P R E D L O G

Z A K O N
O KRITIČNOJ INFRASTRUKTURI

I. OSNOVNE ODREDBE

Predmet zakona

Član 1.

Ovim zakonom uređuje se nacionalna i evropska kritična infrastruktura, identifikacija i određivanje kritične infrastrukture Republike Srbije (u daljem tekstu: kritična infrastruktura), zaštita kritične infrastrukture, nadležnost i odgovornost organa i organizacija u oblasti kritične infrastrukture (u daljem tekstu: nadležni organi i organizacije) i informacije, izveštavanje, pružanje podrške odlučivanju, zaštita podataka, upravljanje i nadzor u oblasti kritične infrastrukture.

Značenje izraza

Član 2.

Pojedini izrazi upotrebljeni u ovom zakonu imaju sledeće značenje:

1) sektori kritične infrastrukture su oblasti određene ovim zakonom, u kojima se vrši postupak identifikacije i određivanja kritične infrastrukture;

2) identifikacija kritične infrastrukture je postupak utvrđivanja sistema, mreža, objekata ili njihovih delova u određenom sektoru koji se, u skladu sa utvrđenim kriterijumima, identifikuju kao kritična infrastruktura;

3) određivanje kritične infrastrukture podrazumeva postupak utvrđivanja sistema, mreža, objekata, ili njihovih delova kao kritične infrastrukture u skladu sa ovim zakonom;

4) zaštita kritične infrastrukture predstavlja skup aktivnosti i mera koje imaju za cilj osiguranje funkcionisanja kritične infrastrukture u slučaju ometanja ili uništenja, odnosno zaštitu u slučaju pretnji i sprečavanje nastanka posledice ometanja ili uništenja;

5) operatori kritične infrastrukture su državni organi, organi autonomne pokrajine, organi jedinice lokalne samouprave, javna preduzeća, privredna društva ili druga pravna lica koja upravljaju sistemima, mrežama, objektima ili njihovim delovima koji su određeni kao kritična infrastruktura;

6) Bezbednosni plan operatora za upravljanje rizikom je plan koji izrađuje operator kritične infrastrukture, kojim se definišu bezbednosni ciljevi i mere operatora na osnovu analize rizika koju plan sadrži;

7) oficir za vezu je lice zaposleno kod operatora kritične infrastrukture, a koje je kontakt između operatora kritične infrastrukture i ministarstva nadležnog za unutrašnje poslove (u daljem tekstu: Ministarstvo);

8) evropska kritična infrastruktura podrazumeva kritičnu infrastrukturu koja se nalazi na teritoriji zemlje članice Evropske unije, čije bi ometanje ili uništenje imalo značajan uticaj na najmanje dve zemlje članice.

Načela delovanja

Član 3.

Nadležni organi i organizacije, građani i drugi subjekti dužni su da se u preduzimanju mera i aktivnosti utvrđenih ovim i drugim zakonom, programima,

planovima i drugim dokumentima u oblasti kritične infrastrukture rukovode sledećim načelima:

1) načelo integrisanog pristupa – u zaštiti kritične infrastrukture pre, za vreme i posle ometanja ili prekida u funkcionisanju kritične infrastrukture, učestvuju svi nadležni organi i organizacije, građani i drugi subjekti uzimajući u obzir različite vrste opasnosti koje proističu iz analize rizika, i uzimajući u obzir međuzavisnost sektora kritične infrastrukture i njihovu interakciju;

2) načelo odgovornosti – za funkcionisanje kritične infrastrukture direktno su odgovorni operatori kritične infrastrukture, a za unapređenje zaštite kritične infrastrukture, pored operatora, i svi nadležni organi i organizacije, građani i drugi subjekti;

3) načelo zaštite od raznih vrsta pretnji – operatori, nadležni organi i organizacije, građani i drugi subjekti u obezbeđivanju kontinuiranog rada kritične infrastrukture dužni su da uzmu u obzir različite vrste rizika;

4) načelo kontinuiranog planiranja zaštite kritične infrastrukture – zaštita kritične infrastrukture zasniva se na stalnom procesu analize rizika po funkcionisanje kritične infrastrukture i procene adekvatnosti mera zaštite;

5) načelo razmene podataka i informacija i zaštite podataka – operatori, nadležni organi i organizacije, građani i drugi subjekti dužni su da blagovremeno i kontinuirano razmenjuju potrebne podatke i informacije istovremeno štiteći podatke vezane za kritičnu infrastrukturu, u skladu sa propisima kojima se uređuje zaštita tajnih podataka.

Kritična infrastruktura

Član 4.

Kritična infrastruktura su sistemi, mreže, objekti ili njihovi delovi, čiji prekid funkcionisanja ili prekid isporuke roba odnosno usluga može imati ozbiljne posledice na nacionalnu bezbednost, zdravlje i živote ljudi, imovinu, životnu sredinu, bezbednost građana, ekonomsku stabilnost, odnosno ugroziti funkcionisanje Republike Srbije.

Ministarstvo uređuje, planira, koordinira, kontroliše aktivnosti, komunicira i daje informacije u vezi sa kritičnom infrastrukturom.

II. IDENTIFIKACIJA I ODREĐIVANJE KRITIČNE INFRASTRUKTURE

Identifikacija kritične infrastrukture

Član 5.

Identifikacija kritične infrastrukture vrši se sektorski u skladu sa utvrđenim kriterijumima.

Za sprovođenje postupka identifikacije kritične infrastrukture u određenom sektoru zadužena su ministarstva nadležna za određene oblasti.

Kriterijume za identifikaciju kritične infrastrukture i način izveštavanja, propisuje Vlada.

Sektori kritične infrastrukture

Član 6.

Sektori u kojima se vrši identifikacija i određivanje kritične infrastrukture jesu:

1) eneregetika;

2) saobraćaj;

3) snabdevanje vodom i hranom;

4) zdravstvo;

5) finansije;

6) telekomunikacione i informacione tehnologije;

7) zaštita životne sredine;

8) funkcionisanje državnih organa.

Osim sektora iz stava 1. ovog člana, kritična infrastruktura može se odrediti i u drugim sektorima, na predlog ministarstva nadležnog za određenu oblast, u skladu sa ovim zakonom.

Utvrđivanje sektora iz stava 2. ovog člana i kriterijume za identifikaciju kritične infrastrukture u tim sektorima, propisuje Vlada aktom iz člana 5. stav 3. ovog zakona.

Određivanje kritične infrastrukture

Član 7.

Kritičnu infrastrukturu na predlog Ministarstva određuje Vlada.

Ministarstva zadužena za sektore kritične infrastrukture dužna su da u roku od šest meseci od donošenja akta iz člana 5. stav 3. ovog zakona, a nakon završenog postupka identifikacije u skladu sa utvrđenim kriterijumima, Ministarstvu dostave predloge kritične infrastrukture u svom sektoru.

Ministarstva zadužena za sektore kritične infrastrukture dužna su da redovno, a najmanje jednom kvartalno izveštavaju Ministarstvo o novonastalim promenama u svom sektoru.

Ministarstva zadužena za sektore kritične infrastrukture dužna su da nakon završenog postupka identifikacije Ministarstvu svake godine, najkasnije do 31. oktobra, dostave predloge izmena i dopuna kritične infrastrukture u svom sektoru.

Ministarstvo može ukazati ministarstvima zaduženim za sektore kritične infrastrukture na potencijalne kritične infrastrukture.

Zaštita, čuvanje, korišćenje, kontrola i nadzor kritične infrastrukture u nadležnosti Ministarstva odbrane i Vojske Srbije sprovodi se u skladu sa Zakonom o odbrani i Zakonom o vojsci Srbije.

Akt o određivanju kritične infrastrukture ažurira se svake godine, najkasnije do 31. decembra.

III. ZAŠTITA KRITIČNE INFRASTRUKTURE

Bezbednosni plan operatora za upravljanje rizikom

Član 8.

Bezbednosni plan operatora za upravljanje rizikom je dokument kojim se utvrđuju mere smanjenja rizika, definišu odgovornosti i određuju dužnosti, te uspostavlja okvir za postupanje u cilju otklanjanja, odnosno smanjenja posledica bezbednosnih pretnji definisanih u analizi rizika, koja je sastavni deo plana.

Operatori kritične infrastrukture dužni su da izrade Bezbednosni plan operatora za upravljanje rizikom i na isti pribave saglasnost Ministarstva odmah, a najkasnije šest meseci po određivanju sistema, mreža, objekata ili njihovih delova za kritičnu infrastrukturu.

Metodologiju, način izrade i sadržaj Bezbednosnog plana operatora za upravljanje rizikom propisuje ministar nadležan za unutrašnje poslove (u daljem tekstu: ministar).

Oficir za vezu

Član 9.

Operatori kritične infrastrukture moraju imati oficira za vezu, odnosno lice koje služi kao kontakt između operatora i Ministarstva, koje obezbeđuje stalnu kontrolu rizika i pretnji, obaveštava o promenama u odnosu na kritičnu infrastrukturu, obaveštava Ministarstvo o evaluaciji rizika, pretnji i ranjivosti, koordinira Bezbednosnim planom operatora za upravljanje rizikom, vrši testiranja kroz vežbe i druge aktivnosti predviđene planom i obavlja sve druge poslove vezane za kritičnu infrastrukturu.

Oficira za vezu imenuje Ministarstvo na predlog operatora kritične infrastrukture iz redova zaposlenih.

Operator kritične infrastrukture Ministarstvu dostavlja predlog za imenovanje oficira za vezu najkasnije tri meseca po određivanju sistema, mreža, objekata ili njihovih delova za kritičnu infrastrukturu.

Predloženo lice mora posedovati licencu za oficira za vezu.

Ministarstvo izdaje licencu iz stava 4. ovog člana licu koje ima:

1) visoko obrazovanje (master akademske studije, specijalističke akademske ili specijalističke strukovne studije, odnosno osnovne studije u trajanju od najmanje četiri godine po propisu koji je uređivao visoko obrazovanje do 10. septembra 2005. godine);

2) položen poseban stručni ispit za oficira za vezu.

Polaganje posebnog stručnog ispita iz tačke 2. ovog člana organizuje i sprovodi Ministarstvo.

Način i program za polaganje posebnog stručnog ispita propisuje ministar.

Operatori kritične infrastrukture obezbeđuju kontinuitet vršenja funkcije oficira za vezu u slučaju njegovog odsustva obaveštavanjem Ministarstva o privremenom obavljanju ovih poslova od strane drugog lica, sa svim potrebnim podacima.

Kritična infrastruktura u planskim dokumentima

Član 10.

Prilikom izrade planskih dokumenata u oblasti prostornog i urbanističkog planiranja, dokumenata iz oblasti nacionalne bezbednosti i oblasti smanjenja rizika i upravljanja vanrednim situacijama, kritična infrastruktura mora se tretirati na poseban način, naročito u delu preventivnih aktivnosti i aktivnosti vezanih za odgovor na vanredne situacije u kojima mora imati prioritet.

Republički štab za vanredne situacije

Član 11.

U slučaju nastupanja okolnosti ugrožavanja, ometanja rada ili uništenja kritične infrastrukture rukovođenje i koordinaciju sprovođenja mera i zadataka u navedenim okolnostima preduzima Republički štab za vanredne situacije, u skladu sa zakonom.

Ministarstvo pruža stručnu podršku štabu iz stava 1. ovog člana i dostavlja sve neophodne podatke i informacije u cilju nesmetanog obavljanja aktivnosti na sprovođenju utvrđenih zadataka.

IV. EVROPSKA KRITIČNA INFRASTRUKTURA

Pojam

Član 12.

Evropska kritična infrastruktura je kritična infrastruktura od interesa za najmanje dve države članice Evropske unije.

Određivanje evropske kritične infrastrukture

Član 13.

Evropska kritična struktura može se odrediti u sektorima koje određuje Evropska komisija.

Evropsku kritičnu infrastrukturu na teritoriji Republike Srbije, na predlog Ministarstva, određuje Vlada, na zahtev i u saglasnosti sa zainteresovanim državama članicama Evropske unije i obaveštava zainteresovane države članice o određivanju evropske kritične infrastrukture na teritoriji Republike Srbije.

Ako se kritična infrastruktura od značaja za Republiku Srbiju nalazi na području druge države članice Evropske unije, Vlada predlaže nadležnom telu te države određivanje evropske kritične infrastrukture.

Zaštita evropske kritične infrastrukture

Član 14.

Evropska kritična infrastruktura na teritoriji Republike Srbije štiti se na isti način kao i kritična infrastruktura Republike Srbije, osim kada je to propisima Evropske unije drugačije uređeno.

Izveštavanje o evropskoj kritičnoj infrastrukturi

Član 15.

Vlada usvaja godišnji izveštaj o broju evropske kritične infrastrukture po sektoru i broju zainteresovanih država na koje svaka određena kritična infrastruktura ima uticaj, na predlog Ministarstva.

Izveštaj iz stava 1. ovog člana dostavlja se Evropskoj komisiji i zainteresovanim državama na koje svaka određena kritična infrastruktura ima uticaj.

Razmena informacija o evropskoj kritičnoj infrastrukturi

Član 16.

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

V. POSTUPANJE SA TAJNIM PODACIMA

Određivanje i razmena

Član 17.

Određeni podaci u vezi sa kritičnom infrastrukturom mogu se odrediti kao tajni podaci u skladu sa propisima kojima se uređuje tajnost podataka.

Tajni podaci koji se odnose na Evropsku kritičnu infrastrukturu razmenjuju se sa stranim državama i organima Evropske unije u skladu sa zakonom kojim je uređena tajnost podataka i potpisanim međunarodnim sporazumima o razmeni tajnih podataka.

VI. NADZOR

Nadležnost

Član 18.

Nadzor nad primenom ovog zakona i propisa donetih na osnovu njega vrši Ministarstvo.

Ministarstvo vrši inspekcijski nadzor preko inspektora.

Ovlašćenja inspektora

Član 19.

U vršenju inspekcijskog nadzora, inspektor ima pravo da:

1) utvrdi stanje izvršavanja obaveza predviđenih ovim zakonom, upozori na uočene nepravilnosti i odredi mere i rokove za njihovo otklanjanje;

2) vrši uvid u dokumenta koja se odnose na kritičnu infrastrukturu;

3) proverava sprovođenje izdatih naredbi i zaključaka i naloži mere za izvršenje;

4) naloži izradu, donošenje i ažuriranje dokumenata predviđenih ovim zakonom;

5) naloži obustavu mera i radnji koje nisu u skladu sa Bezbednosnim planom operatora za upravljanje rizikom;

6) naloži otklanjanje utvrđenih nedostataka u sprovođenju propisanih mera utvrđenih Bezbednosnim planom operatora za upravljanje rizikom;

7) podnese predlog za pokretanje postupaka za utvrđivanje prekršajne odgovornosti protiv pravnih i odgovornih lica;

8) naredi preduzimanje hitnih mera;

9) preduzme i druge mere za koje je ovlašćen zakonom.

Protiv rešenja inspektora može se izjaviti žalba u roku od osam dana od dana dostavljanja rešenja.

Žalba protiv rešenja inspektora donetog na osnovu stava 1. tač. 5) i 8) ovog člana ne odlaže izvršenje rešenja.

VII. KAZNENE ODREDBE

Član 20.

Novčanom kaznom u iznosu od 100.000 do 1.000.000 dinara kazniće se za prekršaj javno preduzeće, privredno društvo ili drugo pravno lice koje upravlja sistemima, mrežama, objektima ili njihovim delovima koji su određeni kao kritična infrastruktura ako:

1) ne pribavi saglasnost Ministarstva na Bezbednosni plan operatora za upravljanje rizikom (član 8. stav 2);

2) ne dostavi Ministarstvu predlog za imenovanje oficira za vezu (član 9. stav 3);

3) ne postupi po nalogu inspektora (član 19. stav 1).

Član 21.

Novčanom kaznom od 50.000 do 100.000 dinara kazniće se za prekršaj odgovorno lice u nadležnom državnom organu, organu teritorijalne autonomije ili organu jedinice lokalne samouprave, ako:

1) ne dostavi Ministarstvu predloge kritične infrastrukture u svom sektoru (član 7. stav 2);

2) ne izveštava Ministarstvo o novonastalim promenama u svom sektoru (član 7. stav 3);

3) ne dostavi Ministarstvu predloge izmena i dopuna kritične infrastrukture u svom sektoru (član 7. stav 4);

4) ne postupi po nalogu inspektora (član 19. stav 1).

VIII. PRELAZNE I ZAVRŠNE ODREDBE

Rok za donošenje podzakonskih akata

Član 22.

Podzakonski akti za sprovođenje ovog zakona doneće se u roku od šest meseci od dana stupanja na snagu ovog zakona.

Rok za usaglašavanje opšteg akta

Član 23.

Izmene akta o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu unutrašnjih poslova doneće ministar u roku od 30 dana od dana stupanja na snagu ovog zakona.

Primena odredaba o evropskoj kritičnoj infrastrukturi

Član 24.

Odredbe ovog zakona koje se odnose na evropsku kritičnu infrastrukturu počinju da se primenjuju danom pristupanja Republike Srbije Evropskoj uniji.

Stupanje na snagu

Član 25.

Ovaj zakon stupa na snagu osmog dana od objavljivanja u „Službenom glasniku Republike Srbije”.

OBRAZLOŽENJE

I. USTAVNI OSNOV ZA DONOŠENjE ZAKONA

Ustavni osnov za donošenje ovog zakona sadržan je u odredbama člana 97. stav 1. tač. 4) i 17) Ustava Republike Srbije, kojima je utvrđeno da Republika Srbija uređuje i bezbednost njenih građana i da uređuje i druge odnose od interesa za Republiku Srbiju, u skladu sa Ustavom.

II. RAZLOZI ZA DONOŠENjE ZAKONA

S obzirom da oblast kritične infrastrukture nije na jedinstven način uređena ni jednim zakonom Republike Srbije, a da je oblast kritične infrastrukture preobimna, uočena je potreba da se ova oblast objedini i jasno uredi imajući u vidu značaj materije na koju se odnosi.

Budući da se radi o širokoj nedefinisanoj temi, neophodno je kritičnu infrastrukturu urediti zakonom, kojim bi se dalo usmerenje za druge posebne zakone, i kako bi se utvrdile striktne nadležnosti i odgovornosti države.

Pojam „kritične infrastrukture” pominje se u više različitih propisa i strateških dokumenata:

Zakonom o vanrednim situacijama („Službeni glasnik RS”, br. 111/09, 92/11 i 93/12), Republika Srbija opredelila se da Ministarstvo unutrašnjih poslova bude nadležno za izradu procene ugroženosti od elementarnih nepogoda i drugih nesreća, koju dostavlja Vladi na usvajanje. Autonomne pokrajine, jedinice lokalne samouprave, ministarstva i drugi organi i organizacije izrađuju procenu ugroženosti u delu koji se odnosi na njihov delokrug i dostavljaju je Ministarstvu unutrašnjih poslova. Sam zakon se ne bavi kritičnom infrastrukturom, već time na koji način ove opasnosti posredstvom kritične infrastrukture utiču na vrednosti koje treba zaštiti. Ovaj zakon propisuje da se procenom ugroženosti identifikuju izvori mogućeg ugrožavanja, sagledavaju moguće posledice, potrebe i mogućnosti sprovođenja mera i zadataka zaštite i spasavanja od elementarnih nepogoda i drugih nesreća. Procena ugroženosti sadrži naročito: 1) karakteristike teritorije, kritična postrojenja, kritična mesta i prostore sa gledišta ugroženosti od elementarnih nepogoda i drugih nesreća, sa eventualnim prekograničnim efektima udesa; 2) povredivost teritorije od elementarnih nepogoda i drugih nesreća; 3) analizu mogućih posledica od elementarnih i drugih nesreća; 4) potrebe i mogućnosti za zaštitu ljudi, materijalnih dobara i životne sredine od posledica elementarnih i drugih nesreća. Procena predviđa sveobuhvatan pristup u zaštiti kritične infrastrukture, mada orijentisan na identifikovanje izvora opasnosti i posledica koje poremećaji i prekid u funkcionisanju kritične infrastrukture ima po ekonomiju i ekologiju.

Na osnovu Zakona o vanrednim situacijama doneta je ***Uredba o sadržaju i načinu izrade plana zaštite i spasavanja u vanrednim situacijama*** („Službeni glasnik RS”, broj 8/11). Ovim propisom, pored već navedenih elemenata procene ugroženosti, koji su utvrđeni u Zakonu o vanrednim situacijama, predviđa se da će deo procene biti i procena kritične infrastrukture sa gledišta elementarnih nepogoda i drugih većih nesreća. U Republici Srbiji se ovom uredbom prvi put uvodi pojam kritične infrastrukture, ali i dalje bez jasnog određivanja o kojim je elementima ili oblastima infrastrukture reč. Takođe, nisu određeni subjekti koji bi snosili odgovornost u zaštiti kritične infrastrukture.

Pored navedenog, pitanje kritične infrastrukture može se prepoznati i u drugim normativno-pravnim dokumentima koji su u prethodnom periodu doneti u Republici Srbiji.

Jedan takav dokument, u kojem se pominje kritična infrastruktura, je ***Strategije razvoja informacionog društva u Republici Srbiji do 2020. godine***, u

kojoj se u okviru poglavlja 6.2. pominje sledeće: „Potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija na kritične infrastrukturne sisteme, što pored informaciono-komunikacionih sistema mogu biti i drugi infrastrukturni sistemi kojima se upravlja korišćenjem informaciono-komunikacionih tehnologija, poput elektro-energetskog sistema. U vezi toga je potrebno dodatno urediti kriterijume za utvrđivanje kritične infrastrukture sa stanovišta informacione bezbednosti, kriterijume za karakterizaciju napada primenom informacionih tehnologija na takvu infrastrukturu u odnosu na klasične oblike napada, kao i uslove zaštite u ovoj oblasti".

U okviru ***Strategije nacionalne bezbednosti Republike Srbije*** se ne pominje direktno pojam „kritična infrastruktura", ali se navode njeni elementi u delovima koji se odnose na: probleme ekonomskog razvoja Republike Srbije usled višegodišnjih ekonomskih sankcija i uništenja vitalnih objekata privredne i saobraćajne infrastrukture, energetsku međuzavisnost i osetljivost infrastrukture za proizvodnju i transport energenata i visokotehnološki kriminal i ugrožavanje informacionih i telekomunikacionih sistema.

U ***Zakonu o informacionoj bezbednosti*** *(*„Službeni glasnik RS", broj 6/16*)*, pojam kritične informacione infrastrukture se ne pominje kao takav, ali zakon predviđa IKT (informaciono-komunikacioni sistem) sisteme od posebnog značaja koji obavljaju delatnosti od opšteg interesa, među kojima mnogi predstavljaju kritičnu infrastrukturu, kao što su, recimo, IKT sistemi koji se koriste u obavljanju delatnosti u oblastima energetike, saobraćaja, proizvodnje i prometa naoružanja i vojne opreme, komunalnih delatnosti, IKT sistemi u zdravstvu i finansijskim institucijama. Ovi subjekti će imati obaveze da zaštite svoje IKT sisteme na odgovarajuće načine i da prijavljuju incidente nadležnim telima, čime se želi postići podizanje nivoa pripremljenosti operatora (operator IKT sistema je pravno lice, organ javne vlasti ili organizaciona jedinica organa javne vlasti koji koristi IKT sistem u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti;) i zaštite IKT sistema u Republici Srbiji. Na predlog resornog ministarstva, Vlada Republike Srbije je u martu 2016. godine obrazovala Telo za koordinaciju poslova informacione bezbednosti (u čiji sastav ulaze predstavnici ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Uprave za zajedničke poslove republičkih organa i Nacionalnog CERT-a.)

Zakon o privatnom obezbeđenju („Službeni glasnik RS", br. 104/13 i 42/15) definiše pojam „obavezno obezbeđenih objekata" kao „objekata od strateškog značaja za RS i njene građane, kao i objekata od posebnog značaja čijim oštećenjem ili uništenjem bi mogle nastupiti teže posledice po život ili zdravlje ljudi ili koji su od interesa za odbranu zemlje." Pod obavezno obezbeđenim objektima smatra se i prostor na kome se nalaze ti objekti i čine njihov sastavni deo, kao i prateći objekti koji su u funkciji tih objekata.

Pored navedenih, postoji još čitav niz sektorskih zakona u oblastima odbrane, tajnosti podataka, voda, bezbednosti hrane, prostornom planiranju, zaštiti od požara, zaštiti životne sredine, javno-privatnom partnerstvu, koji ne pominju konkretno termin „kritična infrastruktura", ali koji tretiraju pojedine segmente kritične infrastrukture kao polaznu osnovu.

Takođe, kao jedan od važnih zadataka Republike Srbije na putu evropskih integracija jeste usvajanje normativnog okvira vezanog za kritičnu infrastrukturu koji će biti usklađen sa elementima Direktive Evropskog saveta 2008/114/ES. Direktiva Saveta Evrope 2008/114/ES iz 2008. godine definiše kritičnu infrastrukturu, zajedničke procedure za identifikaciju i označavanje evropske kritične infrastrukture, zajednički pristup u proceni potreba za poboljšavanje zaštite. Ona predstavlja osnovu za naredne korake u definisanju kriterijuma za kritičnu infrastrukturu.

Imajući u vidu najbolju evropsku praksu, izrađena je analiza stanja (gap analiza). Poslednjih godina, Republika Srbija ulaže značajne napore u stvaranje integrisanog sistema zaštite i spasavanja koji bi adekvatno odgovorio u uslovima ugrožavanja, pre svega ljudskih života, ali i kritičnih nacionalnih resursa.

U okvirima Evropske unije, zaštita kritične infrastrukture prvobitno je bila posmatrana iz ugla borbe protiv terorizma. Izazovi sa kojima se današnje društvo suočava u sferi bezbednosne politike su vrlo široki, od sve učestalijih elementarnih nepogoda do različito izazvanih katastrofa, pa je neophodno primeniti dinamički, strateški i, pre svega, multidisciplinarni pristup kada se radi o procesu planiranja zaštite kritične infrastrukture. Različiti su pristupi u utvrđivanju kritične infrastrukture u državama Evropske unije.

Zanimanje EU za kritičnu infrastrukturu zemalja članica proističe iz opasnosti da bi razaranje ili poremećaj izvesne kritične infrastrukture u jednoj zemlji članici mogli neposredno doticati druge zemlje članice. U takvim slučajevima zaštitne mere su onoliko snažne koliko je to njihova najslabija karika.

Evropska komisija identifikovala je određene oblasti kritične infrastrukture. To su: energija, informacione i komunikacione tehnologije, voda, hrana, finansije, građanske vlasti, javni i pravni poredak i sigurnost, saobraćaj, hemijska i nuklearna postrojenja, kosmos i naučno istraživanje.

III. OBJAŠNjENjE OSNOVNIH PRAVNIH INSTITUTA I POJEDINAČNIH REŠENjA

Predlog zakona o kritičnoj infrastrukturi sastoji se od osam poglavlja i 25 članova.

Osnovnim odredbama Predloga zakona (čl. 1–4) određeni su predmet zakona (član 1), značenje pojedinih izraza upotrebljenih u zakonu (član 2), načela delovanja (član 3) i pojam kritične infrastrukture (član 4). Definicije iz člana 2. odnose se na izraze koji se koriste u zakonu. Ukupno je obuhvaćeno osam izraza, počev od sektora kritične infrastrukture, pa do evropske kritične infrastrukture. Kod utvrđivanja definicija, uglavnom je korišćena prihvaćena međunarodna terminologija, uz odgovarajuća prilagođavanja pravilima i duhu srpskog jezika. Definisani su pojmovi i izrazi čije značenje nije na obavezujući način utvrđeno u nekom drugom propisu, a za potrebe pravilne primene i razumevanja rešenja sadržanih u ovom zakonu neophodna je njihova precizna definicija. Članom 3. Predloga zakona utvrđeno je ukupno pet načela. Član 4. određuje pojam „kritične infrastrukture”.

Drugo poglavlje nosi naslov Identifikacija i određivanje kritične infrastrukture i obuhvata čl. 5–7. Predloga zakona. Navedenim odredbama utvrđena je identifikacija kritične infrastrukture, određivanje kritične infrastrukture kao i obavezni sektori u kojima se kritična infrastruktura identifikuje i određuje, uz ostavljanje mogućnosti da ista bude određena i u drugim sektorima.

Treće poglavlje nosi naslov Zaštita kritične infrastrukture i obuhvata čl. 8–11. Predloga zakona. Navedenim odredbama je definisan Bezbedonosni plan operatora za upravljanje rizikom, pojam oficira za vezu i način njegovog imenovanja, kao i kritična infrastruktura u planskim dokumentima i način njenog tretiranja u istim. Takođe, propisano je da u slučaju ugrožavanja i oštećenja kritične infrastrukture, rukovođenje aktivnostima u nastalim okolnostima vrši Republički štab za vanredne situacije, u skladu sa zakonom kojim se uređuje sistem smanjenja rizika od katastrofa i upravljanje vanrednim situacijama.

Četvrto poglavlje nosi naslov Evropska kritična infrastruktura i obuhvata čl. 12–16. Predloga zakona kojima se definiše evropska kritična infrastruktura, način određivanja evropske infrastrukture, zaštita evropske kritične infrastrukture, kao i

način izveštavanja o evropskoj kritičnoj infrastrukturi i razmeni informacija o evropskoj kritičnoj infrastrukturi.

Peto poglavlje nosi naslov Postupanje sa tajnim podacima i obuhvata član 17. Predloga zakona kojim se predviđa da se određeni podaci u vezi sa kritičnom infrastrukturom mogu odrediti kao tajni podaci u skladu sa zakonom koji uređuje tajnost podataka.

Šesto poglavlje nosi naslov Nadzor i obuhvata čl. 18. i 19. Predloga zakona kojima je utvrđeno ko vrši nadzor nad primenom ovog zakona i propisa donetih na osnovu njega, kao i ovlašćenja inspektora.

Sedmo poglavlje nosi naslov Kaznene odredbe i obuhvata čl. 20. i 21. Predloga zakona kojima su propisane novčane kazne za prekršaje javnih preduzeća, privrednih društava i prekršaje drugog pravnog lica, kao i odgovornog lica u nadležnom državnom organu.

Osmo poglavlje nosi naslov Prelazne i završne odredbe i obuhvata čl. 22–25. Predloga zakona kojima se predviđaju rokovi za donošenje podzakonskih akata, rok u kom su ministarstva u obavezi da dostave predloge kritične infrastrukture u svom sektoru, odloženu primenu odredaba Zakona koje se odnose na evropsku kritičnu infrastrukturu, kao i da zakon stupa na snagu osmog dana od dana objavljivanja u „Službenom glasniku Republike Srbije”.

IV. PROCENA FINANSIJSKIH SREDSTVA ZA SPROVOĐENjE OVOG ZAKONA

Za sprovođenje ovog zakona nije potrebno obezbediti sredstva u budžetu Republike Srbije.

Nove nadležnosti Ministarstva unutrašnjih poslova, u skladu sa ovim zakonom, neće iziskivati novo zapošljavanje, kao ni dodatna sredstva u budžetskoj 2018, 2019. i 2020. godini.

V. RAZLOZI ZA DONOŠENjE ZAKONA PO HITNOM POSTUPKU

Usled sve češćih elementarnih nepogoda, tehničko-tehnoloških nesreća i akcidenata izazvanih ljudskim faktorom, potrebno je sistemsko reagovanje u zaštiti onih sistema, mreža i objekata koji su prepoznati kao kritična infrastruktura a čijim bi uništenjem ili oštećenjem moglo doći do ozbiljnih posledica po nacionalnu bezbednost, zdravlje i živote ljudi, imovinu, životnu sredinu, bezbednost građana, ekonomsku stabilnost, odnosno ugroziti funkcionisanje Republike Srbije, tj. njenih organa i organizacija. Saglasno navedenom, predlaže se donošenje zakona po hitnom postupku kako ne bi došlo do nastupanja štetnih posledica po život i zdravlje ljudi, bezbednost zemlje i rad organa i organizacija.

ANALIZA EFEKATA

1. Koji su problemi koje zakon treba da reši?

Oblast kritične infrastrukture nije regulisana ni jednim zakonom Republike Srbije i postoji potreba da se ova oblast objedini i jasno definiše.

Problem koji Zakon o kritičnoj infrastrukturi treba da reši jeste stvaranje jednog integrisanog sistema zaštite i spasavanja koji bi adekvatno odgovorio u uslovima ugrožavanja, pre svega ljudskih života, ali i kritičnih nacionalnih resursa.

S obzirom da se radi o širokoj, nedefinisanoj temi, neophodno je kritičnu infrastrukturu regulisati zakonom, kojim bi se dalo usmerenje za druge posebne zakone. Naime, Republika Srbija može biti ranjiva i postoji potreba da se ovim zakonom definišu striktne nadležnosti i odgovornosti države.

Zakonom o vanrednim situacijama („Službeni glasnik RS”, br. 111/09, 92/11 i 93/12) Republika Srbija se opredelila da Ministarstvo unutrašnjih poslova bude nadležno za izradu procene ugroženosti od elementarnih nepogoda i drugih nesreća, koju dostavlja Vladi na usvajanje. Autonomne pokrajine, jedinice lokalne samouprave, ministarstva i drugi organi i organizacije izrađuju procenu ugroženosti u delu koji se odnosi na njihov delokrug i dostavljaju je Ministarstvu unutrašnjih poslova. Sam zakon se ne bavi kritičnom infrastrukturom, već kako ove opasnosti posredstvom kritične infrastrukture utiču na vrednosti koje treba zaštiti. Ovaj zakon propisuje da se procenom ugroženosti identifikuju izvori mogućeg ugrožavanja, sagledavaju moguće posledice, potrebe i mogućnosti sprovođenja mera i zadataka zaštite i spasavanja od elementarnih nepogoda i drugih nesreća. Procena ugroženosti sadrži naročito: 1) karakteristike teritorije, kritična postrojenja, kritična mesta i prostore sa gledišta ugroženosti od elementarnih nepogoda i drugih nesreća, sa eventualnim prekograničnim efektima udesa; 2) povredivost teritorije od elementarnih nepogoda i drugih nesreća; 3) analizu mogućih posledica od elementarnih i drugih nesreća; 4) potrebe i mogućnosti za zaštitu ljudi, materijalnih dobara i životne sredine od posledica elementarnih i drugih nesreća. Procena predviđa sveobuhvatan pristup u zaštiti kritične infrastrukture, mada orijentisan na identifikovanje izvora opasnosti i posledica koje poremećaji i prekid u funkcionisanju kritične infrastrukture ima po ekonomiju i ekologiju.

Na osnovu Zakona o vanrednim situacijama doneta je Uredba o sadržaju i načinu izrade plana zaštite i spasavanja u vanrednim situacijama („Službeni glasnik RS”, broj 8/211). Ovim dokumentom, pored već navedenih elemenata procene ugroženosti, koji su definisani u Zakonu o vanrednim situacijama, predviđa se da će deo procene biti i procena kritične infrastrukture sa gledišta elementarnih nepogoda i drugih većih nesreća. U Srbiji se ovom uredbom prvi put uvodi pojam kritične infrastrukture, ali i dalje bez jasnog definisanja o kojim je elementima ili oblastima infrastrukture reč. Takođe, nisu određeni subjekti koji bi snosili odgovornost u zaštiti kritične infrastrukture

Pitanje kritične infrastrukture može se prepoznati i u drugim normativnopravnim dokumentima u Republici Srbiji.

Jedan takav dokument, u kojem se pominje kritična infrastruktura, je Strategija razvoja informacionog društva u Republici Srbiji do 2020, u kojoj se u okviru poglavlja 6.2. pominje sledeće: „Potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija na kritične infrastrukturne sisteme, što pored informaciono-komunikacionih sistema mogu biti i drugi infrastrukturni sistemi kojima se upravlja korišćenjem informaciono-komunikacionih tehnologija, poput elektro-energetskog sistema. U vezi toga je potrebno dodatno urediti kriterijume za utvrđivanje kritične infrastrukture sa stanovišta informacione bezbednosti, kriterijume za karakterizaciju napada primenom informacionih tehnologija na takvu infrastrukturu u odnosu na klasične oblike napada, kao i uslove zaštite u ovoj oblasti”.

U okviru Strategije nacionalne bezbednosti Republike Srbije se ne pominje direktno pojam „kritična infrastruktura”, ali se navode njeni elementi u delovima koji se odnose na: probleme ekonomskog razvoja Republike Srbije usled višegodišnjih ekonomskih sankcija i uništenja vitalnih objekata privredne i saobraćajne infrastrukture, energetsku međuzavisnost i osetljivost infrastrukture za proizvodnju i transport energenata i visokotehnološki kriminal i ugrožavanje informacionih i telekomunikacionih sistema.

U Zakonu o informacionoj bezbednosti („Službeni glasnik RS”, broj 6/16), pojam kritične informacione infrastrukture se ne pominje kao takav, ali zakon predviđa IKT (informaciono-komunikacioni sistem) sisteme od posebnog značaja koji obavljaju delatnosti od opšteg interesa, među kojima mnogi predstavljaju kritičnu infrastrukturu, kao što su, recimo, IKT sistemi koji se koriste u obavljanju delatnosti u oblastima energetike, saobraćaja, proizvodnje i prometa naoružanja i vojne opreme, komunalnih delatnosti, IKT sistemi u zdravstvu i finansijskim institucijama. Ovi subjekti će imati obaveze da zaštite svoje IKT sisteme na odgovarajuće načine i da prijavljuju incidente nadležnim telima, čime se želi postići podizanje nivoa pripremljenosti operatora (operator IKT sistema je pravno lice, organ javne vlasti ili organizaciona jedinica organa javne vlasti koji koristi IKT sistem u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti) i zaštite IKT sistema u Republici Srbiji. Na predlog resornog ministarstva, Vlada Republike Srbije je u martu 2016. godine obrazovala Telo za koordinaciju poslova informacione bezbednosti (u čiji sastav ulaze predstavnici ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Uprave za zajedničke poslove republičkih organa i Nacionalnog CERT-a.)

Zakon o privatnom obezbeđenju („Službeni glasnik RS”, br. 104/13 i 42/15) definiše pojam „obavezno obezbeđenih objekata” kao „objekata od strateškog značaja za Republiku Srbiju i njene građane, kao i objekata od posebnog značaja čijim oštećenjem ili uništenjem bi mogle nastupiti teže posledice po život ili zdravlje ljudi ili koji su od interesa za odbranu zemlje.” Pod obavezno obezbeđenim objektima smatra se i prostor na kome se nalaze ti objekti i čine njihov sastavni deo, kao i prateći objekti koji su u funkciji tih objekata.

Pored navedenih, postoji još čitav niz sektorskih zakona u oblastima odbrane, tajnosti podataka, voda, bezbednosti hrane, prostornom planiranju, zaštiti od požara, zaštiti životne sredine, javno-privatnom partnerstvu, koji ne pominju konkretno termin „kritična infrastruktura”, ali koji tretiraju pojedine segmente kritične infrastrukture kao polaznu osnovu.

Imajući u vidu najbolju evropsku praksu, izrađena je analiza stanja (gap analiza). Poslednjih godina, Republika Srbija ulaže značajne napore u stvaranju integrisanog sistema zaštite i spasavanja koji bi adekvatno odgovorio u uslovima ugrožavanja, pre svega ljudskih života, ali i kritičnih nacionalnih resursa.

Zanimanje EU za kritičnu infrastrukturu zemalja članica proističe iz opasnosti da bi razaranje ili poremećaj izvesne kritične infrastrukture u jednoj zemlji članici mogli neposredno doticati druge zemlje članice. U takvim slučajevima zaštitne mere su onoliko snažne koliko je to njihova najslabija karika.

Evropska komisija identifikovala je određene oblasti kritične infrastrukture. To su: energija, informacione i komunikacione tehnologije, voda, hrana, finansije, građanske vlasti, javni i pravni poredak i sigurnost, saobraćaj, hemijska i nuklearna postrojenja, kosmos i naučno istraživanje.

2. Ciljevi koji se donošenjem Zakona postižu

Cilj Zakona o kritičnoj infrastrukturi jeste identifikacija i određivanje kritične infrastrukture Republike Srbije i identifikacija i određivanje evropske kritične infrastrukture. Određivanje kritične infrastrukture podrazumeva proces određivanja

sistema, mreža i objekata kao i njihovih delova, kao kritične infrastrukture u skladu sa ovim zakonom.

Označavanje kritične infrastrukture ima za cilj da se smanji rizik od poremećaja elemenata kritične infrastrukture, koji mogu uticati na život stanovništva.

S obzirom da infrastruktura, identifikovana kao kritična, ima veliki značaj za društvo, postoji obaveza na stvaranje dovoljno dobrih sigurnosnih mera koje će služiti za umanjenje rizika od prekida rada. Cilj evropske politike u ovom području predstavlja osiguravanje prikladnog i jednakog stepena zaštite za postrojenja odabrane kritične infrastrukture, što je izvodljivo jedino na osnovu zajedničkog evropskog okvira za zaštitu kritične infrastrukture.

Novim Zakonom o kritičnoj infrastrukturi uređuje se :

- identifikacija i određivanje kritične infrastrukture Republike Srbije,
- principi i planiranje zaštite kritične infrastrukture,
- nadležnost i odgovornost organa i organizacija u oblasti kritične infrastrukture,
- informacije, izveštavanje, pružanje podrške odlučivanju, zaštita podataka, upravljanje i nadzor u oblasti kritične infrastrukture.

3. Druge mogućnosti za rešavanje problema

Izradi Zakona o kritičnoj infrastrukturi pristupilo se nakon što se došlo do zaključka da bi jedino donošenje novog zakona na sveobuhvatan i efikasan način moglo da reguliše široku oblast kritične infrastrukture.

4. Zašto je donošenje akta najbolji način rešavanja problema

Ni jednim zakonom ni podzakonskim aktom oblast kritične infrastrukture u Republici Srbiji nije u celini regulisana, zbog čega je neophodno da se ova važna oblast precizno definiše i objedini jednim zakonom, s obzirom da se radi o ozbiljnoj materiji koja je od značaja za Republiku Srbiju i sve njene građane.

Poslednjih godina, Republika Srbija ulaže značajne napore u stvaranje integrisanog sistema zaštite i spasavanja koji bi adekvatno odgovorio u uslovima ugrožavanja, pre svega ljudskih života, ali i kritičnih nacionalnih resursa.

Takođe, jedan od važnih zadataka Republike Srbije na putu evropskih integracija jeste usvajanje normativnog okvira vezanog za kritičnu infrastrukturu koji će biti usklađen sa elementima Direktive Evropskog saveta 2008/114/ES. Direktiva Evropskog saveta 2008/114/ES iz 2008. godine definiše kritičnu infrastrukturu, zajedničke procedure za identifikaciju i označavanje evropske kritične infrastrukture, zajednički pristup u proceni potreba za poboljšavanje zaštite.

5. Na koga i kako će najverovatnije uticati rešenja u zakonu?

Vlada na predlog Ministarstva unutrašnjih poslova određuje kritičnu infrastrukturu.

Ministarstva zadužena za sektore kritične infrastrukture imaju obavezu da u roku definisanim Zakonom, nakon završenog postupka identifikacije u skladu sa definisanim kriterijumima, Ministarstvu koje je zaduženo za implemetaciju i sprovođenje ovog zakona, dostave predloge kritične infrastrukture u svom sektoru.

Operatori kritične infrastrukture su dužni da izrade Bezbednosni plan operatora za upravljanje rizikom i na isti pribave saglasnost Ministarstva, pri čemu su operatori kritične infrastrukture: ministarstva, javna preduzeća, privredna društva ili druga pravna lica koja upravljaju objektima, mrežama ili sistemima, ili njihovim delovima koji su određeni kao kritična infrastruktura.

Takođe ministar nadležan za unutrašnje poslove donosi bliže propise o metodologiji, načinu izrade i sadržaju Bezbednosnog plana operatora za upravljanje rizikom

6. Kakve troškove će primena Zakona izazvati građanima i privredi, naročito malim i srednjim preduzećima

Primena Zakona neće izazvati troškove građanima i privredi, a posebno ne malim i srednjim preduzećima.

7. Da li su pozitivne posledice donošenja zakona takve da opravdavaju troškove koje će on stvoriti?

Za sprovođenje Zakona o kritičnoj infrastrukturi nije potrebno obezbediti dodatna sredstva iz budžeta Republike Srbije, a efekat predloženih rešenja opravdava donošenje Zakona.

8. Da li se Zakonom podržava stvaranje novih privrednih subjekata i tržišna konkurencija

Zakon o kritičnoj infrastrukturi nema uticaja na stvaranje novih privrednih subjekata i na tržišnu konkurenciju.

9. Da li su zainteresovane strane imale prilike da se izjasne o Zakonu

Na izradi Nacrta zakona radila je mnogočlana interresorna radna grupa koja je pored predstavnika nadležnih organa državne uprave u svoj rad uključila i druge subjekte kao što su Stalna konferencija gradova i opština, Privredna komora Srbije, Fakultet bezbednosti, Srpska asocijacija menadžera korporativne bezbednosti i dr. U tom smislu. nije bilo potrebe za održavanjem javne rasprave budući da su svi relevantni subjekti već bili uključeni u izradu Nacrtu zakona.

Tekst nacrt zakona o kritičnoj infrastrukturi dostavljen je na mišljenje, pored ostalih, i nadležnim ministarstvima i subjektima čiji su predstavnici uzeli učešće u radu gore navedene radne grupe.

10. Koje će se mere tokom primene zakona preduzeti da bi se postiglo ono što se zakonom predviđa?

Ministarstvo unutrašnjih poslova vrši nadzor nad primenom Zakona o kritičnoj infrastrukturi i propisa donetih na osnovu njega, kao i inspekcijski nadzor preko inspektora.

Ministarstvo će sprovoditi polaganje ispita i izdavati licence oficirima za vezu, u skladu sa ovim zakonom.

Vlada će doneti propise o kriterijumima za definisanje kritične infrastrukture i načinu izveštavanja, a ministar unutrašnjih poslova doneće propis o metodologiji, načinu izrade i sadržaju Bezbednosnog plan operatora za upravljanje rizikom.

Na kraju, Predlog zakona o kritičnoj infrastrukturi propisuje prekršajne sankcije za pravna lica, kao i za odgovorna lica u državnim organima, ukoliko ne poštuju odredbe ovog zakona ili postupaju suprotno njima.

IZJAVA O USKLAĐENOSTI PROPISA SA PROPISIMA EVROPSKE UNIJE

1. Ovlašćeni predlagač propisa: Vlada
Obrađivač:Ministarstvo unutrašnjih poslova

2. Naziv propisa
Predlog zakona o kritičnoj infrastrukturi
Draft Law on critical infrastructure

3. Usklađenost propisa sa odredbama Sporazuma o stabilizaciji i pridruživanju između Evropskih zajednica i njihovih država članica, sa jedne strane, i Republike Srbije sa druge strane („Službeni glasnik RS", broj 83/08) (u daljem tekstu: Sporazum),

a) Odredba Sporazuma koja se odnose na normativnu saržinu propisa
/
b) Prelazni rok za usklađivanje zakonodavstva prema odredbama Sporazuma

v) Ocena ispunjenosti obaveze koje proizlaze iz navedene odredbe Sporazuma
/
g) Razlozi za delimično ispunjavanje, odnosno neispunjavanje obaveza koje proizlaze iz navedene odredbe Sporazuma
/
d) Veza sa Nacionalnim programom za usvajanje pravnih tekovina Evropske unije
Nacionalni program za usvajanje pravnih tekovina Evropske unije – treća revizija, od februara 2018. godine - u okviru tačke 3.24.7. Borba protiv terorizma, naslov Planovi za usklađivanje sa pravnim tekovinama Evropske unije predviđeno je: „Izvršiće se dodatno usklađivanje sa Direktivom 2008/114/ES po pitanju identifikacije i obeležavanja Evropske kritične infrastrukture. S tim u vezi, predlog zakonodavnog okvira u ovoj oblasti će biti sačinjen tokom 2018. godine".

4. Usklađenost propisa sa propisima Evropske unije

a) Navođenje odredbi primarnih izvora prava EU i usklađenost sa njima
/
b) Navođenje sekundarnih izvora prava EU i ocena usklađenosti sa njima
Direktiva Evropskog saveta 2008/114/ES od 8.12.2008. godine o utvrđivanju i označavanju evropske kritične infrastrukture i proceni 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)

v) Navođenje ostalih izvora prava EU i usklađenst sa njima
/

g) Razlozi za delimičnu usklađenost, odnosno neusklađenost
/
d) Rok u kojem je predviđeno postizanje potpune usklađenosti propisa sa propisima Evropske unije
5. Ukoliko ne postoje odgovarajuće nadležnosti Evropske unije u materiji koju reguliše propis, i/ili ne postoje odgovarajući sekundarni izvori prava Evropske unije sa kojima je potrebno obezbediti usklađenost, potrebno je obrazložiti tu

činjenicu. U ovom slučaju, nije potrebno popunjavati Tabelu usklađenosti propisa. Tabelu usklađenosti nije potrebno popunjavati i ukoliko se domaćim propisom ne vrši prenos odredbi sekundarnog izvora prava Evropske unije već se isključivo vrši primena ili sprovođenje nekog zahteva koji proizilazi iz odredbe sekundarnog izvora prava (npr. Predlogom odluke o izradi strateške procene uticaja biće sprovedena obaveza iz člana 4. Direktive 2001/42/EZ, ali se ne vrši i prenos te odredbe direktive).

6. Da li suprethodno navedeni izvori prava Evropske unije prevedeni na srpski jezik?
Ne

7. Da li je propis preveden na neki službeni jezik Evropske unije?
Preveden je na engleski jezik

8. Saradnja sa Evropskom unijom i učešće konsultanata u izradi propisa i njihovo mišljenje o usklađenosti
Nije bilo učešća konsultanata u izradi ovog propisa.

1. Naziv propisa Evropske unije :	2. „CELEX" oznaka EU propisa
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) Direktiva Evropskog saveta 2008/114/ES od 8.12.2008. godine o utvrđivanju i označavanju evropske kritične infrastrukture i proceni potrebe poboljšanja njene zaštite	32008L0114
3. Ovlašćeni predlagač propisa: Vlada	4. Datum izrade tabele:
Obrađivač: MINISTARSTVO UNUTRAŠNjIH POSLOVA	19.06.2018.
5. Naziv (nacrta, predloga) propisa čije odredbe su predmet analize usklađenosti sa propisom Evropske unije: PREDLOG ZAKONA O KRITIČNOJ INFRASTRUKTURI Draft Law on critical infrastructure	6. Brojčane oznake (šifre) planiranih propisa iz baze NPAA: Propis nije unet u bazu NPAA
7. Usklađenost odredbi propisa sa odredbama propisa EU:	

a)	a1)	b)	b1)	v)	g)	d)
Odredba propisa EU	Sadržina odredbe	Odredbe propisa R. Srbije	Sadržina odredbe	Usklađenost[1]	Razlozi za delimičnu usklađenost, neusklađenost ili neprenosivost	Napomena o usklađenosti
Article 1	Subject matter	Nema odgovarajuće odredbe				
Article 2 2.1.a	Definitions For the purpose of this Directive: (a) 'critical infrastructure' means an	Član 2. 2.1.1	**Značenje izraza** Pojedini izrazi upotrebljeni u ovom zakonu imaju sledeće značenje:	PU		

[1] Potpuno usklađeno - PU, delimično usklađeno - DU, neusklađeno - NU, neprenosivo – NP

a)	a1)	b)	b1)	v)	g)	d)
	asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;		1) *kritična infrastruktura* predstavlja imovinu i usluge, sistem ili njegov deo koji je neophodan za održavanje ključnih društvenih funkcija, zdravstva, bezbednosti, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan uticaj na funkcionisanje države; 3) *sektori kritične infrastrukture* su oblasti određene od strane Vlade u kojima se vrši proces identifikacije i određivanja kritične infrastrukture; 4) *identifikacija kritične infrastrukture* je proces utvrđivanja sistema, mreža, objekata i imovine u određenom sektoru u skladu sa definisanim kriterijumima; 5) *određivanje kritične infrastrukture* podrazumeva proces određivanja sistema, mreža i objekata kao kritične infrastrukture u skladu sa ovim zakonom;			

a)	a1)	b)	b1)	v)	g)	d)
	(b) ‘European critical infrastructure’ or ‘ECI’ means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;	2.1.10	10) *evropska kritična infrastruktura* podrazumeva kritičnu infrastrukturu lociranu na teritoriji zemlje članice, čije bi ometanje ili uništenje imalo značajan uticaj na najmanje dve zemlje članice.	PU		
	(c) ‘risk analysis’ means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;	2.1.8	8) *bezbedonosno-operativni plan za upravljanje rizikom* je plan koji izrađuje operator kritične infrastrukture, a kojim se definišu obim i bezbedonosni ciljevi i mere operatora na osnovu procene rizika;	PU		
	(d) ‘sensitive critical infrastructure protection related information’ means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;	17.1	Podaci u vezi sa kritičnom infrastrukturom predstavljaju tajne podatke u skladu sa zakonom kojim se uređuje tajnost podataka i propisima donetim na osnovu ovog zakona. Tajni podaci koji se odnose na	PU		

a)	a1)	b)	b1)	v)	g)	d)
		17.2	Evropsku kritičnu infrastrukturu razmenjuju se sa stranim državama i organima Evropske unije u skladu sa zakonom kojim je uređena tajnost podataka i potpisanim međunarodnim sporazumima o razmeni tajnih podataka.			
	(e) 'protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;	2.1.6.	6) *zaštita kritične infrastrukture* predstavlja skup aktivnosti i mera koje imaju za cilj osiguranje funkcionalnosti, neprekidnog rada i isporuke usluga i robe objekata i sistema kritične infrastrukture;	PU		
	(f) 'owners/operators of ECIs' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.	2.1.7.	7) *operatori kritične infrastrukture* su ministarstva, javna preduzeća, privredna društva ili druga pravna lica koja upravljaju objektima, mrežama ili sistemima koji su određeni kao kritična infrastruktura;	PU		
3.1.	1. Pursuant to the procedure provided in Annex III, each Member State shall identify potential ECIs which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Article 2(a) and (b). 23.12.2008 Official Journal of the European Union L 345/77 EN (1) OJ L 145, 31.5.2001, p. 43. The Commission may assist Member States at their request to identify potential ECIs. The Commission may draw the attention of the relevant	6.1 6.2. 6.3.	Identifikacija kritične infrastrukture vrši se sektorski u skladu sa definisanim kriterijuma. Za sprovođenje procesa identifikacije kritične infrastrukture u određenom sektoru zadužena su ministarstva nadležna za određene sektore. Bliže propise o definisanju sektora, nadležnih ministarstava i	PU		

a)	a1)	b)	b1)	v)	g)	d)
	Member States to the existence of potential critical infrastructures which may be deemed to satisfy the requirements for designation as an ECI. Each Member State and the Commission shall continue on an		kriterijumima za identifikaciju kritične infrastrukture određuje Vlada.			
		13.3.	Ako se kritična infrastruktura od značaja za Republiku Srbiju nalazi na području druge države članice, Vlada predlaže nadležnom telu te države određivanje evropske kritične infrastrukture.			
		13.1.	Evropska kritična struktura se može odrediti u sektorima koje određuje Evropska komisija.			
		13.2	Evropsku kritičnu infrastrukturu na teritoriji Republike Srbije, na predlog Centra, određuje Vlada, na zahtev i u saglasnosti sa zainteresovanim državama članicama Evropske unije i obaveštava zainteresovane države članice o određivanju evropske kritične infrastrukture na teritoriji Republike Srbije.			
4.1	Each Member State shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI.	13.2.	Evropsku kritičnu infrastrukturu na teritoriji Republike Srbije, na predlog Centra, određuje Vlada, na zahtev i u saglasnosti sa zainteresovanim državama članicama Evropske unije i obaveštava zainteresovane države	PU		

a)	a1)	b)	b1)	v)	g)	d)
			članice o određivanju evropske kritične infrastrukture na teritoriji Republike Srbije.			
4.2.	2. Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI. The Commission may participate in these discussions but shall not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure. A Member State that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State on whose territory the potential ECI is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this issue. The Commission shall without delay communicate this wish to the Member State on whose territory the potential ECI is located and endeavour to facilitate agreement between the parties.	13.3.	Ako se kritična infrastruktura od značaja za Republiku Srbiju nalazi na području druge države članice, Vlada predlaže nadležnom telu te države određivanje evropske kritične infrastrukture.			
4.3	3. The Member State on whose territory a potential ECI is located shall designate it as an ECI following an agreement between that Member State					

a)	a1)	b)	b1)	v)	g)	d)
	and those Member States that may be significantly affected. The acceptance of the Member State on whose territory the infrastructure to be designated as an ECI is located, shall be require					
4.4. 4.5.	4. The Member State on whose territory a designated ECI is located shall inform the Commission on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated ECI. Only those Member States that may be significantly affected by an ECI shall know its identity. 5. The Member States on whose territory an ECI is located shall inform the owner/operator of the infrastructure concerning its designation as an ECI. Information concerning the designation of an infrastructure as an ECI shall be	15.1. 15.2. 17.1.	Vlada usvaja godišnji izveštaj o broju evropske kritične infrastrukture po sektoru i broju zainteresovanih država na koje svaka određena kritična infrastruktura ima uticaj, a na predlog Centra. Izveštaj iz člana 1. ovog člana dostavlja se Evropskoj komisiji i zainteresovanim državama na koje svaka određena kritična infrastruktura ima uticaj. Podaci u vezi sa kritičnom infrastrukturom predstavljaju tajne podatke u skladu sa zakonom kojim se uređuje tajnost podataka i propisima	PU		

a)	a1)	b)	b1)	v)	g)	d)
	classified at an appropriate level.	17.2.	donetim na osnovu ovog zakona. Tajni podaci koji se odnose na Evropsku kritičnu infrastrukturu razmenjuju se sa stranim državama i organima Evropske unije u skladu sa zakonom kojim je uređena tajnost podataka i potpisanim međunarodnim sporazumima o razmeni tajnih podataka.			
5.1. 5.2. 5.3.	The operator security plan ('OSP') procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II. 2. Each Member State shall assess whether each designated ECI located on its territory possesses an OSP or has in place equivalent measures addressing the issues identified in Annex II. If a Member State finds that such an OSP or equivalent exists and is updated regularly, no further implementation action shall be necessary.	9.1. 14. 19.	Bezbednosno-operativni plan za upravljanje rizikom je dokument kojim se utvrđuju mere smanjenja i rizika, definišu odgovornosti i određuju dužnosti, te uspostavlja okvir za postupanje u cilju otklanjanja, odnosno smanjenja posledica bezbednosnih pretnji definisanih u analizi rizika. Evropska kritična infrastruktura na teritoriji Republike Srbije štiti se na isti način kao i kritična infrastruktura Republike Srbije, osim kada je to propisima Evropske unije drugačije uređeno. U vršenju inspekcijskog nadzora,	PU		

a)	a1)	b)	b1)	v)	g)	d)
	3. If a Member State finds that such an OSP or equivalent has not been prepared, it shall ensure by any measures deemed appropriate, that the OSP or equivalent is prepared addressing the issues identified in Annex II. Each Member State shall ensure that the OSP or equivalent is in place and is reviewed regularly within one year following designation of the critical infrastructure as an ECI. This period may be extended in exceptional circumstances, by agreement with the Member State authority and with a notification to the Commission.		inspektor Centra ima pravo da: 1)utvrdi stanje izvršavanja obaveza predviđenih ovim zakonom, upozori na uočene nepravilnosti i odredi mere i rokove za njihovo otklanjanje; 2) vrši uvid u dokumenta koja se odnose na kritičnu infrastrukturu; 3) proverava sprovođenje izdatih naredbi i zaključaka i naloži mere za izvršenje; 4) naloži izradu, donošenje i ažuriranje dokumenata predviđenih ovim zakonom; 5)naloži obustavu mera i radnji koje nisu u skladu sa Bezbedonosno-operativnim planom; 6) naloži otklanjanje utvrđenih nedostataka u sprovođenju propisanih mera utvrđenih Bezbedonosno-operativnim planom;			
6.1. 6.2.	1. The Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority. 2. Each Member State shall assess whether each designated ECI located		Operatori kritične infrastrukture moraju imati Oficira za vezu, odnosno lice koje služi kao kontakt između operatora i Centra, koje obezbeđuje stalnu kontrolu rizika i pretnji, obaveštava o promenama u odnosu na kritičnu infrastrukturu, obaveštava	PU		

a)	a1)	b)	b1)	v)	g)	d)
6.4.	on its territory possesses a Security Liaison Officer or equivalent. If a Member State finds that such a Security Liaison Officer is in place or an equivalent exists, no further implementation action shall be necessary. 4. Each Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned. This communication mechanism shall be without prejudice to national requirements concerning access to sensitive and classified information.	16.	Centar o evaluaciji rizika, pretnji i ranjivosti, koordinira bezbedonosno-operativnim planom, vrši testiranja kroz vežbe i druge aktivnosti predviđene planom i obavlja sve druge poslove vezane za kritičnu infrastrukturu. Kontakt tačka za potrebe razmene informacija i koordinaciju aktivnosti u vezi sa evropskom kritičnom infrastrukturom sa drugim državama članicama i telima Evropske unije je Centar.			
	1. Each Member State shall conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors.	8.2.	Ministarstva zadužena za sektore kritične infrastrukture su dužna da redovno, a najmanje jednom kvartalno izveštavaju Centar o novonastalim promenama u svom sektoru. Ministarstva zadužena za sektore			

a)	a1)	b)	b1)	v)	g)	d)
	2. Each Member State shall report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated pursuant to Article 4 and is located on its territory. A common template for these reports may be developed by the Commission in cooperation with the Member States. Each report shall be classified at an appropriate level as deemed necessary by the originating Member State. 23.12.2008 Official Journal of the European Union L 345/79 EN 3. Based on the reports referred to in paragraph 2, the Commission and the	8.3.	kritične infrastrukture su dužna da nakon završenog postupka identifikacije u skladu sa definisanim kriterijumima Centru svake godine, najkasnije do 31. oktobra dostave predloge izmena i dopuna kritične infrastrukture u svom sektoru.	PU NP	Odnosi se samo na zemlje članice	

a)	a1)	b)	b1)	v)	g)	d)
	Member States shall assess on a sectoral basis whether further protection measures at Community level should be considered for ECIs. This process shall be undertaken in conjunction with the review of this Directive as laid down in Article 11. 4. Common methodological guidelines for carrying out risk analyses in respect of ECIs may be developed by the Commission in cooperation with the Member States. The use of such guidelines shall be optional for the Member States.			NP		
9.1. 9.2.	1. Any person handling classified information pursuant to this Directive on behalf of a Member State or the Commission shall have an appropriate level of security vetting. Member States, the Commission and relevant supervisory bodies shall ensure that sensitive European critical infrastructure protection-related information submitted to the Member States or to the Commission is not used for any purpose other than the protection of critical infrastructures. 2. This Article shall also apply to non-written information exchanged during meetings at which sensitive subjects are discussed.	17.1. 17.2.	Podaci u vezi sa kritičnom infrastrukturom predstavljaju tajne podatke u skladu sa zakonom kojim se uređuje tajnost podataka i propisima donetim na osnovu ovog zakona. Tajni podaci koji se odnose na Evropsku kritičnu infrastrukturu razmenjuju se sa stranim državama i organima Evropske unije u skladu sa zakonom kojim je uređena tajnost podataka i potpisanim međunarodnim sporazumima o razmeni tajnih podataka.	PU		

a)	a1)	b)	b1)	v)	g)	d)
10.1. 10.2.	1. Each Member State shall appoint a European critical infrastructure protection contact point (‘ECIP contact point’). 2. ECIP contact points shall coordinate European critical infrastructure protection issues within the Member State, with other Member States and with the Commission. The appointment of an ECIP contact point does not preclude other authorities in a Member State from being involved in European critical infrastructure protection issues.	17.	Kontakt tačka za potrebe razmene informacija i koordinaciju aktivnosti u vezi sa evropskom kritičnom infrastrukturom sa drugim državama članicama i telima Evropske unije je Centar.	PU		
11.	Review	Nema odgovarajuće odredbe		NP		
12.	Implementation	Nema odgovarajuće odredbe		NP		
13.	Entry into force	Nema odgovarajuće		NP		

a)	a1)	b)	b1)	v)	g)	d)
		odredbe				
14.	Addressees	Nema odgovarajuće odredbe		NP		