

ЗАКОН О КРИТИЧНОЈ ИНФРАСТРУКТУРИ

I. ОСНОВНЕ ОДРЕДБЕ

Предмет закона

Члан 1.

Овим законом уређује се идентификација и одређивање критичне инфраструктуре Републике Србије (у даљем тексту: критична инфраструктура), принципи и планирање заштите критичне инфраструктуре, надлежност и одговорност органа и организација у области критичне инфраструктуре (у даљем тексту: надлежни органи и организације) и информације, извештавање, пружање подршке одлучивању, заштита података, управљање и надзор у области критичне инфраструктуре.

Значење израза

Члан 2.

Поједини изрази употребљени у овом закону имају следеће значење:

1) *критична инфраструктура* представља имовину и услуге, систем или његов део који је неопходан за одржавање кључних друштвених функција, здравства, безбедности, економског или социјалног благостања, а чије би ометање или уништење имало значајан утицај на функционисање државе;

2) *центар за координацију и заштиту критичне инфраструктуре* је организациона јединица Министарства унутрашњих послова која је задужена за имплементацију и спровођење овог закона;

3) *сектори критичне инфраструктуре* су области одређене од стране Владе у којима се врши процес идентификације и одређивања критичне инфраструктуре;

4) *идентификација критичне инфраструктуре* је процес утврђивања система, мрежа, објеката и имовине у одређеном сектору у складу са дефинисаним критеријумима;

5) *одређивање критичне инфраструктуре* подразумева процес одређивања система, мрежа и објеката као критичне инфраструктуре у складу са овим законом;

6) *заштита критичне инфраструктуре* представља скуп активности и мера које имају за циљ осигурање функционалности, непрекидног рада и испоруке услуга и робе објеката и система критичне инфраструктуре;

7) *оператори критичне инфраструктуре* су министарства, јавна предузећа, привредна друштва или друга правна лица која управљају објектима, мрежама или системима који су одређени као критична инфраструктура;

8) *безбедоносно-оперативни план за управљање ризиком* је план који израђује оператор критичне инфраструктуре, а којим се дефинишу обим и безбедоносни циљеви и мере оператора на основу процене ризика;

9) *официр за везу* је лице запослено код оператора критичне инфраструктуре, а које је контакт између оператора критичне инфраструктуре и Центра за координацију и заштиту критичне инфраструктуре;

10) *европска критична инфраструктура* подразумева критичну инфраструктуру лоцирану на територији земље чланице, чије би ометање или уништење имало значајан утицај на најмање две земље чланице.

Начела деловања

Члан 3.

Надлежни државни и други органи, грађани и други субјекти дужни су да се у предузимању мера и активности утврђених овим и другим законом, програмима, плановима и другим документима у области критичне инфраструктуре руководе следећим начелима:

1) начело интегрисаног приступа – у заштити критичне инфраструктуре пре, за време и после квара или прекида функционисања критичне инфраструктуре учествују сви надлежни органи и организације, грађани и други субјекти узимајући у обзир различите врсте опасности које проистичу из процене ризика и узимајући у обзир међузависност сектора критичне инфраструктуре и њихову интеракцију;

2) начело одговорности – за рад критичне инфраструктуре директно су одговорни оператори критичне инфраструктуре, а заунапређење заштите критичне инфраструктуре, поред оператора и сви надлежни органи и организације, грађани и други субјекти;

3) начело заштите од разних врста претњи – оператори, надлежни органи и организације, грађани и други субјекти у обезбеђивању континуираног рада критичне инфраструктуре дужни су да узму у обзир различите врсте ризика;

4) начело континуираног планирања заштите критичне инфраструктуре – заштита критичне инфраструктуре се заснива на сталном процесу процене ризика по рад критичне инфраструктуре и процене адекватности мера заштите;

5) начело размене података и информација и заштите података – оператори, надлежни органи и организације, грађани и други субјекти су дужни да благовремено и континуирано размењују потребне податке и информације истовремено штитећи податке везане за критичну инфраструктуру, у складу са прописима којима се уређује заштита тајних података.

II. ЦЕНТАР ЗА КООРДИНАЦИЈУ И ЗАШТИТУ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Члан 4.

За потребе спровођења овог закона у Министарству унутрашњих послова се образује посебна организациона јединица – „Центар за координацију и заштиту критичне инфраструктуре“ (у даљем тексту: Центар).

Центар регулише, планира, координира, контролише, комуницира и даје информације у вези сакритичном инфраструктуром.

III. ИДЕНТИФИКАЦИЈА И ОДРЕЂИВАЊЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Критична инфраструктура

Члан 5.

Критична инфраструктура су системи, мреже и објекти чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност, економску стабилност, односно угрозити функционисање Републике Србије.

Идентификација критичне инфраструктура

Члан 6.

Идентификација критичне инфраструктуре врши се секторски у складу са дефинисаним критеријума.

За спровођење процеса идентификације критичне инфраструктуре у одређеном сектору задужена су министарства надлежна за одређене секторе.

Ближе прописе о дефинисању сектора, надлежних министарстава и критеријумима за идентификацију критичне инфраструктуре одређује Влада.

Одређивање критичне инфраструктуре

Члан 7.

Критичну инфраструктуру на предлог министра надлежног за унутрашње послове(у даљем тексту: министар), одређује Влада.

Члан 8.

Министарства задужена за секторе критичне инфраструктуре су дужна да у року дефинисаним овим законом, након завршеног поступка идентификације у складу са дефинисаним критеријумима, Центру доставе предлоге критичне инфраструктуре у свом сектору.

Министарства задужена за секторе критичне инфраструктуре су дужна да редовно, а најмање једном квартално извештавају Центар о новонасталим променама у свом сектору.

Министарства задужена за секторе критичне инфраструктуре су дужна да након завршеног поступка идентификације у складу са дефинисаним критеријумима Центру сваке године, најкасније до 31. октобра доставе предлоге измена и допуна критичне инфраструктуре у свом сектору.

Одлука о одређивању критичне инфраструктуре ажурира се сваке године, најкасније до 31. децембра.

IV. ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Безбедоносно-оперативни план за управљање ризиком

Члан 9.

Безбедоносно-оперативни план за управљање ризиком је документ којим се утврђују мере смањења и ризика, дефинишу одговорности и одређују дужности, те успоставља оквир за поступање у циљу отклањања, односно смањења последица безбедносних претњи дефинисаних у анализи ризика.

Ближе прописе о методологији, начину израде и садржају безбедоносно-оперативног плана за управљање ризиком доноси министар.

Оператори критичне инфраструктуре су дужни да израде безбедоносно-оперативни план за управљање ризиком и на исти прибаве сагласност од стране Центра одмах, а најкасније шест месеци по одређивању мреже, система или објекта за критичну инфраструктуру.

Официр за везу

Члан 10.

Оператори критичне инфраструктуре морају имати Официра за везу, односно лице које служи као контакт између оператора и Центра, које обезбеђује сталну контролу ризика и претњи, обавештава о променама у односу на критичну инфраструктуру, обавештава Центар о евалуацији ризика, претњи и рањивости, координира безбедоносно-оперативним планом, врши тестирања кроз вежбе и друге активности предвиђене планом и обавља све друге послове везане за критичну инфраструктуру.

Официра за везу именује Центар на предлог оператора критичне инфраструктуре из редова запослених одмах, а најкасније три месеца по одређивању мреже, система или објекта за критичну инфраструктуру. Предложено лице мора поседовати лиценцу за официра за везу.

Центар издаје лиценцу из става 2. овог члана лицу које има:

1. високо образовање (мастер академске студије, специјалистичке академске или специјалистичке струковне студије, односно основне студије у трајању од најмање четири године по пропису који је уређивао високо образовање до 10. септембра 2005. године);

2. положен посебан стручни испит за официра за везу.

Ближе критеријуме за добијање лиценце за официра за везу, као и Програм и начин полагања посебног стручног испита прописује министар.

Критична инфраструктура у планским документима

Члан 11.

Приликом израде планских документа и докумената из области националне безбедности, области смањења ризика и управљања ванредним ситуацијама критична инфраструктура се мора третирати на посебан начин, поготову у делу превентивних активности и активности везаних за одговор на ванредне ситуације у којима мора имати приоритет.

V. ЕВРОПСКА КРИТИЧНА ИНФРАСТРУКТУРА

Члан 12.

Европска критична инфраструктура је критична инфраструктура од интереса за најмање две државе чланице Европске уније.

Одређивање европске критичне инфраструктуре

Члан 13.

Европска критична структура се може одредити у секторима које одређује Европска комисија.

Европску критичну инфраструктуру на територији Републике Србије, на предлог Центра, одређује Влада, на захтев и у сагласности са заинтересованим државама чланицама Европске уније и обавештава заинтересоване државе чланице о одређивању европске критичне инфраструктуре на територији Републике Србије.

Ако се критична инфраструктура од значаја за Републику Србију налази на подручју друге државе чланице, Влада предлаже надлежном телу те државе одређивање европске критичне инфраструктуре.

Заштита европске критичне инфраструктуре

Члан 14.

Европска критична инфраструктура на територији Републике Србије штити се на исти начин као и критична инфраструктура Републике Србије, осим када је то прописима Европске уније другачије уређено.

Извештавање о европској критичној инфраструктури

Члан 15.

Влада усваја годишњи извештај о броју европске критичне инфраструктуре по сектору и броју заинтересованих држава на које свака одређена критична инфраструктура има утицај, а на предлог Центра.

Извештај из члана 1. овог члана доставља се Европској комисији и заинтересованим државама на које свака одређена критична инфраструктура има утицај.

Размена информација о европској критичној инфраструктури

Члан 16.

Контакт тачка за потребе размене информација и координацију активности у вези са европском критичном инфраструктуром са другим државама чланицама и телима Европске уније је Центар.

VI. ПОСТУПАЊЕ СА ТАЈНИМ ПОДАЦИМА

Члан 17.

Подаци у вези са критичном инфраструктуром представљају тајне податке у складу са законом којим се уређује тајност података и прописима донетим на основу овог закона.

Тајни подаци који се односе на Европску критичну инфраструктуру размењују се са страним државама и органима Европске уније у складу са законом којим је уређена тајност података и потписаним међународним споразумима о размени тајних података.

VII. НАДЗОР

Члан 18.

Надзор над применом овог закона и прописа донетих на основу њега врши Министарство. Министарство врши инспекцијски надзор преко инспектора Центра.

Овлашћења инспектора

Члан 19.

У вршењу инспекцијског надзора, инспектор Центра има право да:

- 1) утврди стање извршавања обавеза предвиђених овим законом, упозори на уочене неправилности и одреди мере и рокове за њихово отклањање;
- 2) врши увид у документа која се односе на критичну инфраструктуру;
- 3) проверава спровођење издатих наредби и закључака и наложи мере за извршење;
- 4) наложи израду, доношење и ажурирање докумената предвиђених овим законом;
- 5) наложи обуставу мера и радњи које нису у складу са Безбедоносно-оперативним планом;
- 6) наложи отклањање утврђених недостатака у спровођењу прописаних мера утврђених Безбедоносно-оперативним планом;
- 7) поднесе предлог за покретање поступака за утврђивање прекршајне одговорности против правних и одговорних лица;
- 8) нареди предузимање хитних мера;
- 9) предузме и друге мере за које је овлашћен законом.

Против решења инспектора може се изјавити жалба у року од осам дана од дана достављања решења.

Жалба против решења инспектора донетог на основу става 1. тач. 5) и 8) овог члана не одлаже извршење решења.

VIII. КАЗНЕНЕ ОДРЕДБЕ

Члан 20.

Новчаном казном у износу од 100.000 до 1.000.000 динара казниће се за прекршај правно лице уколико:

- 1) не доставе Центру предлоге критичне инфраструктуре у свом сектору(члан 8. став 1.);
- 2) не извештавају Центар о новонасталим променама у свом сектору (члан 8. став 2.);
- 3) не доставе Центру предлоге измена и допуна критичне инфраструктуре у свом сектору(члан 8. став 4.);
- 4) не прибаве сагласност Центра на безбедоносно-оперативни план за управљање ризиком(члан 9. став 3.);
- 5) не доставе Центру предлог за именовање официра за везу(члан 10. став 2.);
- 6) лице које је у предлогу за именовање официра за везу достављено Центру не испуњава потребне услове (члан 10. став 3.);
- 7) не поступи по налогу инспектора (члан 19. став 1.).

Члан 21.

Новчаном казном од 50.000 до 100.000 динара казниће се за прекршај из члана 20. став 1. тач. 1) – 7) и одговорно лице у надлежном државном органу.

IX. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 22.

Подзаконски акти за спровођење овог закона донеће се у року од шест месеци од дана ступања овог закона за снагу.

Члан 23.

Измене акта о унутрашњем уређењу и систематизацији радних места у Министарству унутрашњих послова донеће министар у року од 30 дана од дана ступања овог закона на снагу.

Члан 24.

Министарства задужена за секторе критичне инфраструктуре су дужна да у року од шест месеци од усвајања подзаконског акта, а након завршеног поступка идентификације у складу са дефинисаним критеријумима Центру доставе предлоге критичне инфраструктуре у свом сектору.

Члан 25.

Одредбе које се односе на европску критичну инфраструктуру почињу да се примењују даном приступања Републике Србије Европској унији.

Члан 26.

Овај закон ступа на снагу осмог дана од објављивања у „Службеном гласнику Републике Србије“.