НАЦРТ

ЗАКОН

о изменама и допунама Закона о информационој безбедности

Члан 1.

У Закону о информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17) у члану 2. став 1. тач. 2) и 15), члану 5. став 2, члану 6. став 1. тачка 1) и члану 15. став 1. тачка 5) речи: „органи јавне власти” у одређеном падежу замењују се речима: „органи власти” у одговарајућем падежу.

Члан 2.

У члану 2. став 1. тачка 1) подтачка (3) реч: „“похрањује” замењује се речима „воде, чувају”.

У тачки 1) додаје се подтачка (5) која гласи:

„(5) све типове системског и апликативног софтвера и софтверске развојне алате.”.

Тачка 15) мења се и гласи:

„15) орган власти је државни орган, орган аутономне покрајине, орган јединице локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења;”

Тачка 24) мења се и гласи:

„24) информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично;”

После тачке 24) додају се тач. 25) и 26), које гласе:

„25) услуга информационог друштва је услуга у смислу закона којим се уређује електронска трговина;

26) пружалац услуге информационог друштва је пружалац услуге у смислу закона којим се уређује електронска трговина”.

Члан 3.

После члана 3. додаје се назив члана и члан 3а, који гласе:

„Обрада података о личности

Члан 3а

У случају обраде података о личности приликом вршења надлежности и испуњења обавеза из овог закона поступа се у складу са прописима који уређују заштиту података о личности.”

Члан 4.

У члану 5. став 1. након речи „Генералног секретаријата Владе” додају се речи: „Народне банке Србије“, а речи: „ЦЕРТ-а републичких органа и Националног ЦЕРТ-а” замењују се речима: „Центра за безбедност ИКТ система у органима власти и Националног центра за превенцију безбедносних ризика у ИКТ системима.”

Члан 5.

Члан 6. мења се и гласи:

„ИКТ системи од посебног значаја

Члан 6.

ИКТ системи од посебног значаја су системи који се користе:

1) у обављању послова у органима власти;

2) за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности;

3) у обављању делатности од општег интереса и другим делатностима и то у следећим областима:

(1) енергетика:

- производња, пренос и дистрибуција електричне енергије;
- производња и прерада угља;
- истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата;
- истраживање, производња, прерада, транспорт и дистрибуција природног и течног гаса.

(2) саобраћај:

- железнички, поштански, водени и ваздушни саобраћај;

(3) здравство:

- здравствена заштита;

(4) банкарство и финансијска тржишта:

- послови финансијских институција;
- послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама;
- послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта;

(5) дигитална инфраструктура:

- размена интернет саобраћаја;

- управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи)

(6) добра од општег интереса:

- коришћење, управљање, заштита и унапређивање добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја);

(7) услуге информационог друштва:

- услуге информационог друштва у смислу члана 2. тачка 25) овог закона;

(8) остале области:

- електронске комуникације;
- издавање службеног гласила Републике Србије;
- управљање нуклеарним објектима;
- производња, промет и превоз наоружања и војне опреме;
- управљање отпадом;
- комуналне делатности;
- производња и снабдевање хемикалијама.

4) у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности из тачке 3) овог става.

Влада, на предлог министарства надлежног за послове информационе безбедности, утврђује листу делатности из става 1. тачка 3) овог члана.”

Члан 6.

После члана 6. додају се чл. 6а и 6б, који гласе:

„Обавезе оператора ИКТ система од посебног значаја

Члан 6а

Оператор ИКТ система од посебног значаја у складу са овим законом у обавези је да:

1) упише ИКТ систем од посебног значаја којим управља у евиденцију оператора ИКТ система од посебног значаја;

2) предузме мере заштите ИКТ система од посебног значаја;

3) донесе акт о безбедности ИКТ система;

4) врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње;

5) уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја трећим лицима;

6) доставља обавештења о инцидентима који значајно угрожавају информациону безбедност ИКТ система;

7) достави статистичке податке о инцидентима у ИКТ систему.

Евиденција оператора ИКТ система од посебног значаја

Члан 6б

Надлежни орган успоставља и води евиденцију ИКТ система од посебног значаја (у даљем тексту: Евиденција) која садржи:

1) назив и седиште оператора ИКТ система од посебног значаја;

2) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон администратора ИКТ система од посебног значаја;

3) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон одговорног лица ИКТ система од посебног значаја

4) податак о врсти ИКТ система од посебног значаја, у складу са чланом 6. овог закона.

Поред података из става 1. овог члана, евиденција може да садржи и друге допунске податке о ИКТ систему од посебног значаја које прописује Надлежни орган.

Оператор ИКТ система од посебног значаја дужан је да ИКТ систем од посебног значаја којим управља упише у евиденцију из става 1. овог члана.

Оператор ИКТ система од посебног значаја дужан је да надлежном органу достави податке из става 1. најкасније 90 дана од дана усвајања прописа из члана 6. става 2. овог закона, односно 90 дана од дана успостављања ИКТ система од посебног значаја.

Надлежни орган ставља на располагање Националном центру за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: национални ЦЕРТ) ажурну евиденцију из става 1. овог члана.”

Члан 7.

У члану 7. став 2. реч: „минимизација” замењује се речју: „смањење”.

У ставу 3. тачка 11) реч: „односно” замењује се речју: „и”.

У тачки 23) речи: „питања информационе безбедности” замењују се речима: „испуњење захтева за информациону безбедност”.

Члан 8.

Члан 11. мења се и гласи:

„Обавештавање о инцидентима

Члан 11.

Оператори ИКТ система од посебног значаја обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности врше преко портала Надлежног органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима којег одржава Надлежни орган.

Уколико органи из става 1. овог члана буду обавештени о инциденту на други начин, податке о инциденту уносе у систем из става 1. овог члана.

Изузетно од става 1. овог члана, обавештење о инцидентима се упућује:

1) Народној банци Србије, у случају инцидената у ИКТ системима из члана 6. став 1. тачка 3) подтачка (4) алинеја прва овог закона;

2) регулаторном телу за електронске комуникације у случају инцидената у ИКТ системима из члана 6. став 1. тачка 3) подтачка 8) алинеја прва овог закона.

Народна банка Србије и регулаторно тело за електронске комуникације обавештења из става 3. овог члана достављају у јединствени систем за пријем обавештења о инцидентима на начин из става 1. овог члана.

Након пријаве инцидента, уколико је инцидент и даље у току, оператори ИКТ система од посебног значаја достављају обавештења о битним догађајима у вези са инцидентом и активностима које предузимају до престанка инцидента органу коме су у складу са овим законом пријавили инцидент.

Оператори ИКТ система од посебног значаја достављају завршни извештај о инциденту органу кога су у складу са овим законом обавештавали о инциденту у року од 15 дана од дана престанка инцидента.

У случају инцидената у ИКТ системима за рад са тајним подацима оператори тих ИКТ система поступају у складу са прописима којима се уређује област заштите тајних података.

Одредбе ст. 1 и 3. овог члана не односе се на самосталне операторе ИКТ система.

Влада, на предлог Надлежног органа, уређује поступак обавештавања о инцидентима, листу, врсте и значај инцидената према нивоу опасности, поступање и размену информација о инцидентима између органа из члана 5. овог закона.

Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 3. овог члана коме се упућују обавештења о инцидентима, може објавити информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио.

Ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, орган коме је упућено обавештење о инциденту, обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове.

Ако је инцидент повезан са значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање националне безбедности, орган коме је упућено обавештење о инциденту обавештава Безбедносно-информативну агенцију.

У случају наступања околности угрожавања, ометања рада или уништења ИКТ система од посебног значаја руковођење и координацију спровођења мера и задатака у наведеним околностима предузима Републички штаб за ванредне ситуације, у складу са законом.”

Члан 9.

После члана 11. додају се чл. 11а и 11б, који гласе:

„Инциденти у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности

Члан 11а

Оператор ИКТ система од посебног значаја дужан је да пријави следеће инциденте који могу да имају значајан утицај на нарушавање информационе безбедности:

1) инциденте који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;

2) инциденте који утичу на велики број корисника услуга, или трају дужи временски период;

3) инциденте који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;

4) инциденте који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

5) инциденте који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе;

6) инциденте који су настали као последица инцидента у ИКТ систему из члана 6. став 1. тачка 3) подтачка (7) овог закона, када ИКТ систем од посебног значаја у свом пословању користи информационе услуге ИКТ система из члана 6. став 1. тачка 3) подтачка (7) овог закона.

Оператор ИКТ система од посебног значаја дужан је да пријави и инциденте који су довели до значајног повећања ризика од наступања последица из става 1. овог члана.

Достављање статистичких података о инцидентима

Члан 11б

Оператор ИКТ система од посебног значаја дужан је да, поред обавештавања о инцидентима из члана 11. овог закона, достави Националном ЦЕРТ-у статистичке податке о свим инцидентима у ИКТ систему у претходној години најкасније до 28. фебруара текуће године.

Национални ЦЕРТ обједињене статистичке податке из става 1. овог члана доставља Надлежном органу и објављује их на порталу Националног ЦЕРТ-а.

Врсту, форму и начин достављања статистичких података из става 1. овог члана уређује Национални ЦЕРТ.“.

Члан 10.

У члану 12. став 2. речи: „високи ризици” замењују се речју „високоризични”.

Члан 11.

У члану 13. додаје се назив члана који гласи: „Самостални оператори ИКТ система”.

Члан 12.

У члану 14. у називу члана и ставу 1. бришу се речи: „Национални центар за превенцију безбедносних ризика у ИКТ системима”.

Члан 13.

Члан 15. мења се и гласи:

„Надлежности Националног ЦЕРТ-а

Члан 15.

Национални ЦЕРТ прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност, а посебно:

1) прати стање о инцидентима на националном нивоу,

2) пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима,

3) реагује по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и другим ИКТ системима у Републици Србији, тако што пружа савете и препоруке на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања,

4) континуирано израђује анализе ризика и инцидената,

5) подиже свест код грађана, привредних субјеката и органа власти о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљу подизања те свести,

6) води евиденцију Посебних ЦЕРТ-ова;

7) извештава Надлежни орган на кварталном нивоу о предузетим активностима.

Национални ЦЕРТ обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације.

Просторије и информациони системи Националног ЦЕРТ-а морају да се налазе на безбедним локацијама.

У циљу обезбеђивања континуитета рада, Национални ЦЕРТ треба да:

1) буде опремљен са одговарајућим системима за управљање инцидентима;

2) има довољно запослених како би се осигурала доступност у свако доба;

3) обезбеди инфраструктуру чији је континуитет осигуран, односно да обезбеди редундантне системе и резервни радни простор.

Национални ЦЕРТ непосредно сарађује са Надлежним органом, Посебним ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних оператора ИКТ система, као и са ЦЕРТ-ом органа власти.

Национални ЦЕРТ промовише усвајање и коришћење прописаних и стандардизованих процедура за:

1) управљање и санирање ризика и инцидената;

2) класификацију информација о ризицима и инцидентима, односно класификацију према нивоу инцидената и ризика.”

Члан 14.

После члана 15. додаје се члан 15а, који гласи:

„Сарадња ЦЕРТ-ова у Републици Србији

Члан 15а

Национални ЦЕРТ, ЦЕРТ органа власти и ЦЕРТ-ови самосталних оператора ИКТ система одржавају континуирану сарадњу.

ЦЕРТ-ови из става 1. овог члана одржавају међусобне састанке у организацији Националног ЦЕРТ-а најмање три пута годишње, као и по потреби у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији.

Састанцима ЦЕРТ-ова из става 1. овог члана присуствују и представници Надлежног органа.

Састанцима ЦЕРТ-ова из става 1. овог члана могу, по позиву, да присуствују и представници посебних ЦЕРТ-ова, као и друга лица.”

Члан 15.

У члану 16. додаје се назив члана који гласи: „Надзор над радом Националног ЦЕРТ-а”

Члан 16.

У члану 17. став 5. речи: „Надлежни орган” замењују се речима: „Национални ЦЕРТ”.

Члан 17.

У члану 18. и у називу члана речи „републичким органима власти” у одређеном падежу замењују се речима „органима власти”.

У ставу 1. бришу се речи: „Центар за безбедност ИКТ система у републичким органима (у даљем тексту:)”.

Члан 18.

У члану 19. додаје се назив члана који гласи: „ЦЕРТ самосталног оператора ИКТ система”.

У ставу 2. речи: „републичких органа” замењују се речима: „органа власти”.

Члан 19.

После члана 19. додају се назив члана и члан 19а, који гласи:

„Заштита при коришћењу информационо-комуникационих технологија

Члан 19а

Надлежни орган предузима превентивне мере за безбедност и заштиту на интернету, као активности од јавног интереса, путем едукације и информисања грађана, а посебно деце, родитеља и наставника, о предностима, ризицима и начинима безбедног коришћења интернета, као и путем јединственог места за пружање савета и пријем пријава у вези безбедности на интернету, и упућује пријаве надлежним органима ради даљег поступања.

Оператор електронских комуникација који пружа јавно доступне телефонске услуге дужан је да омогући свим претплатницима услугу бесплатног позива према јединственом месту за пружање савета и пријем пријава у вези безбедности на интернету.

У случају да наводи из пријаве упућују на постојање кривичног дела, на повреду права, здравственог статуса, добробити и/или општег интегритета лица, на ризик стварања зависности од коришћења интернета, пријава се прослеђује надлежном органу власти ради поступања у складу са утврђеним надлежностима.

Надлежни орган је овлашћен да врши обраду података о лицу које се обрати Надлежном органу у складу са законом и другим прописима.

Обрада података о лицу из става 4. овог члана обухвата име, презиме и број телефона и/или адресу електронске поште и врши се у складу са законом који уређује заштиту података о личности, у сврху евидентирања поднетих пријава, информисања подносиоца пријаве о статусу предмета и, у случају потребе, упућивања пријаве надлежним органима ради даљег поступања, у складу са законом.

Подаци о личности из става 5. овог члана чувају се у роковима предвиђеним прописима који уређују канцеларијско пословање.

У циљу обезбеђивања континуитета рада јединственог места за пружање савета и пријем пријава у вези безбедности на интернету, надлежни орган треба да:

1) буде опремљен са одговарајућим системима за пријем пријава;

2) има довољно запослених како би се осигурала доступност у раду;

3) обезбеди инфраструктуру чији је континуитет осигуран.

Влада ближе уређује начин спровођења мера за безбедност и заштиту на интернету из ст. 1. и 3. овог члана.”

Члан 20.

У члану 30. ст. 1. и 5. речи: „правно лице” у одговарајућем падежу замењују се речима: „оператор ИКТ система од посебног значаја”.

У ставу 1. додају се тач. 1) и 5), које гласе:

„1) не изврши упис у евиденцију у року из члана 6б овог закона;”

„5) не достави статистичке податке у року из члана 11б овог закона;”

Досадашње тач. 1), 2), 3) и 4) постају тач. 2), 3), 4) и 6).

Члан 21.

Члан 31. мења се и гласи:

„Члан 31.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај оператор ИКТ система од посебног значаја ако:

1) о инцидентима у ИКТ систему не обавести органе из члана 11. ст. 1, 3. и 7. овог закона;

2) не доставља обавештења о битним догађајима у вези са инцидентом и активностима из члана 11 став 5. овог закона;

3) не достави завршни извештај у року из члана 11. став 6. овог закона.

За прекршаје из става 1. овог члана казниће се и одговорно лице у оператору ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Изузетно од ст.1. и 2. овог члана, ако финансијска институција не обавести Народну банку Србије о инцидентима у ИКТ систему од посебног значаја, Народна банка Србије изриче тој финансијској институцији мере и казне у складу са законом којим се уређује пословање финансијских институција.

Члан 22.

Подзаконски акти из чл. 5, 8 и 19. овог закона донеће се у року од шест месеци од дана ступања на снагу овог закона.

Подзаконски акти из чл. 6. и 9. овог закона донеће се у року од три месеца од дана ступања на снагу овог закона.

Члан 23.

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