, informaciono – komunikacione tehnologije, zaštita životne sredine i druge oblasti od javnog interesa, i da 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.
- Nema troškova koje je potrebno opravdati pozitivnim posljedicama propisa.
- Propis ne utiče na stvaranje novih privrednih subjekata na tržištu i tržišnu konkurenciju iz razloga jer je propisano da će se zaštita kritične infrastrukture vršiti 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 su izuzeti Ministarstvo odbrane, Vojska CG, Agencija za nacionalnu bezbjednost, Uprava policije 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).
- Nema administrativnih opterećenja i biznis barijera.

#### **5. Procjena fiskalnog uticaja**

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

- Za implementaciju propisa je potrebno obezbjeđenje finansijskih sredstava iz budžeta Crne Gore.
- Predlog zakona predviđen je za III kvartal 2019. godine, međutim primjena ovog zakona neće biti moguća dok se ne donese gore navedeni podzakonski akt Vlade, na osnovu kojeg su operatori dužni da u roku od godinu dana od donošenja pomenutog akta, a nakon završenog postupka identifikacije Ministarstvu dostave prijedloge kritične infrastrukture u svom sektoru. Navedeni podzakonski akt Vlade je planiran za 2020. godinu i nakon njega u roku od godinu dana će operatori biti dužni da odrede kritičnu infrastrukturu i dostave je Ministarstvu unutrašnjih poslova, koje će objedinjene predloge slati Vladi na usvajanje.

Prema tome 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) imaće finansijske obaveze nakon donošenja akta Vlade u 2020. godini, što će zahtijevati da opredijele sredstva za zaštitu kritične infrastrukture.

- Iz zaštite, shodno ovom Zakonu, izuzeti su Ministarstvo odbrane, Vojska CG, Agencija za nacionalnu bezbjednost, Uprava policije 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), pa time oni neće morati da izdvajaju dodatna finansijska sredstva za implementaciju ovog propisa. Takođe, predviđeno je da se kritična infrastruktura štiti shodno Zakonu o zaštiti lica i imovine na način kako se štiti obavezno šticeći objekat (fizičkom i tehničkom zaštitom), gdje već postoje privredna društva, druga pravna lica i preduzetnici koji vrše poslove zaštite i većina potencijalne kritične infrastrukture se već štiti po Zakonu o zaštiti lica i imovine kao obavezno šticeći objekat, pa tako operatori neće morati da izdvajaju dodatna finansijska sredstva za zaštitu kritične infrastrukture.

- Takođe, Predlogom zakona je propisano da se za zaštitu kritične infrastrukture izrađuje bezbjednosni plan, ali je i navedeno da ako postojeći plan izrađen u skladu sa Zakonom o zaštiti lica i imovine i Zakonom o zaštiti brodova i luka ili drugim posebnim zakonom ispunjava sve uslove u pogledu zaštite kritične infrastrukture, onda nije potrebno raditi bezbjednosni plan u skladu sa ovim Zakonom, već će se priznati takav plan od strane Komisije Ministarstva unutrašnjih poslova, te na ovaj način operatori kritične infrastrukture koji već izrađuju planove po navedenim zakonima neće morati da izdvajaju dodatna finansijska sredstva za izradu bezbjednosnog plana.

- Takođe, obazbjedjenje finansijskih sredstava iz budžeta Crne Gore biće potrebno i za naknade članovima komisije za polaganje stručnog ispita, koju utvrđuje ministar unutrašnjih poslova rješenjem, a koja se isplaćuje iz budžeta Crne Gore. Visina naknade biće određena podzakonskim aktom koji donosi Ministarstvo unutrašnjih poslova.

- Obezbjedjenje finansijskih sredstava je kontinuirano s obzirom na prirodu oblasti koju Predlog zakona uređuje.

- Međunarodne finansijske obaveze proizilaziće u odnosu na kritičnu infrastrukturu Evropske unije koja podrazumijeva kritičnu infrastrukturu koja se nalazi na teritoriji zemlje članice Evropske unije, čije bi ometanje ili uništenje imalo značajan uticaj na najmanje dvije zemlje članice. Međutim, kako Crna Gora još uvijek nije članica Evropske unije, to su i ova pitanja uređena u posebnom poglavlju Predloga zakona čije odredbe će se primjenjivati nakon što ulaska Crne Gore u Evropsku uniju, te će ujedno i međunarodne finansijske obaveze nastati početkom primjene ovih odredbi.

- Prihod za budžet Crne Gore ostvariće se kroz polaganje stručnog ispita za zaštitu kritične infrastrukture, imajući u vidu da operator i lice koje izrađuje bezbjednosni plan snosi troškove polaganja ovog ispita, pa će se prihod ostvariti ukoliko je operator privredno društvo ili drugo pravno lice.

#### **6. Konsultacije zainteresovanih strana**

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

- Predlog zakona je dobio pozitivno mišljenje Evropske komisije.

- Predlog zakona je bio na Javnoj raspravi od 11. aprila do 3. maja tekuće godine.

#### **7: Monitoring i evaluacija**

- **Koje su potencijalne prepreke za implementaciju propisa?**
- **Koje će mjere biti preduzete tokom primjene propisa da bi se ispunili ciljevi?**

- Koji su glavni indikatori prema kojima će se mjeriti ispunjenje ciljeva?
- Ko će biti zadužen za sprovođenje monitoringa i evaluacije primjene propisa?

- Nema prepreka za implementaciju propisa.
- Vlada Crne Gore će biti zadužena za sprovođenje Zakona.

**Datum i mjesto**

Podgorica, 04.10. . 2019. god.



**Starješina**

*[Handwritten signature]*



Crna Gora  
Ministarstvo finansija

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

Br:01-02-03-15406/1

09. oktobar 2019. godine

**MINISTARSTVO UNUTRAŠNJIH POSLOVA**  
-n/r ministra, gospodina Mevludina Nuhodžića -

Poštovani gospodine Nuhodžiću,

Na osnovu Vašeg akta broj: 011/19-18987/3 od 04.10.2019. godine, kojim se traži mišljenje na Predlog zakona o određivanju i zaštiti kritične infrastrukture, Ministarstvo finansija daje sljedeće

**MIŠLJENJE**

Uvidom u tekst Predloga zakona i Izvještaja o analizi uticaja propisa, konstatovana je obaveza privrednim subjektima i ostalim pravnim licima koja upravljaju kritičnom infrastrukturom da planiraju sredstva za zaštitu kritične infrastrukture.

Pored navedenog, dužni su da izrade bezbjednosni plan za zaštitu kritične infrastrukture koju koriste, odnosno kojom upravljaju. Takođe, troškove polaganja stručnog ispita za zaštitu kritične infrastrukture snosi operator kritične infrastrukture, privredno društvo, odnosno drugo pravno lice.

Imajući u vidu da implementacija odredaba Predloga zakona podrazumijeva **značajne troškove za poslodavce koji nijesu kvantifikovani adekvatnom procjenom**, na taj način privredni subjekti su onemogućeni da planiraju buduće troškove. Takođe, uvidom u tekst akta ustanovljeno je da će se troškovi utvrditi nakon donošenja podzakonskih akata. S toga, molimo Vas da uvođenje svakog dodatnog zahtjeva sa posebnom pažnjom razmotrite, imajući u vidu dodatna opterećenja koja će stvoriti predloženi akt.

U dostavljenom Izvještaju o sprovedenoj analizi procjene uticaja propisa, navedeno je da primjena predmetnog zakona neće biti moguća dok se ne usvoji podzakonski akt, na osnovu kojeg su operatori dužni da u roku od godinu dana od donošenja pomenutog akta, a nakon završenog postupka identifikacije, Ministarstvu unutrašnjih poslova dostave prijedloge kritične infrastrukture u svom sektoru.

Navedeni podzakonski akt Vlade je planiran za 2020. godinu, prema tome 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) imaće finansijske obaveze nakon donošenja akta Vlade u 2020. godini, što će zahtijevati da opredijele sredstva za zaštitu kritične infrastrukture.

Shodno predmetnom Zakonu, izuzeti su Ministarstvo odbrane, Vojska CG, Agencija za nacionalnu bezbjednost, Uprava policije i kritična informatička infrastruktura jer se štite po posebnim zakonima, shodno tome oni neće morati da izdvajaju dodatna finansijska sredstva za implementaciju ovog propisa.

Obzirom da ukupni troškovi za implementaciju Predloga zakona o određivanju i zaštiti kritične infrastrukture nijesu navedeni, a imajući u vidu da su kao nosioci aktivnosti prepoznati budžetski korisnici, Ministarstvo finansija predlaže da se prije svega polazi od principa finansijske održivosti koji podrazumijeva da se prilikom implementacije aktivnosti, koje proizilaze iz Predloga zakona, poštuju fiskalna ograničenja definisana godišnjim budžetskim okvirom.

Takođe, navedeno je da će biti potrebno obezbijediti finansijska sredstava iz budžeta Crne Gore i za naknade članovima komisije za polaganje stručnog ispita, koju utvrđuje ministar unutrašnjih poslova rješenjem, a koja se isplaćuje iz budžeta Crne Gore. Visina naknade biće određena podzakonskim aktom koji donosi Ministarstvo unutrašnjih poslova. Ministarstvo finansija smatra da se odredba „da visinu naknade za rad komisije propisuje Ministarstvo“ treba brisati, imajući u vidu da se Zakonom o zaradama zaposlenih u javnom sektoru uređuje način utvrđivanja i ostvarivanja prava na zaradu, naknadu zarade i druga primanja zaposlenih u javnom sektoru, način obezbjeđivanja sredstava i druga pitanja od značaja za ostvarivanje ovih prava.

S poštovanjem,

MINISTAR  
Đarko Radunović





Vlada Crne Gore  
Kabinet predsjednika  
Kancelarija za evropske integracije

Br: 01-004-2617/2

Podgorica, 7. oktobar 2019. godine

**MINISTARSTVO UNUTRAŠNJIH POSLOVA**  
ministru Mevludinu Nuhodžiću


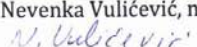
Poštovani gospodine Nuhodžiću,

Dopisom broj 011/19-34327/3 od 7. oktobra 2019. godine tražili ste mišljenje o usklađenosti **Predloga zakona o određivanju i zaštiti kritične infrastrukture** sa pravnom tekovinom Evropske unije.

Nakon upoznavanja sa sadržinom predloga propisa, a u skladu sa nadležnostima definisanim članom 40 stav 1 alineja 2 Poslovnika Vlade Crne Gore („Sl. list CG“, br. 3/12, 31/15, 48/17 i 62/18) Kancelarija za evropske integracije je saglasna sa navodima u obrascu usklađenosti predloga propisa s pravnom tekovinom Evropske unije.


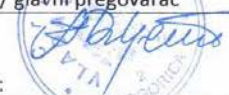
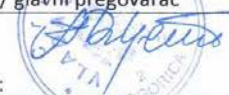
S poštovanjem,

GLAVNI PREGOVARAČ  
  
Aleksandar Drljević  


- Sačinila: Nina Lakić, samostalni savjetnik I 
- Odobrila: Nevenka Vuličević, načelnik Odsjeka za usklađivanje propisa s pravnom tekovinom EU 

**IZJAVA O USKLAĐENOSTI NACRTA/PREDLOGA PROPISA CRNE GORE S PRAVNOM  
TEKOVINOM EVROPSKE UNIJE**

<b>Identifikacioni broj Izjave</b>		<b>MUP/IU/PZ/19/03</b>
<b>1. Naziv nacrt/predloga propisa</b>		
- na crnogorskom jeziku	Predlog zakona o određivanju i zaštiti kritične infrastrukture	
na engleskom jeziku	Proposal for the Law on determining and protecting critical infrastructure	
<b>2. Podaci o obrađivaču propisa</b>		
a) Organ državne uprave koji priprema propis		
Organ državne uprave	Ministarstvo unutrašnjih poslova	
- Sektor/odsjek	Direktorat za strateško-razvojne poslove	
- odgovorno lice (ime, prezime, telefon, e-mail)	mr Safet Korać e-mail: <a href="mailto:safet.korac@mup.gov.me">safet.korac@mup.gov.me</a>	
- kontakt osoba (ime, prezime, telefon, e-mail)	Hermin Šabotić e-mail: <a href="mailto:hermin.sabotic@mup.gov.me">hermin.sabotic@mup.gov.me</a> , 067 340 273	
b) Pravno lice s javnim ovlaštenjem za pripremu i sprovođenje propisa		
- Naziv pravnog lica	/	
- odgovorno lice (ime, prezime, telefon, e-mail)	/	
- kontakt osoba (ime, prezime, telefon, e-mail)	/	
<b>3. Organi državne uprave koji primjenjuju/sprovode propis</b>		
- Organ državne uprave	Ministarstvo unutrašnjih poslova, Uprava policije, Ministarstvo saobraćaja i pomorstva, Ministarstvo ekonomije, Ministarstvo finansija, Ministarstvo zdravlja, Ministarstvo odbrane, Ministarstvo javne uprave, Ministarstvo poljoprivrede i ruralnog razvoja, Ministarstvo održivog razvoja i turizma i ostali organi državne uprave po potrebi	
<b>4. Usklađenost nacrt/predloga propisa s odredbama Sporazuma o stabilizaciji i pridruživanju između Evropske unije i njenih država članica, s jedne strane i Crne Gore, s druge strane (SSP)</b>		
a) Odredbe SSPa s kojima se usklađuje propis		
Sporazum ne sadrži odredbu koja se odnosi na normativni sadržaj predloga propisa.		
b) Stepem ispunjenosti obaveza koje proizilaze iz navedenih odredbi SSPa		
	<input type="checkbox"/>	ispunjava u potpunosti
	<input type="checkbox"/>	djelimično ispunjava
	<input type="checkbox"/>	ne ispunjava
c) Razlozi za djelimično ispunjenje, odnosno neispunjenje obaveza koje proizilaze iz navedenih odredbi SSPa		
/		
<b>5. Veza nacrt/predloga propisa s Programom pristupanja Crne Gore Evropskoj uniji (PPCG)</b>		
- PPCG za period	2019-2020	
- Poglavlje, potpoglavlje	Poglavlje 24 Pravda, sloboda i bezbjednost, 1. Planovi i potrebe 1.2. Zakonodavni okvir E.2. Borba protiv terorizma	
- Rok za donošenje propisa	III kvartal 2019	
- Napomena	Zbog procedure usaglašavanja sa Evropskom komisijom, kao i međuresorne saradnje, predlog zakona nije utvrđen u planiranom roku.	
<b>6. Usklađenost nacrt/predloga propisa s pravnom tekovinom Evropske unije</b>		
a) Usklađenost s primarnim izvorima prava Evropske unije		
Ne postoji odredba primarnih izvora prava EU s kojom bi se predlog propisa mogao uporediti radi dobijanja stepena njegove usklađenosti.		
b) Usklađenost sa sekundarnim izvorima prava Evropske unije		

<b>32008L0114</b>	
Direktive Savjeta 2008/114/EZ od 8. decembra 2008. o utvrđivanju i označavanju Evropske kritične infrastrukture i procjeni potrebe poboljšanja njene zaštite/Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, (Text with EEA relevance), OJ L 345, 23.12.2008.	
<b>Potpuno usklađeno/Fully harmonized</b>	
c) Usklađenost s ostalim izvorima prava Evropske unije	
Ne postoji izvor prava EU ove vrste s kojim bi se predlog propisa mogao uporediti radi dobijanja stepena njegove usklađenosti.	
<b>6.1. Razlozi za djelimičnu usklađenost ili neusklađenost nacrt/predloga propisa Crne Gore s pravnom tekovinom Evropske unije i rok u kojem je predviđeno postizanje potpune usklađenosti</b>	
/	
<b>7. Ukoliko ne postoje odgovarajući propisi Evropske unije s kojima je potrebno obezbijediti usklađenost konstatovati tu činjenicu</b>	
/	
<b>8. Navesti pravne akte Savjeta Evrope i ostale izvore međunarodnog prava korišćene pri izradi nacrt/predloga propisa</b>	
Ne postoje izvori međunarodnog prava s kojima je	/
potrebno uskladiti predlog propisa.	
<b>9. Navesti da li su navedeni izvori prava Evropske unije, Savjeta Evrope i ostali izvori međunarodnog prava prevedeni na crnogorski jezik (prevode dostaviti u prilogu)</b>	
Navedeni izvori prava EU preveden je na crnogorski jezik.	
<b>10. Navesti da li je nacrt/predlog propisa iz tačke 1 Izjave o usklađenosti preveden na engleski jezik (prevod dostaviti u prilogu)</b>	
Predlog zakona o određivanju i zaštiti kritične infrastrukture preveden je na engleski jezik	
<b>11. Učešće konsultanata u izradi nacrt/predloga propisa i njihovo mišljenje o usklađenosti</b>	
U izradi Predloga zakona o određivanju i zaštiti kritične infrastrukture nije bilo učešća konsultanata.	
Potpis / ovlašćeno lice obrađivača propisa	Potpis / glavni pregovarač
 Datum: 07.10.2019. g.	 Datum: 

**Prilog obrasca:**

1. Prevodi propisa Evropske unije
2. Prevod nacrt/predloga propisa na engleskom jeziku (ukoliko postoji)

**TABELA USKLAĐENOSTI**

<b>1. Identifikacioni broj (IB) nacrt/predloga propisa</b>		<b>1.1. Identifikacioni broj izjave o usklađenosti i datum utvrđivanja nacrt/predloga propisa na Vladi</b>		
MUP/TU/PZ/19/03		MUP/IU/PZ/19/03		
<b>2. Naziv izvora prava Evropske unije i CELEX oznaka</b>				
Direktiva Savjeta 2008/114/EZ od 8. decembra 2008. o utvrđivanju i označavanju Evropske kritične infrastrukture i procjeni potrebe poboljšanja njene zaštite - <b>32008L0114</b>				
<b>3. Naziv nacrt/predloga propisa Crne Gore</b>				
<b>Na crnogorskom jeziku</b>		<b>Na engleskom jeziku</b>		
Predlog zakona o određivanju i zaštiti kritične infrastrukture		Proposal for the Law on designation and protection of critical infrastructure		
<b>4. Usklađenost nacrt/predloga propisa s izvorima prava Evropske unije</b>				
a)	b)	c)	d)	e)
Odredba i tekst odredbe izvora prava Evropske unije (član, stav, tačka)	Odredba i tekst odredbe nacrt/predloga propisa Crne Gore (član, stav, tačka)	Usklađenost odredbe nacrt/predloga propisa Crne Gore s odredbom izvora prava Evropske unije	Razlog za djelimičnu usklađenost ili neusklađenost	Rok za postizanje potpune usklađenosti
<b>Direktiva Savjeta 2008/114/EZ</b>				
<b>Član 1 Predmet</b>	<b>Predmet Član 1</b>	Potpuno usklađeno		
<p>Ovom Direktivom uspostavljaju se postupak za utvrđivanje i označavanje evropske kritične infrastrukture („EKI”) i zajednički pristup procjeni potrebe poboljšanja zaštite takve infrastrukture kako bi se doprinijelo zaštiti ljudi</p>	<p>Kritična infrastruktura određuje se i štiti na način i pod uslovima propisanim ovim zakonom, međunarodnim ugovorima i standardima Evropske unije.</p>			
<b>Član 2 Definicije</b>	<b>Kritična infrastruktura Član 2</b>	Potpuno usklađeno		
<p>Za potrebe ove Direktive:</p> <p>(a) „kritična infrastruktura” znači imovina, sastav ili njihov dio koji se nalazi u državama članicama i neophodan je za održavanje osnovnih društvenih funkcija, zdravlja, sigurnosti, zaštite, ekonomske i socijalne dobrobiti ljudi, čiji</p>	<p>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 bezbjednost, zdravlje i život ljudi, imovinu, životnu sredinu, bezbjednost građana, ekonomsku</p>			

<p>bi poremećaj rada ili čije bi uništenje, kao posljedica neuspjelog održavanja tih funkcija, moglo imati znatan uticaj u državi članici;</p>	<p>stabilnost, odnosno vršenje djelatnosti od javnog interesa.</p>			
<p>(b) „evropska kritična infrastruktura” ili „EKI” znači kritična infrastruktura koja se nalazi u državama članicama, a čiji bi poremećaj u radu ili čije bi uništenje imalo znatan uticaj na najmanje dvije države članice. Značaj uticaja ocjenjuje se s obzirom na međusektorska mjerila. To uključuje uticaje koji su rezultat međusektorskih zavisnosti o drugim vrstama infrastrukture;</p>	<p style="text-align: center;"><b>Značenje izraza Član 5</b></p> <p>Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja: 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.</p>	<p style="text-align: center;">Potpuno usklađeno</p>		
<p>(c) „analiza rizika” znači razmatranje odgovarajućih scenarija opasnosti kako bi se ocijenile slabosti i mogući uticaj poremećaja u radu ili uništenja kritične infrastrukture;</p>	<p style="text-align: center;"><b>Značenje izraza Član 5</b></p> <p>Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja: 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;</p>	<p style="text-align: center;">Potpuno usklađeno</p>		
<p>(d) „osjetljive informacije o zaštiti kritične infrastrukture” znači činjenice o kritičnoj infrastrukturi koje bi se, kad bi bile otkrivene, mogle upotrijebiti za planiranje i djelovanje s ciljem prouzrokovanja poremećaja u radu ili uništenja postrojenja kritične infrastrukture;</p>	<p style="text-align: center;"><b>Značenje izraza Član 5</b></p> <p>Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja: 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;</p>	<p style="text-align: center;">Potpuno usklađeno</p>		
<p>(e) „zaštita” znači sve djelatnosti kojima je cilj obezbijediti funkcionalnost, neprekidnost i cjelovitost kritičnih infrastruktura kako bi se odvratila, ublažila ili neutralizirala prijetnja, rizik ili slabost;</p>	<p style="text-align: center;"><b>Zaštita kritične infrastrukture Član 3</b></p> <p>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</p>	<p style="text-align: center;">Potpuno usklađeno</p>		

	<p>funkcionisanje kritične infrastrukture u slučaju poremećaja u radu ili oštećenja i spriječe nastanak posljedica poremećaja u radu, odnosno oštećenja ili uništenja kritične infrastrukture.</p>			
<p>(f) „vlasnici/operatori EKI-jeva” znači oni subjekti odgovorni za ulaganja u određenu imovinu, sastav ili njihov dio koji je na osnovu ove Direktive označen kao EKI i/ili za njihov svakodnevni rad.</p>	<p style="text-align: center;"><b>Značenje izraza</b> <b>Član 5</b></p> <p>Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:</p> <p>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;</p>	<p>Potpuno usklađeno</p>		
<p style="text-align: center;"><b>Član 3</b> <b>Utvrđivanje EKI-jeva</b></p> <p>1. U skladu sa postupkom predviđenom u Prilogu III., svaka država članica utvrđuje potencijalne EKI-je koji ispunjavaju međusektorska i sektorska mjerila te odgovaraju definicijama određenima u članu 2 stavovima (a) i (b).</p> <p>Komisija može državama članicama na njihov zahtjev pomoći u utvrđivanju potencijalnih EKI-ja.</p> <p>Komisija može odgovarajućim državama članicama skrenuti pažnju na postojanje potencijalnih kritičnih infrastruktura za koje se može smatrati da ispunjavaju zahtjeve za označivanje EKI-jeva.</p> <p>Svaka država članica i Komisija nastavljaju neprekidan postupak utvrđivanja potencijalnih EKI-ja.</p> <p>2. Međusektorska mjerila iz stava 1 obuhvataju sljedeće:</p>	<p style="text-align: center;"><b>Kriterijumi za određivanje kritične infrastrukture</b> <b>Član 6</b></p> <p>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).</p> <p>Kriterijumi za određivanje kritične infrastrukture mogu biti sektorski i međusektorski.</p> <p style="text-align: center;"><b>Sektorski kriterijumi za određivanje kritične infrastrukture</b> <b>Član 7</b></p> <p>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</p>	<p>Potpuno usklađeno</p>		

- (a) broj žrtava (koji se procjenjuje s obzirom na mogući broj mrtvih i ranjenih);
- (b) ekonomske posljedice (koje se procjenjuju s obzirom na značaj ekonomskog gubitka i/ili srozavanje kakvoće proizvoda ili usluga; uključujući moguće uticaje na okolinu);
- (c) uticaj na javnost (koji se procjenjuje s obzirom na uticaj na povjerenje javnosti, tjelesne patnje i remećenje svakodnevnog života; uključujući gubitak osnovnih usluga).

Pragovi za međusektorska mjerila temelje se na ozbiljnostiremećenja rada ili uništenja određene infrastrukture. Konkretni kriterijumi koji se primjenjuju na međusektorska mjerila utvrđuju države članice za određenu kritičnu infrastrukturu, za svaki slučaj posebno. Svaka država članica izvještavaju Komisiju jednom godišnje o broju infrastruktura po sektoru za koje se raspravljalo o pragovima za međusektorska mjerila.

Međusektorska mjerila trebaju uzeti u obzir karakteristike pojedinih sektora EKI-ja.

Komisija zajedno s državama članicama razvija smjernice za primjenu međusektorskih i sektorskih mjerila i približne pragove koji će se rabiti za utvrđivanje EKI-jeva. Mjerila su klasifikovana. Korišćenje smjernica nije obavezno za države članice.

3. Za potrebe sprovođenja ove Direktive koriste se sektori energije I prevoza. Podsektori su utvrđeni u Prilogu 1. Ako se prilikom preispitivanja ove Direktive, kako je utvrđeno u članu 11., bude smatralo primjerenim, mogu se odrediti I naknadni sektori koji će se koristiti za sprovođenje ove Direktive. Sektoru IKT-a daje se prednost poboljšanja njene zaštite.

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-

	komunikacione tehnologije, zaštita životne sredine, funkcionisanje državnih organa, kao i druge oblasti od javnog interesa.			
<p style="text-align: center;"><b>Član 4</b> <b>Označavanje EKI-jeva</b></p> <p>1. Svaka država članica obavijestit će ostale države članice na koje potencijalni EKI može imati značajan štetni uticaj na njegovo postojanje i razloge za njegovo proglašavanje potencijalnim EKI.</p> <p>2. Svaka država članica na čijoj se teritoriji nalazi potencijalni EKI uključit će se u bilateralne i / ili multilateralne razgovore s drugim državama članicama na koje potencijalni EKI može imati značajan štetni uticaj. Komisija može učestvovati u ovim raspravama, ali nema pravo na pristup detaljnim informacijama koje bi omogućile nedvosmisleni identifikaciju određene infrastrukture.</p> <p>Država članica koja ima razloga da vjeruje da potencijalni EKI može imati značajan štetni uticaj na njega, ali koju država članica na čijoj se teritoriji nalazi potencijalni EKI nije identifikovala kao takva, može da obavijesti Komisiju o svojoj želji da se uključi u bilateralne i / ili multilateralne pregovore o ovoj temi. Komisija će bez odlaganja dostaviti ovaj zahtjev državi članici na čijoj se teritoriji nalazi potencijalni EKI i nastojat će da olakša sporazum između strana.</p> <p>3. Država članica na čijoj se teritoriji nalazi potencijalni EKI mora je odrediti kao EKI na osnovu sporazuma između te države članice i onih država članica na koje bi mogao značajno uticati. Potrebna je saglasnost države članice na čijoj je teritoriji infrastruktura označena kao EKI.</p> <p>4. Država članica na čijoj se teritoriji nalazi obilježeni EKI</p>	<p style="text-align: center;"><b>IV. EVROPSKA KRITIČNA INFRASTRUKTURA</b></p> <p style="text-align: center;"><b>Određivanje evropske kritične infrastrukture</b> <b>Član 24</b></p> <p>Evropska kritična infrastruktura može se odrediti u sektorima koje utvrđuje organ Evropske komisije nadležan za zaštitu kritične infrastrukture.</p> <p>Evropsku kritičnu infrastrukturu na teritoriji Crne Gore određuje Vlada, na predlog Ministarstva, a na zahtjev i uz saglasnost zainteresovanih država članica Evropske unije.</p> <p>O određivanju evropske kritične infrastrukture na teritoriji Crne Gore Ministarstvo obavještava zainteresovane države članice Evropske unije.</p> <p>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.</p> <p style="text-align: center;"><b>Izvještavanje o evropskoj kritičnoj infrastrukturi</b> <b>Član 25</b></p> <p>Vlada, na predlog Ministarstva, usvaja godišnji izvještaj o evropskoj kritičnoj infrastrukturi po sektorima i broju zainteresovanih država na koje svaka određena kritična infrastruktura ima uticaj.</p> <p>Izvještaj iz stava 1 ovog člana Ministarstvo dostavlja organu Evropske komisije nadležnom za zaštitu kritične infrastrukture.</p> <p>Vlada Crne Gore, svake dvije godine, dostavlja organu Evropske komisije nadležnom za zaštitu kritične</p>	Potpuno usklađeno		



<p>obavijestiti Komisiju jednom godišnje o broju EZI-a koji su označeni po sektorima i o broju država članica koji zavise od svake određene EKI.</p> <p>Njegov identitet poznat je samo u onim državama članicama na koje EKI može imati značajan štetni uticaj.</p> <p>5. Država članica na čijoj se teritoriji nalazi EKI obavijestiti vlasnika / operatora o infrastrukturi da je ona određena kao EKI. Informacije o označavanju EKI infrastrukture klasifikovane su na odgovarajući nivo.</p> <p>6. Postupak identifikacije i označavanja EKI u skladu sa članom 3. i ovim članom završava se do 12. januara 2011. i redovno se preispituje.</p>	<p>infrastrukture pregled podataka o vrstama opasnosti, prijetnji i slabosti utvrđenih u svakom sektoru u kojem je u Crnoj Gori određena evropska kritična infrastruktura.</p> <p>Izveštaj 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.</p> <p><b>Primjena odredaba o kritičnoj infrastrukturi Evropske unije</b> <b>Član 37</b></p> <p>Odredbe poglavlja IV primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.</p>			
<p><b>Član 5</b> <b>Planovi zaštite operatora</b></p> <p>1. Proces bezbjednosnog plana operatora („SPO“) identifikuje sredstva kritične EKI infrastrukture i bezbjednosna rješenja koja postoje ili se sprovode da bi se zaštitila. Minimalni sadržaj koji treba da se obradi postupkom EKI SPO naveden je u Prilogu II.</p> <p>2. Svaka država članica procjenjuje da li svaki određeni EKI smješten na svom području ima svoju SPO ili postoje jednake mjere za rješavanje pitanja navedenih u Aneksu II. Ako država članica otkrije da postoje takve SPO ili ekvivalentne mjere i redovno se ažuriraju, dalje nisu potrebne akcije.</p> <p>3. Ako država članica otkrije da nije pripremljena takva SPO ili ekvivalentne mjere, ona će osigurati da će svaka mjera koju ocijeni potrebnom osigurati pripremu SPO-a ili ekvivalentne mjere za rješavanje problema utvrđenih u Prilogu II. Svaka država članica osigurava da se SPO ili ekvivalentne mjere uspostave i redovno preispituju u roku od jedne godine nakon što je kritična infrastruktura imenovana EKI. Taj se period u izuzetnim okolnostima</p>	<p><b>Zaštita evropske kritične infrastrukture</b> <b>Član 25</b></p> <p>Evropska kritična infrastruktura na teritoriji Crne Gore štiti se u skladu sa ovim zakonom, ako propisima Evropske unije nije drukčije propisano.</p> <p><b>Način zaštite kritične infrastrukture</b> <b>Član 13</b></p> <p>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.</p> <p>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,</p>	<p>Potpuno usklađeno</p>		

može produžiti uz saglasnost vlasti države članice i uz notifikaciju Komisiji.

4. U slučaju već uspostavljenih aranžmana za praćenje EKI-a, na njih neće uticati ovaj član, a nadležno tijelo države članice iz ovog člana je nadzornik na osnovu tih postojećih aranžmana.

5. Poštovanje mjera, uključujući mjere Zajednice, koje zahtijevaju ili upućuju na potrebu za planom sličnim ili ekvivalentnom JSB-u i nadzor koji vrši odgovarajuće tijelo smatraće se da ispunjava sve zahtjeve država članica u skladu sa ovim članom ili usvojeni u skladu sa ovim članom. Smjernice za sprovođenje iz člana 3 (2) sadrže indikativnu listu tih mjera.

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 preduzimaju u 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 zaštite iz člana 15 ovog zakona ne ispunjava uslove u pogledu zaštite kritične infrastrukture postupaće na način

	<p>iz stava 2 ovog člana.</p> <p>Operatori kritične infrastrukture dužni su da postupe po uputstvima, odnosno preporukama iz st. 2 i 4 ovog člana, u roku od 90 dana.</p> <p>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.</p>			
<p style="text-align: center;"><b>Član 6</b></p> <p style="text-align: center;"><b>Službenici za vezu zaduženi za sigurnost</b></p> <p>1. Službenik za vezu sa bezbjednošću deluje kao kontaktna tačka za bezbjednosna pitanja između vlasnika / operatera EKI i nadležnog organa države članice.</p> <p>2. Svaka država članica procjenjuje da li ima određeno EKI smješteno na njenoj teritoriji službenika za vezu ili osobu sa jednakim ovlašćenjem. Ako država članica utvrdi da je zadužen takav službenik za vezu ili osoba sa jednakim ovlašćenjem, nisu potrebne dodatne mjere izvršenja.</p> <p>3. Ako država članica utvrdi da ne postoji takav službenik za vezu u bezbjednosti ili ekvivalentna osoba u odnosu na imenovani EKI, ona će osigurati, bilo kojom mjerom koju ocijeni primjerenom, imenovanje takvog službenika za vezu u sigurnosti ili sličnog osoblja.</p> <p>4. Svaka država članica primjenjuje odgovarajući mehanizam komunikacije između odgovarajućeg organa države članice i nadležnog službenika za vezu ili lica sa ekvivalentnim ovlašćenjem za razmjenu relevantnih informacija o utvrđenim rizicima i prijetnjama u odnosu na predmetnu EKI. Ovaj mehanizam komunikacije ne dovodi u pitanje nacionalne zahtjeve u pogledu pristupa osjetljivim i tajnim podacima.</p>	<p style="text-align: center;"><b>Koordinator</b></p> <p style="text-align: center;"><b>Član 18</b></p> <p>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 susistemi, mreže, objekti, odnosno njihovi djelovi koje oni koriste, odnosno kojima upravljaju određeni kao kritična infrastruktura.</p> <p>Koordinator može biti lice koje:</p> <ol style="list-style-type: none"> <li>1) ima prebivalište, odnosno odobren boravak u Crnoj Gori;</li> <li>2) ima VII1 nivo kvalifikacije obrazovanja;</li> <li>3) ima opštu zdravstvenu sposobnost;</li> <li>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;</li> <li>5) je stručno osposobljeno za zaštitu kritične infrastrukture; i</li> <li>6) ima položen stručni ispit za zaštitu kritične infrastrukture.</li> </ol> <p>Zdravstvena sposobnost iz stava 1 tačka 3 ovog člana dokazuje se uvjerenjem koje izdaje nadležna zdravstvena ustanova, u skladu sa zakonom.</p>	<p>Potpuno usklađeno</p>		

5. Poštovanje mjera, uključujući mjere Zajednice, koje zahtijevaju ili upućuju na potrebu postojanja odgovornog službenika za vezu ili lica sa jednakim ovlaštenjima u određenom sektoru, smatraće se da ispunjavaju sve zahtjeve država članica u skladu sa ovim članom ili usvojene u skladu sa ovim članom. Smjernice za sprovođenje iz člana 3 (2) sadrže indikativnu listu tih mjera.

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;

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

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

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

#### **Izveštavanje 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

	<p>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.</p> <p>Izveštaj 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.</p> <p><b>Primjena odredaba o kritičnoj infrastrukturi Evropske unije</b> <b>Član 37</b></p> <p>Odredbe poglavlja IV primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.</p>			
<p><b>Član 7</b> <b>Izveštavanje</b></p> <p>1. Svaka država članica procjenjuje prijetnje EKI podsektorima u roku od jedne godine nakon što kritična infrastruktura na njenoj teritoriji bude imenovana EKI u tim podsektorima.</p> <p>2. Svaka država članica svake dvije godine podnosi Komisiji sažetak opštih podataka o vrstama rizika, prijetnji i slabosti koje su pronađene u svakom od sektora u kojima je EKI određen u skladu sa članom 4. i koji se nalazi na njenoj teritoriji. Komisija može u saradnji s državama članicama razviti zajednički obrazac za ove izvještaje. Svaki izveštaj klasifikuje se na odgovarajućem nivou koji država članica porijekla smatra odgovarajućim.</p>	<p><b>Izveštavanje o evropskoj kritičnoj infrastrukturi</b> <b>Član 26</b></p> <p>Vlada, na predlog Ministarstva, usvaja godišnji izvještaj o evropskoj kritičnoj infrastrukturi po sektorima i broju zainteresovanih država na koje određena kritična infrastruktura ima uticaj.</p> <p>Izveštaj iz stava 1 ovog člana Ministarstvo dostavlja organu Evropske komisije nadležnom za zaštitu kritične infrastrukture.</p> <p>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.</p> <p>Izveštaj 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.</p> <p><b>Razmjena informacija o evropskoj kritičnoj infrastrukturi</b></p>	<p>Potpuno usklađeno</p>		

	<p style="text-align: center;"><b>Član 27</b></p> <p style="text-align: center;">Kontakt tačka za razmjenu informacija i koordinaciju aktivnosti u vezi sa evropskom kritičnom infrastrukturom sa drugim državama članicama i organima Evropske unije je Ministarstvo.</p>			
<p>3. Na osnovu izveštaja navedenih u stavu 2, Komisija i države članice procenjuju da li je u pojedinačnim sektorima za EKI potrebno razmotriti dalje mjere zaštite na nivou Zajednice. Ovaj postupak se sprovodi u vezi sa revizijom ove direktive kako je utvrđeno u članu 11.</p> <p>4. Komisija može, u saradnji s državama članicama, razviti zajedničke metodološke smjernice za sprovođenje analiza rizika u pogledu EKI-ja. Upotreba takvih smjernica nije obavezna za države članice.</p>	<p style="text-align: center;">Nema odgovarajuće odredbe</p>	<p style="text-align: center;">Neprenosivo</p>		
<p style="text-align: center;"><b>Član 8</b> <b>Podrška Komisije</b></p> <p>EKI-u Komisija, preko odgovarajućeg organa države članice, podržava vlasnike / operatore određenih EKI-ja, obezbjeđujući pristup dostupnim najboljim praksama i metodama, i podržava obuku i razmjenu informacija o novim tehnološkim dostignućima u vezi sa zaštitom kritične infrastrukture.</p>	<p style="text-align: center;">Nema odgovarajuće odredbe</p>	<p style="text-align: center;">Neprenosivo</p>		
<p style="text-align: center;"><b>Član 9</b> <b>Osjetljive informacije o zaštiti evropske kritične infrastrukture</b></p> <p>1. Svako lice koje rukuje tajnim podacima u skladu sa ovom Direktivom u ime države članice ili Komisije mora imati odgovarajući nivo bezbjednosnog odobrenja. Države članice, Komisija i nadležna nadzorna tijela osiguravaju da se osjetljive informacije o zaštiti evropske kritične infrastrukture koje se dostave državama članicama ili Komisija ne upotrebljavaju u druge svrhe osim za zaštitu kritične infrastrukture.</p> <p>2. Ovaj član se takođe primenjuje na nepisane informacije, razmijenjene na sastancima na kojima se razgovara o</p>	<p style="text-align: center;"><b>Postupanje sa tajnim podacima i osjetljivim informacijama</b> <b>Član 28</b></p> <p>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.</p> <p>Operatori evropske kritične infrastrukture, koordinatori i drugi subjekti iz stava 1 ovog člana dužni su da osjetljive informacije u vezi sa evropskom kritičnom</p>	<p style="text-align: center;">Potpuno usklađeno</p>		

<p>osjetljivim temama.</p>	<p>infrastrukturu koriste isključivo u svrhu zaštite evropske kritične infrastrukture.</p> <p>Određbe 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.</p> <p style="text-align: center;"><b>Postupanje sa podacima o ličnosti</b> <b>Član 29</b></p> <p>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.</p>			
<p style="text-align: center;"><b>Član 10</b></p> <p><b>Kontakt tačke za zaštitu evropske kritične infrastrukture</b></p> <p>1. Svaka država članica određuje kontaktnu tačku za zaštitu evropske kritične infrastrukture („kontaktna tačka za ZEKI“).</p> <p>2. Kontakt-tačka za ZEKI koordinira pitanja koja se odnose na zaštitu evropske kritične infrastrukture u državama članicama sa ostalim državama članicama i Komisijom. Određivanje kontaktnih tačaka za ZEKI ne sprječava druga tijela u državi članici da učestvuju u radu na zaštiti evropske kritične infrastrukture.</p>	<p style="text-align: center;"><b>Razmjena informacija o evropskoj kritičnoj infrastrukturi</b> <b>Član 27</b></p> <p>Kontakt tačka za razmjenu informacija i koordinaciju aktivnosti u vezi sa evropskom kritičnom infrastrukturom sa drugim državama članicama i organima Evropske unije je Ministarstvo.</p>	<p style="text-align: center;">Potpuno usklađeno</p>		
<p style="text-align: center;"><b>Član 11</b> <b>Preispitivanje</b></p> <p>Preispitivanje ove direktive počinje 12. januara 2012. godine.</p>	<p style="text-align: center;">Nema odgovarajuće odredbe</p>	<p style="text-align: center;">Neprenosivo</p>		
<p style="text-align: center;"><b>Članak 12.</b> <b>Sprovođenje</b></p> <p>Države članice preuzimaju mjere potrebne za poštovanje ove Direktive do 12. januara 2011. One o tome odmah obavještavaju Komisiju i dostavljaju tekst tih mjera i njihov odnos prema ovoj Direktivi.</p>	<p style="text-align: center;">Nema odgovarajuće odredbe</p>	<p style="text-align: center;">Neprenosivo</p>		



Kad države članice donesu ove mjere, te mjere prilikom njihove službene objave sadrže upućivanje na ovu Direktivu ili se uz njih navodi takvo upućivanje. Načine tog upućivanja utvrđuju države članice.

**Član 13**  
**Stupanje na snagu**  
Ova Direktiva stupa na snagu dvadesetog dana od dana objave u Službenom listu Evropske unije.

Nema odgovarajuće odredbe

Neprenosivo

**PRILOG I.**  
Popis sektora EKI-ja  
(tabelarni prikaz)

**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.

Potpuno usklađeno

**PRILOG II.**  
POSTUPAK EKI SPO

SPO će utvrditi imovinu kritične infrastrukturne i

**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.

**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

Potpuno usklađeno

<p>sigurnosna rješenja koja postoje ili se primjenjuju radi njihove zaštite. Postupak EKI SPO obuhvata najmanje:</p> <ol style="list-style-type: none"> <li>1. utvrđivanje važne imovine;</li> <li>2 sprovođenje analize rizika na osnovu scenarija glavnih . prijetnji, slabosti svake imovine i mogućega učinka;</li> </ol> <p>te</p> <p>3 utvrđivanje, odabir i određivanje prioriteta za protivmjere . i postupke, pri čemu treba razlikovati:</p> <ul style="list-style-type: none"> <li>–trajne sigurnosne mjere kojima se utvrđuju neizostavna sigurnosna ulaganja i sredstva za koja je važno da su angažovana cijelo vrijeme. Pod tim se misli na informacije o opštim mjerama kao što su tehničke mjere (uključujući postavljanje sredstava za otkrivanje, nadzor pristupa, zaštitu i sprečavanje); organizacijske mjere (uključujući postupke za uzbunjivanje i upravljanje krizama); mjere za nadzor i provjeru; komunikaciju; podizanje svijesti i osposobljavanje i sigurnost informacijskih sistema,</li> <li>–postupne sigurnosne mjere koje se mogu aktivirati zavisno o različitim nivoima rizika i prijetnji.</li> </ul>	<p>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.</p> <p>Bezbjednosni plan sadrži naročito:</p> <ol style="list-style-type: none"> <li>1) opis sistema, mreža, objekata, odnosno njihovih djelova koji predstavljaju kritičnu infrastrukturu;</li> <li>2) analizu rizika; i</li> <li>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: <ul style="list-style-type: none"> <li>- trajne mjere bezbjednosti (tehničke, organizacione, komunikacione mjere i mjere ranog upozoravanja i jačanja svijesti) koje se kontinuirano preduzimaju; i</li> <li>- mjere bezbjednosti koje se preduzimaju u zavisnosti od nivoa rizika i prijetnji za funkcionisanje kritične infrastrukture.</li> </ul> </li> </ol> <p>Bliži sadržaj bezbjednosnog plana propisuje Ministarstvo.</p> <p>Bezbjednosni plan i akt iz stava 3 ovog člana označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.</p>			
<p style="text-align: center;"><b>PRILOG III.</b></p> <p>Postupak prema kojem države članice utvrđuju kritične infrastrukture koje se u skladu s članom 3. mogu označiti kao EK</p> <p>Članom 3. zahtijeva se da svaka država članica utvrdi kritične infrastrukture koje se mogu označiti kao EKI. Svaka</p>	<p style="text-align: center;"><b>Obaveza operatora kritične infrastrukture</b></p> <p style="text-align: center;"><b>Član 10</b></p> <p>Ministarstva nadležna za sektore za koje su utvrđeni sektorski kriterijumi za određivanje kritične infrastrukture operatorima kritične infrastrukture daju podatke o sektorskim kriterijumima propisanim aktom iz</p>	<p style="text-align: center;">Potpuno usklađeno</p>		

država članica sprovodi taj postupak u sljedećem nizu uzastopnih koraka.

Potencijalni EKI koji ne ispunjava zahtjeve jednoga od sljedećih uzastopnih koraka smatra se „neodgovarajućim da bude EKI” i isključuje ga se iz postupka. Potencijalni EKI koji ispunjava zahtjeve podliježe sljedećim koracima u ovom postupku.

#### **Korak 1.**

Svaka država članica primjenjuje sektorska mjerila kako bi učinila prvi odabir kritičnih infrastruktura unutar sektora.

#### **Korak 2.**

Svaka država članica na potencijalni EKI utvrđen na osnovu koraka 1. primjenjuje definiciju kritične infrastrukture u skladu s članom 2. tačkom (a).

Značaj učinka određuje se bilo upotrebom nacionalnih metoda za utvrđivanje kritičnih infrastruktura bilo upućivanjem na međusektorska mjerila, na odgovarajućem nacionalnom nivou. Za infrastrukturu koja osigurava osnovnu uslugu u obzir se uzimaju raspoloživost alternativa i trajanje poremećaja u radu/oporavka.

#### **Korak 3.**

Svaka država članica na potencijalni EKI koji je prošao prva dva koraka ovog postupka primjenjuje prekogranični element definicije EKI-ja u skladu s članom 2. tačkom (b). Potencijalni EKI koji ispunjava definiciju nastavlja u iduću korak postupka. Za infrastrukturu koja osigurava osnovnu uslugu u obzir se uzimaju raspoloživost alternativa i trajanje poremećaja u radu/oporavka.

#### **Korak 4.**

Svaka država članica na preostale potencijalne EKI-je primjenjuje međusektorska mjerila. Međusektorska mjerila

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.

u obzir uzimaju: ozbiljnost učinka; i, za infrastrukturu koja osigurava osnovnu uslugu, raspoloživost alternativa; i trajanje poremećaja u radu/oporavka. Smatraće se da potencijalni EKI koji ne ispunjava međusektorska mjerila nije EKI.

Obavještenje o potencijalnom EKI-ju koji je prošao kroz ovaj postupak dostavlja se samo državama članicama na koje bi potencijalni EKI mogao imati znatan nepovoljni učinak.

### **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.