ОБРАЗЛОЖЕЊЕ

I. УСТАВНИ ОСНОВ

Уставни основ за доношење Закона о информационој безбедности садржан је у члану 97. тачка 12. Устава Републике Србије, којим је предвиђено да Република Србија уређује и обезбеђује развој Републике Србије, политику и мере за подстицање равномерног развоја појединих делова Републике Србије, укључујући и развој недовољно развијених подручја; организацију и коришћење простора; научно-технолошки развој.

II. РАЗЛОЗИ ЗА ДОНОШЕЊЕ ЗАКОНА

Како би се Република Србија успешно укључила у јединствено европско дигитално тржиште неопходно је обезбедити регулаторне и институционалне услове за убрзан развој дигиталног тржишта у Републици Србији, као и обезбедити да се тај развој одвија у сигурним условима како за сваког појединца, тако и за друштво у целини.

У дигиталном окружењу које се мења, императив је да Влада, пословни субјекти и организације раде заједно на развоју регулаторног оквира који унапређује ИКТ системе и мреже на начин да је омогућено безбедно и неометано чување података и пружање услуга, као и одвијање других процеса. Са константним порастом употребе ИКТ у свакодневном животу, као и са порастом броја услуга које се нуде грађанима електронским путем, неопходно је благовремено одговорити на развијне изазове и пратити динамичан развој сектора уз обавезу сталног усклађивања и праћења прописа Европске уније из ове области.

Област информационе безбедности уређена је Законом о информационој безбедности („Службени гласник РС”, бр. 6/2016, 94/2017 и 77/2019, у даљем тексту: ЗИБ) и подзаконским актима донетим на основу тог закона.

ЗИБ се ослања на Директиву ЕУ 2016/1148 Европског парламента и Савета од 6. јула 2016. године која се тиче мера за високи заједнички ниво безбедности мрежа и информационих система (у даљем тексту: НИС1). У процесу испуњавања услова за пуноправно чланство у Европској унији, Република Србија је дужна да своје законодавство усклади са правним тековинама Европске уније у области информационе безбедности. У међувремену, ЕУ је свој регулаторни оквир употпунила и ревидирала усвајњем Акта ЕУ о сајбер безбедности 2019. године и у свајањем нове Директиве (ЕУ) 2022/2055 Европског парламента и Савета од дана 14. децембра 2022. године о мерама за висок заједнички ниво сајбер безбедности (у даљем тексту НИС2). У том смислу, први разлог доношења новог закона лежи у потреби да се регулаторни оквир усагласи са оквиром који је на снази у ЕУ како би се благовремено испратили развојни трендови у овој области и омогућило да се употреба ИКТ у Републици Србији одвија у складу са најсавременијим регулаторним тенденцијама.

Директива НИС2 са собом доноси редефинисан приступ информационој безбедности, превасходно у смислу идентификације оператора ИКТ система од посебног значаја и разликовања истих на приоритетне и важне, уз пропратне

обавезе и појачани инспекцијски надзор и ревизију, као и строжију казнену политику. Потом јача улогу Националног ЦЕРТ-а у смислу надлежности и реаговања на инцидент или претњу да може доћи до инцидента, омогућава бољу координацију надлежних органа и детаљније уређује питање међународне сарадње и размене информација.

Акт о сајбер безбедности ЕУ 2019/881, између осталог, успоставља обавезу развоја националног оквира сертификације, као и шема сертификације ИКТ производа, процеса и услуга са циљем унапређења ових сајбер производа у погледу њихових безбедносних аспеката.

Такође, имајући у виду опсег ових прописа и додатне обавезе на страни државних органа да омогуће безбедну употребу ИКТ, створила се и потреба за ревизијом досадашњег институционалног оквира са циљем да се надлежни органи припреме за неопходан развој капацитета за одговор на ризике и претње приликом употребе ИКТ система и мрежа.

Имајући у виду наведено, најзначајнији циљеви који се доношењем новог закона у области информационе безбедности имају постићи јесу усклађивање са НИС2 и Актом о сајбер безбедности са сврхом да се утврди регулаторни оквир који одговара савременим развојним тенденцијама на тлу Европе и испуни обавеза из Споразума о стабилизацији и придруживању и поступка приступања Републике Европској унији, као и да се унапреди институционални оквир са циљем да се он оспособи да правилно примењује новоуспостављене обавезе и надлежности. Поред тога, овом изменом законског оквира потребно је и унапредити постојећа решења на основу искуства из досадашње примене, као и организационо и структурално унапредити законски текст.

Нацртом закона уређују се следеће области:

1. основне одредбе, којима се уређује предмет закона као и значење појединих појмова који се користе у закону;
2. безбедност ИКТ система од посебног значаја;
3. правни положај и надлежности органа надлежних за превенцију и заштиту од безбедносних ризика у ИКТ системима у Републици Србији;
4. криптобезбедност и заштита од компромитујућег електромагнетног зрачења;
5. надлежности и одговорности субјеката за надзор над спровођењем закона;
6. казнене одредбе;
7. казнене одредбе;
8. прелазне и завршне одредбе.

Основни разлози због којих се предлаже доношење закона су:

- унапређење законских решења и отклањање недостатака важећег закона који су уочени кроз његову досадашњу примену;
- спровођење активности које су усмерене на даље јачање капацитета и развојних могућности органа надлежних за област информационе безбедности;
- унапређење безбедне употребе ИКТ система и мрежа у Републици Србији;
- промовисање додатног јачања конкуренције на тржишту даљим развојем начина пружања услуга електронским путем;

- унапређење заштите неометаног пружања услуга електронским путем, као и безбедности чувања података;
- стимулисање домаћих и страних инвестиција;
- успостављање правног основа и надлежности за развој оквира и шема сертификације ИКТ производа, процеса и услуга;
- стварање оптималних услова за безбедно коришћење ИКТ од стране појединаца, организација, привредних субјеката и државних органа и организација.

Овом регулаторном изменом постижу се циљеви који се тичу усклађености са важећим регулаторним оквиром ЕУ, остварује се креирање регулаторног оквира који је у стању да омогући унапређени и координисани заједнички одговор на информационо - безбедносне ризике и претње и унапређују се институционални капацитети на начин који ће омогућити њихов даљи развој и стварање способности да преузму проширене надлежности и задатке.

Имајући у виду да је у поступку придруживања Европској унији Република Србија преузела обавезу да усклади своје законодавство са прописима Европске уније, потребно је извршити усклађивање законодавства доношењем овог закона и тиме испунити преузете обавезе. Како је приступ информационој безбедности новим оквиром фундаментално измењен и уводе се поједине нове тематске области у вези са којима постоји правна празнина, као и да значајније унапређење институционалног оквира може само законом да се успостави, ни једна друга могућност осим законодавна измена није адекватна за остварење ових циљева. Закони, а посебно системски, представљају основ за развој области.

Сви наведени ефекти новог закона треба да омогуће адекватан одговор на ризике и претње у вези са употребом ИКТ у одвијању свакодневних активности, пружању услуга и циркулисању података.

Такође, изражена је потреба да и законска решења буду флексибилна и отворена за нова технолошка достигнућа, да се заснивају на решењима садржаним у међународним документима, прописима и стандардима Европске уније, а посебно на решењима технолошки развијених земаља.

Доношење овог закона није само најбољи, већ је, у постојећем нормативном оквиру и једини начин за решавање проблема и достизање циљева, али и за потпуно транспоновање европског регулаторног оквира.

Најважнија законска решења односе се на:

- Дефинисање приоритетних и важних ИКТ система од посебног значаја;
- Оснивање Канцеларије за информациону безбедност;
- Одређивање активности које ИКТ системи од посебног значаја треба да предузму ради заштите безбедности ИКТ система (мере заштите, процена ризика, акт о безбедности)
- Процедуре у случају инцидента који значајно угрожавају информациону безбедност оператора ИКТ система
- Активну улогу Националног ЦЕРТ-а и ЦЕРТ-а органа у отклањању инцидената у ИКТ системима
- Проширена инспекцијска овлашћења.

Сходно одредбама НИС2 директиве, овим законом се дефинишу оператори ИКТ система од посебног значаја који се деле на приоритетне и важне. Приоритетни ИКТ системи од посебног значаја од кључног значаја за одржавање критичних друштвених и економских активности чији би прекид или поремећај у пружању услуга имао значајан утицај на јавну безбедност, јавно здравље, функционисање других сектора или би створио значајан системски ризик. Реч је о ИКТ системима у областима које су виталне за функционисање друштва (енергетика, здравство, банкарство и друге области) и који због свог значаја морају да буду безбедни како би се делатности обављале неометано.

Поред ових система, закон прописује и важне ИКТ системе од посебног значаја, и то из области чије би угрожавање потенцијално могло да има неповољан ефекат на на јавни интерес, функционисање других сектора или би створио значајан системски ризик.

Услед неопходности да функционишу несметано и сачувају интегритет података и услуга које пружају, ИКТ системи од посебног значаја треба да буду заштићени применом различитих мера (примена мера заштите у складу са законом, националним и међународним стандардима, одговарајућа процена ризика, доношење акта о безбедности, редовне периодичне провере ИКТ система).

Посебна новина у односу на постојећи законски режим је обавезно обављање процене ризика ИКТ система и доношење Акта о процени ризика ИКТ система, имајући у виду да организације морају да буду свесне опасности које могу да угрозе информациону безбедност и на основу тога предузму мере заштите одговарајућег нивоа у односу на потенцијални ризик.

Закон предвиђа процедуре у случају инцидената који значајно угрожавају информациону безбедност у Републции Србији. Предложена је класификација инцидената према нивоу опасности, као и поступање надлежних органа зависно од нивоа опасности. Дефинисано је и поступање у случају кризе информационе безбедности, која је догађај или стање које угрожава, омета рад или онемогућује рад ИКТ система од посебног значаја и при том изазива ризике, претње или последице по становништво, материјална добра или животну средину изузетно великог обима и интензитета које није могуће спречити или отклонити редовним деловањем надлежних органа и служби, а одговор на такав догађај или стање захтева учешће више надлежних органа, као и примену одговарајућих мера.

У складу са све чешћом праксом других развијених земаља, које оснивају органе посебно задужене за информациону безбедност, тако и наша земља планира да овим законом оснује Канцеларију за информациону безбедност.

Канцеларија за информациону безбедност, која би имала статус посебне организације у смислу закона којим се уређује државна управа и која би почела са својим радом 1. јуна 2027. године, треба да удружи постојеће ресурсе у области информационе безбедности и тиме побољша одговор Републике Србије на изазове у области информационе безбедности. Планирано је да Канцеларија за информациону безбедност врши послове координације и управљања одговором на инциденте у ИКТ системима од посебног значаја који значајно угрожавају информациону безбедност, како би се благовремено и адекватно реаговало на инциденте у овим системима Канцеларија за информациону безбедност биће дужна да реагује хитно и без одлагања и да активно учествује у отклањању инцидента који могу да наруше безбедност ИКТ система од посебног значаја, и угрозе функционисање државе, привреде и

грађана. Такође, Канцеларија за информациону безбедност обавља послове Националног ЦЕРТ-а, ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе, врши послове јединствене тачке контакта у међународној сарадњи, прописује минималне мере заштите ИКТ система органа, у сарадњи са надлежним органима и другим субјектима из јавног, академског, привредног и невладиног и приватног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности у органима и друге послове у складу са законом. Законом је предвиђено да до образовања Канцеларије за информациону безбедност ове послове вршиће Канцеларија за информационе технологију и електронску управу.

Законом се уређују и послови криптобезбедности и заштите од компромитујућег електромагнетног зрачења (КЕМЗ). Министарство одбране, као и у досадашњем законском режиму, послове информационе безбедности који се односе на одобравање криптографских производа који се користе за заштиту преноса и чувања података који су одређени као тајни, дистрибуцију криптоматеријала и заштиту од компромитујућег електромагнетног зрачења и послове и задатке у складу са законом и прописима донетим на основу закона.

Поред овога, предложене су и одредбе које се односе на надзор над применом овог закона и санкције у случају непоштовања одредби.

III. ОБЈАШЊЕЊЕ ПОЈЕДИНИХ РЕШЕЊА

Члан 1. Нацрта закона – Овим законом се уређују мере заштите од безбедносних ризика у информационо - комуникационим системима, одговорности субјеката приликом управљања и коришћења информационо-комуникационих система, поступци и мере за постизање високог општег нивоа информационе безбедности и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите, праћење правилне примене прописаних мера заштите, као и надлежности субјеката за надзор над спровођењем овог закона.

Члан 2. Нацрта закона – овим чланом утврђује се значење појединих термина у смислу овог закона.

Члан 3. Нацрта закона – овим чланом утврђују се начела информационе безбедности приликом планирања и примене мера заштите ИКТ система.

Члан 4. Нацрта закона – прописује се опште правило у вези са обрадом података о личности.

Члан 5. Нацрта закона – овим чланом утврђују се приоритетни оператори ИКТ система од посебног значаја, односно они оператори ИКТ система од кључног значаја за одржавање критичних друштвених и економских активности чији би прекид или поремећај у пружању услуга имао значајан утицај на јавну безбедност, јавно здравље, функционисање других сектора или би створио значајан системски ризик. Оператори су идентификовани према делатностима у следећим областима: енергетика, саобраћај, банкарство и финансијска тржишта, здравство, вода за пиће, отпадне воде, дигитална инфраструктура, пружање услуга ИКТ операторима ИКТ система од посебног значаја, управљање нукеларник објектима, пружање услуга од поверења, пружање услуга ДНС, делатност електронских комуникација, тачка за размену интернет саобраћаја, и она делатност где постоји само један пружалац услуге. Поред ових субјеката, приоритетним операторима ИКТ система сматрају се органи јавне власти, сви

субјекти који су препознати као оператори критичне инфраструктуре и оператори који су по постојећем закону препознати као оператори ИКТ система у наведеним делатностима.

Члан 6. Нацрта закона – овим чланом уређују се важни оператори ИКТ система од посебног значаја чији би пекид или поремећај у пружању услуга магао да има значајан утицај на јавни интерес, функционисање других сектора или би се створио значајан системски ризик. Они су препознати као оператори у следећим делатностима: поштанске услуге, управљање отпадом, хемикалије, храна, рачунари и електронски и оптички производи, електрична опрема, машине и уређаји, услуге информационог друштва, наоружање и војна опрема, научноистраживачки рад, оператори у делатностима из члана 5. који не прођу секторски праг за приоритетне операторе ИКТ система. Предвиђено је и доношење подзаконског акта којим се ближе уређују услови, општи и сектроски критеријуми за одређивање оператора приоритетних и важних ИКТ система од посебног значаја које доноси Влада, на предлог министарства надлежног за послове информационе безбедности.

Члан 7. Нацрта закона – овим чланом уређују се обавезе оператора ИКТ система у смислу овог закона.

Члан 8. Нацрта закона – овим чланом уређују се обавезе самосталних оператора ИКТ система у смислу овог закона.

Члан 9. Нацрта закона – овим чланом уређују се питања вођења евиденције опеартора ИКТ система од посебног значаја, изузеци од обавезе уписа у евиденцију, садржина и подаци који се уносе у евиденцији, сврха обраде података о личности.

Члан 10. Нацрта закона – овим чланом прописују се мере заштите ИКТ система које је сваки опеартор ИКТ система од посебног значаја дужан да предузима.

Члан 11. Нацрта закона – овим чланом прописује обавеза доношења Акта о процени ризика ИКТ система од посебног значаја.

Члан 12. Нацрта закона – овим чланом прописује се обавеза доношења Акта о безбедности ИКТ система од посебног значаја.

Члан 13. Нацрта закона – овим чланом уређује се обавеза обавештавања оператора ИКТ система од посебног значаја о инцидентима који значајно нарушвају информациону безбедност.

Члан 14. Нацрта закона – овим чланом уређује се достављање обавештења о инцидентима, као изузеци који се односе на Народну банку Србије, регулаторно тело за електронске комуникације, самосталне операторе и начин поступање по пријави инцидента уколико је реч о инциденту који је одређен као критична инфраструктура у складу са законом којим се уређује критична инфраструктура

Члан 15. Нацрта закона – овим чланом уређује се садржај обавештења о инциденру, које садржи податке који се односе на подносиоца пријаве, врсту и опис инцидента, датум и време почетка и трајања инцидента, предузете активности, процена нивоа и утицаја опасности и друге релевантне информације.

Члан 16. Нацрта закона – овим чланом врши се идентификација инцидената према њиховом значају и домету, као и нивоу опасности.

Члан 17. Нацрта закона – овим чланом успоставља се оперативни тим за реговање на инциденте „високог“ и „веома високог“ новоа, који образује Канцеларија за информациону безбедност.

Члан 18. Нацрта закона – овим чланом уређује се план за реаговање у случају инцидента „високог“ нивоа, криза информационе безбедности, који доноси Влада на предлог Канцеларије за информациону безбедност.

Члан 19. Нацрта закона – овим чланом уређује се поступање по пријему обавештења о инциденту.

Члан 20 - 23. Нацрта закона – овим чланом уређује се поступање у случају инцидента према следећем нивоу опасности и то: „низак“, „средњи“, „висок“ и „веома висок“.

Члан 24. Нацрта закона – овим чланом уређује се начин извештавања оператора ИКТ система од посебног о инциденту, током ицидента и након инцидента у зависности од нивоа опасности.

Члан 25. Нацрта закона – овим чланом уређује начин достављања статистичких података о инцидентима.

Члан 26 - 27. Нацрта закона – овим члановима уређује се надлежност Министарства информисања и телекомуникација и успоставља се Тело за координацију послова информационе безбедности.

Члан 28-29-30. Нацрта закона – овим члановима оснива се Канцеларија за информациону безбедност као посебна организација са својством правног лица, утврђује се њен делокруг надлежности, као и надзор над њеним радом.

Члан 31. Нацрта закона – овим чланом прописују се послови Националног ЦЕРТ-а, у циљу превенције и заштите од безбедносних ризика и инцидената.

Члан 32. Нацрта закона – овим чланом утврђују се послови ЦЕРТ-а Јединствене информационо- комуникационе мреже електронске управе.

Члан 33 - 34. Нацрта закона – овим члановима уређује се сарадња надлежних органа на националном нивоу, као и међународна сарадња и послови јединствене тачке контакта за размену информација о инцидентима.

Члан 35. Нацрта закона - овим чланом уређују се питања посебних центара за превенцију безбедносних ризика у ИКТ системима.

Члан 36. Нацрта закона – овим уређује се обавеза успостављања и одржавање базе рањивости.

Члан 37. Нацрта закона – овим чланом уређује се питање заштите деце при коришћењу ИКТ технологија.

Члан 38 - 45. Нацрта закона – овим члановима уређује се питање одобравања криптографских производа, дистрибуција криптоматеријала и заштита од компромитујућег електромагнетног зрачења.

Члан 46 - 47 Нацрта закона – овим члановима успоставња се инспекција за информацину безбедност и прописију овлашћења инспектора за информациону безбедност.

Члан 48 - 51. Нацрта закона – ови члановима прописују се износи новчане казне за прекршај који учине правно лице, одговорно лице у правном лицу, као и предузетник и оне су подељене у више распона зависно од утврђеног прекршаја.

Члан 52 - 56. Нацрта закона – овим члановима уређују се прелазне и завршне одредбе и то: рокови за доношење подзаконских аката, примена одређених одредби Закона о информационој безбедности који је на снази, престанак важења Закона о информационој безбедности и ступање на снагу.

IV. ПРОЦЕНА ФИНАНСИЈСКИХ СРЕДСТАВА ПОТРЕБНИХ ЗА СПРОВОЂЕЊЕ ЗАКОНА

Средства за извршење закона у 2024. години планирана су у складу са Законом о буџету Републике Србије за 2024. годину, на Разделу 38 – Министарство информисања и телекомуникација, Програм 0703 – Телекомуникација и информационо друштво, функција 460 - Комуникације, програмска активност 5005 – Изградња и унапређење капацитета МИТ, националног ЦЕРТ-а РС и ЦЕРТ-а републичких органа ради превенције и брзог реаговања на инциденте у области информационе безбедности, економска класификација 512 – Машине и опрема, у износу од 50.000.000 динара. Са истих буџетских позиција пројектују се и износи у 2025. години (50.000.000 динара) и 2026. години (50.000.000 динара).