И З В Е Ш Т А Ј
О СПРОВЕДЕНОЈ ЈАВНОЈ РАСПРАВИ О НАЦРТУ ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Предлагач: Министарство информисања и телекомуникација

На основу члана 41. став 3. Пословника Владе („Службени гласник РС”, бр. 61/06 – пречишћен текст, 69/08, 88/09, 33/10, 69/10, 20/11, 37/11, 30/13, 76/14 и 8/19 – др. пропис), на предлог Министарства информисања и телекомуникација, Одбор за привреду и финансије Владе донео је Закључак 05 Број: 011-6721/2023 од 26. јула 2023. године, којим се одређује да спровођење јавне расправе у Републици Србији о Нацрту закона о информационој безбедности у периоду 27. јула до 30. августа 2023. године.

Програмом јавне расправе било је предвиђено да се Нацрт закона о информационој безбедности са пратећим материјалом објави на интернет страници Министарства информисања и телекомуникација www.mit.gov.rs и на Порталу „е-Консултације”, као и одржавање округлих столова у Београду дана 18. августа 2023. године у просторијама општине Стари град са почетком у 10 часова и у Крагујевцу дана 21. августа 2023. године у просторијама eKG InfoData doo са почетком у 11 часова, у организацији Министарства информисања и телекомуникација.

Први округли сто је одржан 18.08.2023 у Свечана сала Градске општине Стари град на адреси Македонска 42 и њему су присуствовали представници следећих организација: ЦЕТИН, БИА, Службени гласник, Друштво за информатику, А1, Канцеларија за информационе технологије и електронску управу, УНА ТВ, Вечерње новости, Министарство спољних послова, Женевског центра за управљање безбедносним сектором, ГО Чукарица, eGovernance Academy, Фондација Мрежа за сајбер безбедност, РАТЕЛ, Share фондација, ГО Савски венац, Expertise France, Addiko банка, Удружење банака Србије, Миленијум осигурање, ГО Палилула, НАЛЕД, Танјуг, УНДП и неколико грађана.

Други округли сто је одржан 21.08.2023 у Конференцијска сала eKG InfoData доо на адреси Краља Петра I 16, IV спрат. и њему су присуствовали представници следећих организација: ЈП Пошта Србије, Data Cloud Technology доо, Општинска управа Рача, Општинска управа Ћуприја, Правни факултет у Крагујевцу, ЈП Шумадија Крагујевац, e-KG Info Data, ЈКП Водовод и канализација Крагујевац, РАТЕЛ, Војска Србије, Општинска управа Лапово, Центар за безбедност, истраге и одбрану ДБА, Телеком Србија, ЈКП Шумадија, Бизнис иновациони центар, НАЛЕД, Градска управа Ниш, Државни дата центар, Средња стручна школа Крагујевац.

У току јавне расправе, прикупљени су иницијативе, коментари и сугестије од 17 подносилаца који су сви достављени у електронској форми на адресу електронске поште nevena.antonijevic@mit.gov.rs. Није пристигао ни један коментар на порталу е-Консултације, као ни поштом на адресу Министарства информисања и телекомуникација. Коментари су се односили на текст Нацрта у целини и поједини су били опште природе у вези са будућом применом закона, док су поједини били предлози за конкретне измене законског текста. Све сугестије које су испуњавале услове који се односе на усклађивање прописа са релевантним прописима ЕУ, унапређење законодавног и институционалног

оквира, уклањање неких недостатака постојећег прописа на основу искустава у вези са применом у пракси, представљају законску материју и представљају материју регулисања овог закона, као и који су формулисани тако да на други начин доприносе унапређењу квалитета законског текста су прихваћене и уграђене у текст закона који ће бити упућен у процедуру усвајања. Коментари и сугестије који нису прихваћени нису прихваћени из једног од следећих разлога: превише су опште формулисани и не могу да буду предмет законског регулисања, нису законодавна материја, нису материја регулисања овог закона, нису јасно формулисани да се разуме интенција предлагача, нису у складу са одредбама прописа ЕУ с којим се Нацрт закона о информационој безбедности усклађује, нису у складу са другим општим прописима и предлажу измене које одступају од Јединствених методолошких правила за израду прописа.

У наставку се налази Преглед коментара и сугестија на Нацрт закона о информационој безбедности достављених у току јавне расправе, уз назнаку да ли је коментар или сугестија прихваћен у целини или делимично или није прихваћен, као и разлоге зашто је делимично прихваћен или није прихваћен. У прилогу Извештаја налазе се и записници са одржаних округлих столова у Београду и Крагујевцу.

Преглед примљених иницијатива, коментара и сугестија на Нацрт закона о информационој безбедности

Део или делови материјала на које се коментар односи	Учесник или група учесника који упућује коментар	Примљени коментар	Одговор предлагача и образложење
Члан 1	НИС ад Нови Сад	У члану 1. Нацрта закона речи: „мере заштите од безбедносних ризика“, заменити речима: „мере заштите из области информационе безбедности“.	НИЈЕ ПРИХВАЋЕН Предлагач ће задржати постојећу одредницу имајући у виду да је у духу терминологије која се користи у каснијим члановима Нацрта где се предметне мере утврђују и да је више у складу са терминологијом из члана 1. став 2(б) НИС2 директиве.
	Национална алијанса за локални економски развој (НАЛЕД)	Члан 1. – уместо „општег нивоа“ безбедности требало би да стоји „високог нивоа опште безбедности.“ Уколико то није намера законодавца, потребно је прецизирати нивое безбедности.	НИЈЕ ПРИХВАЋЕН Предлагач ће задржати термин „високог општег нивоа информационе безбедности“ јер сматрамо да јасније указује на то да је реч о општем нивоу информационе

			безбедности, а не свеукупне безбедности, имајући у виду да је само информациона безбедност предмет уређивања овог закона, а унапређењем општег нивоа информационе безбедности унапређује се и ниво опште безбедности у земљи.
		Такође, имајући у виду шта све Нацрт закона уређује, предлажемо алтернативну формулацију: „Овим законом се уређују начела информационе безбедности Републике Србије; организација система за управљање информационом безбедношћу Републике Србије; надлежности и одговорности субјеката у систему за управљање информационом безбедношћу Републике Србије; мере заштите информационе безбедности Републике Србије од безбедносних ризика у информационо-комуникационим системима субјеката система за управљање информационом безбедношћу Републике Србије; као и организација, надлежности и одговорности субјеката за надзор над спровођењем овог закона“.	ДЕЛИМИЧНО ПРИХВАЋЕН Оцена је да је предлог сличан у основи постојећој одредби Нацрта, да у неким сегментима не одговара у потпуности самој садржини закона. Прихваћена је сугестија да се у уводној одредби укаже и на област надзора над применом закона.
Члан 2	Америчка привредна комора у Србији (AmCham)	Ускладити дефиницију „информационе безбедности“ из става 1, тачка 3, са Уредбом ЕУ 2019/881 , тако да гласи:	НИЈЕ ПРИХВАЋЕН Дефиниција информационе безбедности садржана у Нацрту закона је производ опсежне дебате

		„Информациона безбедност означава скуп активности и мера неопходних за заштиту информационо-комуникационих система, корисника таквих система и других лица погођених претњама са интернета;….. “	у оквиру Радне групе и решење које је прихватљиво за све надлежне органе имајући у виду да су постојали различити опречни ставови. Овај предлог је заправо дефиниција сајбер безбедности из ЕУ Акта о сајбер безбедности. Због још неуврежене прихваћености термина и неуједначеног разумевања сајбер безбедности међу субјектима овог закона, определили смо се да задржимо постојећи термин информациона безбедност и унапредимо дефиницију по узору на термин безбедност мрежа и информационих система из чл. 6 ст. 1(2) НИС2 директиве
		План одговора на инциденте је од кључне је важности како би надлежна лица тачно знала шта треба да предузму у циљу спречавања штете, те га је потребно експлицитно дефинисати чланом 2: „План одговора на инциденте је документација стандардног, унапред одређеног скупа упутстава или процедура за откривање, реаговање и задржавање злонамерних напада на информационо-комуникационе системе.“	НИЈЕ ПРИХВАЋЕН Имајући у виду да смо се када је реч о дефиницијама руководили НИС2 директивом, а да ово није дефиниција која се налази у члану 6 овог прописа, сматрамо да није потребно ни да је уносимо у Нацрт закона. Што се тиче саме садржине плана одговора, сматрамо да је одредбама које се односе на обавезу израде акта о безбедности и акта о процени ризика ова обавеза већ успостављена овим законом.

		Чланом 2. дефинисати значајну угроженост безбедности ИКТ система од посебног значаја, имајући у виду да се помиње у члану 7, став 1, тачка 7.	НИЈЕ ПРИХВАЋЕН Предлагач сматра да нема потребе за дефинисањем значајне угрожености јер то није појам који има неко посебно значење за потребе овог закона већ правни стандард.
		Размотрити регулисање унутрашње претње која долази од корисника који имају легитиман приступ информационо-комуникационим системима.	НИЈЕ ПРИХВАЋЕН Предлагач сматра да постојећа дефиниција претње обухвата и претњу описану у овом предлогу.
	Национална алијанса за локални економски развој (НАЛЕД)	Члан 2. став 1. - Потребно је прецизирати да се сви термини који се односе на лица и особе, а који су употребљени у мушком граматичком облику односе и на женска лица.	ПРИХВАЋЕН
		Члан 2. тачка 3) - дефиниција информационе безбедности није комплетна јер недостаје непорецивост извршилаца. Предлог алтернативне дефиниције: „информациона безбедност представља скуп мера заштите поверљивости, интегритета и расположивости информација у ИКТ систему, као и аутентичности извршилаца и непорецивости њихових радњи, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.“	ПРИХВАЋЕН
		Члан 2. тачка 4) - Предлог да се брише тачка која се односи на тајност података.	ПРИХВАЋЕН Тајност података је довољан за разумевање

		Термин „тајност“ из тачке 4) се преклапа са термином „поверљивост“ из тачке 8) и са термином „тајни податак“ из тачке 21). Сматрамо да тачка 8) и тачка 21) правилно дефинишу појмове поверљивост, односно тајне податке, те је неопходно обрисати тачку 4). Потребно је проверити даље кроз Нацрт закона да ли су правилно коришћена ова два термина.	дела законског текста на који се овај термин односи.
		Члан 2. тачка 16) - Дефиниција инцидента тренутно није довољно прецизна, те може резултирати недоумицама приликом извештавања о инцидентима у зависности од тумачења „догађаја који угрожава“. Предлог је да се фокус стави на последицу, а то је стваран негативан утицај на исправно функционисање система и на његову намену. Самим тим долази до већег нарушавања информационе безбедности, што је скраћени опис нарушавања поверљивости, интегритета и расположивости информација у ИКТ систему, као и аутентичности извршилаца и непорецивости њихових радњи.	НИЈЕ ПРИХВАЋЕН Дефиниција садржана у Нацрту је превод дефиниције инцидента из НИС2 директиве. Због обавезе да се закон усклади са овим прописом у највишој могућој мери, а имајући у виду да су и остале одредбе у вези са транспозицијом овог прописа, предлагач даје предност дефиницијама садржаним у овом ЕУ пропису у односу на све остале дефиниције у оптицају. Такође, инцидентом се сматра и ситуација која можда и није имала последицу јер је последица нпр. благовремено спречена, тако да суштински инцидент заиста подразумева догађај који угрожава ИКТ систем, а не само оне догађаје који су произвели штетне последице. Термин непорецивост је додат у дефиницију јер је реч о омашци.

		Члан 2. тачка 26) – Веома је важно дати значење скраћенице ЦЕРТ. Неусклађена је са касније коришћеним појмом „Центар за превенцију безбедносних ризика“. Потребно је да буде усаглашен и назив и делатност центара. Суштински њихов посао јесте превенција и заштита од инцидената а не од ризика. Прихватљиво је да буде и синергија појмова: нпр. Центар за превенцију безбедносних ризика и реаговање на инциденте.	ПРИХВАЋЕН Додат је пун назив ЦЕРТ-а у дефиницију ЦЕРТ-а.
		Члан 2. тачка 32) - Предлажемо да дефиниција безбедносне зоне обухвати зоне чије би нарушавање физичке безбедности изузетно лоше утицало на очување информационе безбедности ИКТ система (на пример дата центри или витална критична инфраструктура), у складу са ISO 27001 контрола A11.1 Безбедне области. Безбедносна зона није само функција чувања тајних података.	У ОБРАДИ У оквиру процедуре усвајања, МИТ ће упутити коментар предлагачу дела текста Нацрта закона на који се овај термин односи ради разматрања.
	Удружење банака Србије	Члан 2. тачка 13) Избегнути инцидент: Инцидент у пракси означава догађај који се реализовао и има неку категоризацију по утицају или другом критеријуму. Реч избегнути уводи забуну да се ради о догађају где до инцидента није ни дошло што је по нашем мишљењу збуњујуће.	НИЈЕ ПРИХВАЋЕН Избегнути инцидент је дефиниција из чл. 6. ст, 1(5) НИС2 директиве. С обзиром на то да је обавеза Републике Србије да усклади Нацрт закона са овим прописом ЕУ, предлагач настоји да дефиниције задржи што ближим њиховом изворном облику кад год је то могуће.

		Предлог измене: „безбедносни догађај“.	
		Члан 2. тачка 15) Озбиљна претња По нашем мишљењу може изазвати различита тумачења и створити различите забуне приликом даље примене Закона, нарочито у домену извештавања. У дефиниције се такође спомињу и значајне негативне последице што може бити предмет сличних дилема. Предлог измене: Прецизније објаснити и дати јасне смернице за категоризацију претњи и инцидената.	НИЈЕ ПРИХВАЋЕН Озбиљна претња је дефиниција преузета из чл. 6 ст. 1(11) НИС2 директиве. С обзиром на то да је обавеза Републике Србије да усклади Нацрт закона са овим прописом ЕУ, предлагач настоји да дефиниције задржи што ближим њиховом изворном облику кад год је то могуће.
	Регулаторно тело за електронске комуникације и поштанске услуге (РАТЕЛ)	Члан 2. став 1.: тачка 11) изменити тако да гласи: „11) рањивост је слабост или недостатак у ИКТ производима или услугама који се могу искористити за претњу“;	ПРИХВАЋЕНО Предлог је више у духу НИС2 директиве од постојећег решења у Нацрту.
		Тачка 26) изменити тако да гласи: „26) ЦЕРТ је организациона јединица у оквиру органа или правног лица задужена за превенцију и заштиту од инцидената“; Предлажемо да ЦЕРТ, буде дефинисан као организациона јединица у оквиру органа (Национални ЦЕРТ, ЦЕРТ мреже еУправе, ЦЕРТ-ови самосталних оператора) или правног лица (Посебни ЦЕРТ-ови).	ПРИХВАЋЕНО

	Нафтна индустрија Србије (НИС)	У дефиницији појмова (члан 2. став 1. тачка (26)) као и у целом тексту нацрта закона потребно је скраћеницу ЦЕРТ, као и скраћенице ДНС и ИП написати латиницом. Образложење: С обзиром да је скраћеница CERT настала од Computer Emergency Response Team целисходно је коришћење латинице. Потребно је исто урадити и са скраћеницама у закону као што су ДНС и ИП и употребити скраћенице написане латиницом DNS и IP.	У ОБРАДИ Предлагач ће у процесу усвајања прописа консултовати Републички секретаријат за законодавство у смислу усклађености са Јединственим методолошким правилима за израду прописа и поступити у складу са упутствима.
		Предлаже се да се члан 2. став 1. тачка 1) подтачка (2) измени тако што ће се иза речи „врши“ брисати реч „аутоматска“. Сматрамо да би предложеном изменом дефиниција била потпунија. ИКТ систем је целина која обухвата и обраду података која није аутоматска.	НИЈЕ ПРИХВАЋЕН Дефиниција је преузета из члана 6. ст 1(1)(б) НИС2 директиве. Имајућу у виду да је реч аутоматска употребљена у контексту уређаја односно групе уређаја, сматрамо да је употреба ове речи на овом месту адекватна.
		Члан 2. став 1. тачка 6) потребно је изменити тако да гласи: „6) расположивост је својство којим се осигурава доступност и употребљивост ИНФОРМАЦИОНОГ ДОБРА на захтев овлашћеног субјекта или процеса онда када им је потребан;“ Дата је потпунија дефиниција с обзиром на то да термин расположивост не представља само расположивост ИКТ система, већ може да се односи и на расположивост	НИЈЕ ПРИХВАЋЕН С обзиром на дефиницију ИКТ система, сматрамо да је постојећа дефиниција довољна да обухвати и предложене појмове.

		информационог добра/ IT ресурса/IKT сервиса и сл.	
		Члан 2. став 1. тачка 33) потребно је изменити тако што ће се у истом дефинисати и појмови као што су ИКТ добро, ИКТ сервис, IT ресурс и сл. Сходно томе како је дефинисан појам информациона добра, рачунар, свич, рутер или било који други асет који има IP адресу не представљају информационо добро. Уколико исти не представљају информационо добро потребно је дефинисати и појмове ИКТ добро, ИКТ ресурс, IT ресурс, како би се олакшао рад лицима који спроводе овај закон, као и лицима који раде на овим пословима свакодневно и задужени су за спровођење мера заштите из области информационе безбедности, а у свакодневном раду.	У ОБРАДИ Министарство ће проследити коментар органу који је предложио део закона на који се односи ова дефиниција на разматрање током интерне процедуре усвајања прописа.
	Српске кабловске мреже (СББ)	Члан 2. став 1. тачка 27) компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података. Коментар: Да ли су у питању намерне или ненамерне електромагнетне емисије.	У ОБРАДИ Министарство ће проследити коментар органу који је предложио део закона на који се односи ова дефиниција на разматрање током интерне процедуре усвајања прописа.
		Члан 2. став 1. тачка 43) услуге рачунарства у	НИЈЕ ПРИХВАЋЕН

		клауду (енгл. „cloud computing service”) су дигиталне услуге које омогућавају управљање на захтев и широки даљински приступ надоградивом и еластичном скупу дељивих рачунарских ресурса, укључујући и ситуације када су такви ресурси распоређени на неколико локација; Коментар: Ако је „компјутер“ преведен као „рачунар“, онда и „cloud“ треба превести као „облак“, па би превод овог термина био „рачунарство у облаку“...	Радна група је разматрала да ли да се определи за израз у клауду или у облаку, и определила се за израз у клауду јер је оценила да је постао уобичајенији у правном промету, а и због усклађености са другим прописима где се овај термин користи.
	Друштво за информатику Србије	У члану 2. (значење појединих термина) треба још објаснити следеће термине и то: - акт о безбедности ИКТ система, - после тачке 26) увести појам Канцеларија за информациону безбедност, - вештачка интелигенција (АИ) и њен значај за информациону безбедност.	НИЈЕ ПРИХВАЋЕНО Акт о безбедности није термин с неким посебним значењем у смислу овог закона, већ једна од обавеза оператора ИКТ система од посебног значаја, због тога нема потребе да се утврђује његово значење као правног термина. Канцеларија за информациону безбедност такође није термин за потребе овог закона већ посебна организација која се овим законом оснива, те сматрамо да јој није место међу терминима. Вештачка интелигенција није предмет регулисања овог закона, сам термин вештачка интелигенција не користи се нигде у даљем тексту тако да сматрамо да нема потребе да се посебно

			одреди као термин за потребе овог закона.
	Савет страних инвеститора	Члан 2. став 1. тачка (3) податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања. Предлог: Уместо термина „податке“ треба користити „информациона добра“. То је прецизнија дефиниција у склопу овог закона, а подразумева и сирови појам.	НИЈЕ ПРИХВАЋЕНО Имајући у виду да Нацрт закона највише тежи што већем степену усклађености са прописом НИС2 ЕУ и да тај пропис у овом контексту користи термин подаци, предлагач се опредељује да задржи постојеће решење.
		Члан 2. став 1. тачка 4) тајност је својство које значи да податак није доступан неовлашћеним лицима. Предлог: Потребно је направити разлику између термина поверљивост и тајност у смислу Закона о тајности података. Зато смо и претходно предложили да се уместо тајност овде користи појам поверљивост, а да се за дефинисање појма тајност позовемо на Закон о тајности података. Предлог: поверљивост је својство којим се осигурава да су информације и функције ИКТ система доступне само овлашћеним лицима; Образложење: Усклађивање са дефиницијом 3.10 ISO 27000.	ПРИХВАЋЕНО Може да се уклони термин тајност, појам тајног податка је довољан за разумевање релевантних одредби закона. Што се тиче дефиниције поверљивости, она је изнета и током састанака Радне групе, и предлагач је прихватио ову сугестију и садржана је у тексту Нацрта закона.

		Члан 2. став 1. тачка 6) расположивост је својство којим се осигурава доступност и употребљивост ИКТ система на захтев овлашћеног субјекта или процеса онда када им је потребан; Предлог: расположивост је својство којим се осигурава доступност и употребљивост ИКТ система на захтев овлашћеног субјекта или процеса онда када им је потребан. Образложење: Усклађивање са дефиницијом 3.7 ISO 27000	ПРИХВАЋЕНО Предлог је изнет и током рада Радне групе и тада је прихваћен од стране предлагача и налази се у Нацрту закона.
		Члан 2. став 1. тачка 7) аутентичност је својство којим се осигурава могућност да се провери и потврди да је информацију створио или послао онај за кога се тврди да је ту радњу извршио; Предлог: аутентичност је својство којим се осигурава могућност да се провери и потврди да је информацију створио или послао онај за кога се тврди да је ту радњу извршио; Образложење: Усклађивање са дефиницијом 3.6 ISO 27000.	ПРИХВАЋЕН Предлог је изнет и током рада Радне групе и тада је прихваћен од стране предлагача и налази се у Нацрту закона.
		Члан 2. став 1. тачка 16) инцидент је сваки догађај који угрожава расположивост, аутентичност, интегритет или поверљивост података који се чувају, преносе или обрађују или услуге које се	НИЈЕ ПРИХВАЋЕН Дефиниција садржана у Нацрту је превод дефиниције инцидента из НИС2 директиве. Због обавезе да се закон усклади са овим прописом у највишој

		пружају, односно које су доступне путем ИКТ система; Инцидент је један или низ неочекиваних догађаја који имају стваран негативан утицај на исправно функционисање и намену ИКТ система, односно нарушавају информациону ИКТ система.	могућој мери, а имајући у виду да су и остале одредбе у вези са транспозицијом овог прописа, предлагач даје предност дефиницијама садржаним у овом ЕУ пропису у односу на све остале дефиниције у оптицају. Такође, инцидентом се сматра и ситуација која можда и није имала последицу јер је последица нпр. благовремено спречена, тако да суштински инцидент заиста подразумева догађај који угрожава ИКТ систем, а не само оне догађаје који су произвели штетне последице.
		Члан 2. став 1. тачка 32) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци Предлог: Предлажемо да дефиниција безбедносне зоне обухвати зоне чије би нарушавање физичке безбедности изузетно лоше утицало на очување информационе безбедности ИКТ система (на пример Data centri или витална критична инфраструктура). Образложење: ISO 27001 контрола A11.1 Безбедне области. Погрешно је свести безбедносну зону само на функцију чувања тајних података.	У ОБРАДИ У оквиру процедуре усвајања, МИТ ће упутити коментар предлагачу дела текста Нацрта закона на који се овај термин односи ради разматрања.
Члан 3	Савет страних инвеститора	Члан 3. Наслов: Начела	ПРИХВАЋЕН

		Предлог допуне: Начела информационе безбедности	
	НАЛЕД	Након члана 2 предлажемо одвајање целине тако да гласи „ДЕО II НАЧЕЛА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ“	ДЕЛИМИЧНО ПРИХВАЋЕН Коригован је наслов члана, али оцењено је да нема потребе да се он налази у засебном делу истог назива.
	Друштво за информатику Србије	Члан 3. Предлог: Требало би додати тачку 5) Начело примерености субјеката надзора: Појединачна лица која се законски прате каналима комуникације, не угрожавајући права осталих лица која имају права на своју приватност;	НИЈЕ ПРИХВАЋЕН Рад инспекцијских органа уређен је општим прописом и одредбе се примењују и на инспекцију успостављену овим законом.
	Слободан Максимов	Члан 3. Не наводи или не позива на јасније дефиниције ризика што може довести до слободног тумачења истих од стране оператора, иако је у члану 21. наведено да се исти прописују радом Канцеларије, али за члан 9.	НИЈЕ ПРИХВАЋЕН Појам ризика дефинисан је у члану 2. Нацрта закона у складу са дефиницијом из НИС2 директиве.
Члан 4	Друштво за информатику Србије	Члан 4. Додати: Начела транспарентности рада свих учесника у процесу обезбеђивања безбедности информационог система, а сагласно потреби да се обезбеди склад између доступности информација и неширења штетних информација.	НИЈЕ ПРИХВАЋЕН Оцењено је да је реч о општем начелу које се односи на рад државних органа и организација и да нема потребе да се посебно наглашава овим законом.
	Саша Милашиновић	Члан 4. треба бити регулисан подзаконским актом а не Законом. Поставио је питање: - Да ли је потребно дефинисати у овом Закону	НИЈЕ ПРИХВАЋЕН Обрада података о личности мора бити регулисана законом у складу са чланом 13. Закона о заштити података о личности.

		и да ли је то у складу са истим?	
Члан 5	Национална алијанса за локални економски развој (НАЛЕД)	Члан 5. тачка 4. – Предлаже се брисање тачке где се реферише на дефиниције из старог закона, будући да је овим чланом већ опредељена категорија оператора приоритетних ИКТ система од посебног значаја.	ПРИХВАЋЕН
	Службени гласник	Чланом 5. Нацрта дефинисани су оператори приоритетних ИКТ система од посебног значаја као „системи 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“. У Образложењу нацрта, у одељку III. ОБЈАШЊЕЊЕ ПОЈЕДИНИХ РЕШЕЊА, код члана 5. наведено је да су оператери приоритетних ИКТ система од посебног значаја 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 нуклеарним објектима, пружање услуга од поверења, пружање услуга ДНС, делатност	ПРИХВАЋЕН

		електронских комуникација, тачка за размену интернет саобраћаја, и она делатност где постоји само један пружалац услуге. Предлог: У члану 5. Нацрта, у став 2. тачка 9) Закона додаје се алинеја шеста која гласи: „- издавање Службеног гласника Републике Србије и вођење Правно-информационог система Републике Србије“. Образложење: Будући да је објављивање закона и општих аката Републике Србије неопходан предуслов за ступање општег акта на снагу, прекид или поремећај у обављању делатности објављивања службеног гласила Републике Србије имао би кључан утицај на несметано функционисање свих система у Републици Србији, јер би била доведена у питање интеграција општих аката у правни систем Републике Србије и тиме њихова примена, посебно имајући у виду неретке ситуације када због разлога хитности прописи ступају на снагу даном објављивања или наредног дана од дана објављивања у „Службеном гласнику Републике Србије“. Такође, у складу са Законом о објављивању закона и других прописа и општих аката, ЈП	

		„Службени гласник“ једини је пружалац услуге издавања службеног гласила Републике Србије, као и вођења Правно-информационог система Републике Србије, у оквиру кога се објављује електронски облик Службеног гласника у PDF формату, који је званично издање. Због наведеног, а имајући у виду да су испуњене основне претпоставке за идентификовање система као приоритетног ИКТ система од посебног значаја (делатност од кључног значаја у којој постоји само један пружалац услуге), предлажемо да се, уместо у члану 6. Нацрта, делатност издавања службеног гласила Републике Србије, предвиди у члану 5, као и да њоме буде обухваћено и вођење Правно-информационог система Републике Србије, у циљу усклађивања решења са Законом о објављивању закона и других прописа и општих аката.	
	Слободан Максимов	Члан 5. Пропуштено је да се макар у делу Саобраћај дода и део везан за Комуникациону мрежу, већ се само штуро у делу "Дигитална инфраструктура" наводи клауд и дата центар без кључне ствари а то је мрежа.	НИЈЕ ПРИХВАЋЕН Одређивање оператора ИКТ система од посебног значаја је у потпуности усклађено са НИС2 директивом. За додатно прецизирање, предвиђено је доношење подзаконског акта у члану 6. Нацрта.
	Друштво за информатику Србије	Члан 5. Закона о ИБ, где у 2. ставу тачка 1 треба додати линију:	НИЈЕ ПРИХВАЋЕН Ова делатност није у НИС2 директиви

		- производња, дистрибуција и снабдевање енергијом из обновљивих извора енергије (соларна, енергија ветра, геотермална, биомаса, биогас, хидроенергија и др.);	препозната као делатност оператора приоритетних ИКТ система од посебног значаја. Како настојимо да постигнемо режим успостављен НИС2 директивом, определили смо се за овакво решење.
		Члан 5. Закона о ИБ, где у 2. ставу тачка 3 треба додати: 3 Образовање - омогућити установама образовања чији је оснивач Република Србија несметан рад и коришћење најсавременије инфраструктуре, - управљање ИКТ инфраструктуром Министарства просвете, Завода за вредновање квалитета образовања и васпитања, Завода за унапређивање образовања и васпитања и Акредитационе комисије за високо образовање, - послови вођења ЈОБ-а, електронског дневника, сервиса ЈИСП и др. - електронских сервиса који служе да омогуће вођење евиденције образовања у Републици Србији, - истраживачка делатност и научно-технолошки паркови, - фундаментална, основна и технолошка истраживања, реализована на научним институтима у Србији, - репозиторијум докторских дисертација,	НИЈЕ ПРИХВАЋЕН Ни једна од ових делатности није на овај начин препозната као делатност оператора ИКТ система од посебног значаја у НИС2 директиви. Имајући у виду да НИС2 директива поставља прилично широк обухват обвезника закона, предлагач се определио да се придржава овог приступа без додатног ширења круга обвезника, посебно не у условима институционалне реформе и развоја институционалних капацитета за спровођење закона.

		базе података из различитих поља науке и уметности, - обезбеђивање квалитета прикупљених научних радова, патената и пројеката са института, као и из САНУ-а,...	
Члан 6	А1	Предлог: У вези са члановима 5. и 6. Нацрта Закона којима се уређују оператори приоритетних и важних ИКТ система од посебног значаја, предлажемо да се у правни основ за доношење подзаконског акта из члана 6. став којим Влада, на предлог министарства надлежног за послове информационе безбедности, ближе уређује услове, опште и секторске критеријуме и подсекторске прагове за одређивање оператора из чл. 5. и 6. овог закона, као и процедуру идентификовања и одређивања оператора ИКТ система од посебног значаја, допуни тако да се пропише да овај подзаконски акт садржи и шифре делатности под које потпадају оператори приоритетних и важних ИКТ система од посебног значаја. Образложење: Наведена допуна члана се предлаже у циљу ближег дефинисања делатности које обављају оператори ИКТ система од посебног значаја и отклањања недоумица у примени Закона у погледу тумачења да ли неки правни субјект	У ОБРАДИ Предлог ће бити размотрен током процедуралне консултације са надлежним министарствима.

		обавља делатност због које се сматра оператором система од посебног значаја или не.	
	Службени гласник	У члану 6. став 1. тачка 1) алинеја 11. Нацрта, као делатност коју обављају оператори важних ИКТ система од посебног значаја наведено је издавање службеног гласила Републике Србије. Предлог: У члану 6. став 1. тачка 1) алинеја 11. брише се.	ПРИХВАЋЕН
Члан 7	Нафтна индустрија Србије (НИС)	Предлаже се да се у члану 7. став 1. тачка 6) изврши допуна на тај начин што ће се прописати да свако ко пружа услугу Оператору ИКТ система од посебног значаја дужан да поштује закон, прати и примењује најбољу праксу и др. Према нацрту закона оператор ИКТ система је у обавези да уреди однос са трећим лицима. Размотрити опцију да је свако ко пружа услугу Оператору ИКТ система од посебног значаја дужан да поштује закон, прати и примењује најбољу праксу и др.	НИЈЕ ПРИХВАЋЕН Свако је дужан да поштује прописе који важе на територији Републике Србије. Закон о информационој безбедности препознаје оне операторе које обављају делатности које уколико би биле угрожене сајбер нападом то би отежало функционисање критичних друштвених и економских активности и ови оператори имају обавезу поступања у складу са законом и подлежу надзору у складу са законом и санкционисању у складу са прекршајним одредбама. Остали субјекти могу да се придржавају прописаних мера, слободни су да примењују и строже мере, али они нису обвезници закона, не подлежу надзору и казненом режиму. Сваки обвезник Закона има слободу да у оквиру

			својих уговорних односа са трећим лицима који нису обвезници овог Закона тражи испуњење мера заштите утврђених Законом.
	Српске кабловске мреже (СББ)	Члан 7. став 1. тачка 7) – доставља обавештења, без одлагања, о сваком инциденту који је значајно угрозио безбедност ИКТ систем од посебног значаја. Коментар: део који гласи „значајно угрозио“ потребно је дефинисати шта он представља.	НИЈЕ ПРИХВАЋЕН Реч је о правном стандарду који мора да има у себи дозу флексибилности како би могао да се примени на различите системе.
		Члан 7. став 1. тачка 8) доставља обавештења о озбиљним претњама за ИКТ систем од посебног значаја Коментар: Шта се све подразумева под термином „озбиљне претње“ потребно је дефинисати.	НИЈЕ ПРИХВАЋЕН Термин озбиљна претња дефинисан је у члану 2 Нацрта закона.
	Интернет клуб	Ако сматрате да је оваква допуна сврсисходна, предлажемо да се појави као ставка 10) у Члан у7: Члан 7 10) „обезбеди основни ниво обуке из области безбедности информационих система за све запослене који имају приступ ИКТ систему“. Образложење допуне: Ову допуну предлажемо зато што се значајан број сигурносних продора у заштићене ИКТ системе догодио због неодговарајућих потеза запослених који нису имали ни основна знања из области безбедности	ДЕЛИМИЧНО ПРИХВАЋЕН Део који се односи на обезбеђивање обука је прихваћен и унет у Нацрт текста, с тим да напомињемо да је реч о мери која је већ била обухваћена у члану 10. став 1. тачка 4) Нацрта закона. Ради јасноће, наведена тачка је допуњена. Предлог који се односи на захтеве везане за сертификацију није прихваћен. Предлагач сматра да још ниво информационе безбедности и капацитети оператора да улажу у информациону

		информационих система. Предложена допуна није у супротности са НИС 2 регулативом, у којој се у Члану 21 став 2г) од оператора тражи да предузме одређене активности и који у оригиналу гласи: „basic cyber hygiene practices and cybersecurity training“ Предлажемо да се у Члану 7 дода и ставка 11), која би од оператора тражила да преиспита своје кључне добављача у контексту квалификоване оспособљености за безбедно управљање информационим системом.	безбедност још увек нису на довољном нивоу да се прописује обавезна сертификације као законска обавеза. Напомињемо да је предвиђено да Канцеларија за информациону безбедност има надлежности да припреми и развија оквир и шеме сертификације у области сајбер безбедности и да, када се за то створе услови превасходно у ЕУ, предузме конкретне кораке да заједно са другим надлежним органима приступи реализацији ове још увек нове области у развоју. У овом тренутку је преурањено прописивање овакве обавезе јер је неопходно утврдити тачно који ИКТ производи, услуге и процеси се сертификују, на који начин, у складу са којим шемама и стандардима (националним, европским, међународним), у ком поступку, од стране којих акредитованих тела, како акредитовати тела, како поступити уколико таква тела која би могла да се акредитују не постоје на територији Републике Србије, испитати колико таквих тела постоји у иностранству и друго. Сертификација у области

			сајбер безбедности је у повоју у Европској унији и предлагач је става да је за сада могуће једино идентификовати надлежност институције за праћење и развој ове области јер би прописивање конкретне обавезе остало de facto непримењиво јер су изузетно оскудни примери добре праксе у овом подухвату. Наравно, у оквиру својих уговорних аранжмана са трећим лицима сваки оператор може да захтева и одређене доказе о испуњености услова по питању сајбер безбедности што је гарантовано слободом уговарања, а и пожељно из угла доприноса подизању нивоа свеукупне сајбер безбедности у земљи. У складу са НИС2, за сада оператори ИКТ система од посебног значаја имају обавезу да уреде 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 са трећим лицима. Такође, и пружаоци управљаних услуга и управљаних безбедносних услуга препознати су као оператори ИКТ система од посебног значаја по

			новом предложеном законском решењу, што их чини обвезницима закона независно од њихових уговорних обавеза.
	Саша Милашиновић	Члан 7. Обавезе оператора ИКТ система од посебног значаја врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система и то најмање два пута годишње Потребно је преиспитивати и ризике, заједно са усклађености мера заштите. Довољно је преиспитивати „минимум једном годишње“.	НИЈЕ ПРИХВАЋЕН У поступку консултација за припрему за израду Нацрта закона, представници оператора ИКТ система од посебног значаја изјаснили су се да је у савременим условима и два пута годишње превазиђено, да се те провере морају вршити и чешће, али због великих финансијских, кадровских и организационих разлика између оператора који потпадају под исту категорију определили смо се за овај минимум за који је оцењено да сви могу да обезбеде капацитете да га спроведу. Свака додатна провера мимо законског минимума је пожељна.
Члан 9	Српске кабловске мреже (СББ)	Члан 9. став 1. тачка 7) веб страница оператора ИКТ система од посебног значаја; Коментар: Шта ако оператор ИКТ система има више веб страница – која се сматра главном и коју је потребно пријавити¬? Оператори ИКТ система обично имају једну пословну страницу која је обично веб презентација, а кроз друге веб странице пружају услуге, које су евентуално још ризичније	НИЈЕ ПРИХВАЋЕН Податак који се тражи већ се тражи на основу Правилника о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја(Сл. гласник РС бр. 9/2020) Предлагач је одлучио да сада све податке који се уносе у евиденцију пропише законом јер се то сматра исправнијим и прегледнијим решењем.

		од основне веб странице на којој је само презентација предузећа. потребно је да регулатор дефинише о којој страници жели да добије податке (са аспекта безбедности пре оне кроз које се пуштају сервиси).	Повереник за заштиту података о личности је сугерисао у оквиру Радне групе да је правилан приступ да се подаци који се прикупљају ипак пропишу у закону, а не у подзаконском акту и предлагач је поступио у складу са том сугестијом. До сада у пракси нисмо имали ни један упит у вези са тумачењем одредбе члана 2 поменутог Правилника којим се обавеза достављања ове информације прописује, у том смислу немамо посебну забринутост да ће то убудуће стварати нејасноће, али свакако се једноставним језичким тумачењем може закључити да је то једна или више страница без обзира на то да ли је она презентација или има и друге функционалности. У сваком случају предвиђено је доношење подзаконског акта који ће питање евиденције уредити до детаља и ова сугестија ће у том смислу бити узета у обзир
	А1	Упис у регистар оператора ИКТ система од посебног значаја Предлог: У вези са чланом 9. Нацрта Закона који уређује садржај Евиденције оператора ИКТ система од посебног значаја, имајући у виду да ће у складу са ставом 1.	ПРИХВАЋЕН

		тачка 6) прописано да наведена евиденција садржи „адресни опсег интернет протокола (енгл. „ip address range“) који припадају ИКТ систему од посебног значаја“ предлажемо да се ова одредба прецизира тако да се он односи на јавне статичке ИП адресе које користи оператор ИКТ система од посебног значаја. Образложење: Ова допуна се предлаже како би се ефикасније остварио циљ увођења ове одредбе, тј. да би у случају одређеног инцидента могло да се одреди да ли он потиче од система оператора ИКТ система од посебног значаја и да се може одмах приступити предузимању одговарајућих мера. Сматрамо да то није могуће урадити на ефикасан начин уколико се користе динамичке ИП адресе, нити ће бити могуће да оператори ИКТ система од посебног значаја који нису оператори електронских комуникација изврше пријаву адресних опсега интернет протокола, имајући у виду да се адресе мењају приликом коришћења динамичких ИП адреса.	
	SHARE фондација	Члан 9. Нацрта закона предвиђа да је Евиденција оператора ИКТ система од посебног значаја тајни податак у складу са законом којим се уређује	НИЈЕ ПРИХВАЋЕН Појединачни подаци садржани у евиденцији сами по себи нису тајни и сама евиденција представља збир

		тајност података, која се тако налази у режиму веома осетљивих података једне државе, где су са друге стране посебни услови за њихово приступање итд. У том смислу, можемо поставити питање да ли је оправдано да комплетна Евиденција буде тајна, уместо само конкретних техничких података о ИКТ системима од посебног значаја (нпр. опсези IP адреса) који се могу злоупотребити за њихову енумерацију и евентуалне техничке нападе.	појединачно јавно доступних података или података које њихов ималац може по сопственој вољи да учини доступним јавности и/или трећим лицима. Ипак, сматрамо да евиденција као целина представља скуп података који може да буде злоупотребљен на начин да угрози информациону безбедност како појединачних оператора и делатности, тако и свеукупну информациону безбедност у земљи. Такође, руковалац обраде података, имајући у виду да она садржи и податке о личности (администратор и одговорно лице), означавањем евиденције одговарајућим степеном тајности и гарантовањем њене рестриктивне доступности једино може да у потпуности обезбеди наменску употребу и чување садржаних података уз минимизацију ризика од злоупотребе. Напомињемо да је сврха поседовања евиденције извршење одредби овог закона у погледу достављања обавештења и упозорења значајних за безбедност ИКТ система од посебног значаја, као и ради успостављања комуникације надлежних државних органа и

			оператора ИКТ система од посебног значаја и остваривања сарадње у циљу отклањања штетних последица инцидената и превентивног деловања. Тако да информације садржане у њој практичан значај имају само органима надлежним за спровођење закона и за друге сврхе се прикупљени подаци не могу користити. Изложеност садржине или дела садржине евиденције јавности са собом носи одређену рањивост и појачану изложеност сајбер претњама и инцидентима, као и другим злонамерним радњама, а потреба да се спрече злоупотребе у конкретном случају, према оцени предлагача, претеже над интересом јавности у погледу ових информација који је, с обзиром на њихову природу, заиста минималан. Некакво делимично објављивање евиденције је технички прилично компликовано због природе ових података и њихове динамичности и немогућности да се правилно оцени до које мере би такво објављивање могло да буде злоупотребљено. Наравно, појединачне информације из

			евиденције које представљају информације од јавног значаја достављају се у складу са законом који уређује ову област. Такође, према сазнањима предлагача, свака држава ЕУ са којом је предлагач до сада сарађивао у оквиру међународне сарадње, овакве евиденције држи под одређеним степеном тајности у складу са националним законодавством из горенаведених разлога. Такође, консултанти (Савет Европе и Женевски центар за управљање безбедносним сектором) који су ангажовани за потребе оцене усклађености Нацрта закона са прописима ЕУ препоручили су да задржимо постојеће решење јер је ризик од злоупотребе оваквог скупа података претежући у односу на било који други легитиман јавни интерес.
	Америчка привредна комора у Србији (AmCham)	Члан 9. У ставу 1. тачка 7. потребно је прецизирати на коју веб страницу оператора ИКТ система од посебног значаја се мисли, тј. дефинисати да се односи на веб страницу преко које се пружају услуге. Наиме, обично оператори ИКТ система имају једну пословну страницу, која је	НИЈЕ ПРИХВАЋЕН Податак који се тражи већ се тражи на основу Правилника о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја(Сл. гласник РС бр. 9/2020) Предлагач је одлучио да сада све податке који се уносе у евиденцију

		обична веб презентација правног лица, а кроз друге веб странице пружају услуге, које су потенцијално још ризичније од основне веб странице.	пропише законом јер се то сматра исправнијим и прегледнијим решењем. Повереник за заштиту података о личности је сугерисао у оквиру Радне групе да је правилан приступ да се подаци који се прикупљају ипак пропишу у закону, а не у подзаконском акту и предлагач је поступио у складу са том сугестијом. До сада у пракси нисмо имали ни један упит у вези са тумачењем одредбе члана 2 поменутог Правилника којим се обавеза достављања ове информације прописује, у том смислу немамо посебну забринутост да ће то убудуће стварати нејасноће, али свакако се једноставним језичким тумачењем може закључити да је то једна или више страница без обзира на то да ли је она презентација или има и друге функционалности. У сваком случају предвиђено је доношење подзаконског акта који ће питање евиденције уредити до детаља и ова сугестија ће у том смислу бити узета у обзир.
Члан 10	Америчка привредна комора у Србији (AmCham)	Члан 10. Потребно је чланом 10. прописати и мере санације последица инцидената.	ПРИХВАЋЕН

	Спрске кабловске мреже (СББ)	Члан 10. став 2. Мерама заштите ИКТ система осе обезбеђује превенција од настанка инцидента, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Коментар: Шта је са мерама за детекцију и мерама за опоравак информационог система након инцидента? Да ли оне нису потребне да се имплементирају? Мере/контроле се деле на: превентивне (покривено) / детективне (није покривено) и корективне (није покривено) потребно је предвидети.	НИЈЕ ПРИХВАЋЕН У члану 10 превасходно су предвиђене мере које уколико се примењују може се сматрати да је ИКТ систем безбедан, односно мере које су по својој природи превентивне. Закон као целина успоставља низ обавеза оператора ИКТ система, као и надлежних органа које су усмерене и на детекцију и на отклањање штетних последица. Предвиђено је доношење подзаконског акта којим се ближе уређују мере заштите, као и подзаконског акта који ближе уређује садржину акта о безбедности, и методологије за израду акта о процени ризика, где би предлог да се изврши оваква класификација мера могао бити узет у разматрање.
	Савет страних инвеститора	Члан 10. Мере заштите ИКТ система од посебног значаја Предлог допуне наслова: Мере заштите информационе безбедности Републике Србије	НИЈЕ ПРИХВАЋЕН Ово нису мере заштите информационе безбедности Републике Србије, већ мере заштите које је оператор ИКТ система од посебног значаја дужан да предузме као обвезник закона, због чега подлеже инспекцијском надзору и казненом режиму.
	Национална алијанса за локални економски	Пре члана 10. потребно је уметнути посебан одељак који гласи Мере заштите информационе безбедности Републике Србије.	НИЈЕ ПРИХВАЋЕН Ово нису мере заштите информационе безбедности Републике Србије, већ мере заштите

	развој (НАЛЕД)		које је оператор ИКТ система од посебног значаја дужан да предузме као обвезник закона, због чега подлеже инспекцијском надзору и казненом режиму.
	Нафтна индустрија Србије (НИС)	Чланом 10. став 3. тачка 18) прописано је: „18) праћење мрежних система у циљу откривања рањивости и претњи“ У наведеној одредби користи се термин мрежни систем који није дефинисан и није најјасније на шта се тачно односи, што може произвести погрешно тумачење закона. Предлог је да се додатно дефинише. Члан 10. став 3. тачка 13) потребно је изменити тако да гласи: „13) спречавање неовлашћеног ОДЛИВА података;“ Како став 3. наведеног члана почиње са "Мере заштите ИКТ система се односе на:, препорука је да се измена изврши на начин да се "примена мера заштите ради" избрише. Енглески термин Data Leak Prevention/Data Loss Prevention преводи се са „заштита од одлива података“, стога би део у тачки 13) био јаснији уколико се измени на начин да се реч прикупљања замени са речју "одлива". На овај начин ближе би се прецизирало значење ове одредбе.	ДЕЛИМИЧНО ПРИХВАЋЕНО Прихваћена је сугестија делимично, с тим да је употребљен термин „отицање“ који се више користи у стручним круговима, а има исто значење.

		У члану 10. став 3. тачка 25) потребно је извршити појашњење. У наведеном члану прописано је да се мере заштите ИКТ система односе на „25) обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система ". Није јасно шта треба да се обезбеди, што може довести до двојаког тумачења.	НИЈЕ ПРИХВАЋЕН Сматрамо да је термин довољно прецизан и напомињемо да ће се ова мера заштите, као и остале, ближе разрадити подзаконским актом.
		У члану 10. став 3. тачка 31) потребно је појаснити/дефинисати шта су средства и шта је потребно да се чува од пружаоца услуга. У наведеном члану није дефинисано шта су средства, што може довести до погрешног тумачења (нпр. средства могу бити аутомобили, цистерне, столови, кациге, и др.) као и шта треба да се чува од пружаоца услуга.	НИЈЕ ПРИХВАЋЕН Одредба је непромењена од 2016. године је у примени. До сада нисмо примили ни једну примедбу ни од обвезника закона ни од надлежних органа да им ствара одређене нејасноће у примени.
Члан 11	Партнери Србија	Члан 11. Акт о процени ризика ИКТ система од посебног значаја – Потребно је допунити члан тако што ће се прописати рок у ком је оператор дужан да донесе предметни акт;	ПРИХВАЋЕН Рок за доношење акта додат у прелазне и завршне одредбе.
	Саша Милашиновић	Члан 11. Акт о процени ризика ИКТ система од посебног значаја израђује се у складу са општом методологијом за процену ризика у ИКТ системима од посебног значаја коју доноси	НИЈЕ ПРИХВАЋЕН Законом не прописујемо одабир конкретних стандарда из разлога што се мењају. Канцеларија као надлежни орган ће на основу своје стручне процене израдити

		Канцеларија за информациону безбедност. Прописати методологију у складу са ИСО 31000 или ИСО 27005 Акт из става 1. овог члана ревидира се најмање једном годишње. За све ИКТ системе (приоритетни и важни) довољно је једном годишње спроводити преиспитивање (ревизију).	методологију руководећи се релевантним изворима. На сугестију у вези са ревизијом акта је одговорено у ранијем истом коментару.
	Друштво за информатику Србије	Члан 11. допунити новим ставом: - Процена ризика ИКТ система од посебног значаја се врши у складу са ИСО 31000 или 27005.	НИЈЕ ПРИХВАЋЕН Законом не прописујемо обавезу у погледу конкретних стандарда јер се мењају.
	Удружење банака Србије	Члан 11. Закон захтева спровођење Процене ризика и доношење Акта о процени ризика, што је позитивна промена. Финансијске институције имају сложене и веома регулисане ИКТ системе нарочито у домену Управљања ризицима тако да се овим сегментом баве већ дужи низ година на врло високом нивоу (контрола НБС, банкарских групација и др.). Предлог измене: Размотрити увођење одредби у Закону које би постојеће процене ризика сматрала као валидан доказ о пракси Управљања ризицима и као доказ о усклађености са захтевима из Закона.	ПРИХВАЋЕН Прихваћено, с тим да је наведено да постојећи акти морају да обухватају захтеве из опште методологије коју доноси Канцеларија за информациону безбедност.
Члан 12	Саша Милашиновић	Члан 12. Акт о безбедности ИКТ система од посебног значаја	НИЈЕ ПРИХВАЋЕН

		Оператор важног ИКТ система од посебног значаја дужан је да, самостално или уз ангажовање спољних експерата, врши проверу из претходног става најмање једном годишње и да о томе сачини извештај. Коментар: За све ИКТ системе (приоритетни и важни) довољно је једном годишње спроводити преиспитивање (ревизију) и обавезно је за све да сачине извештај (документована информација, објективни доказ).	Одговорено је на ранији исти коментар истог подносиоца.
	Партнери Србија	Члан 12. Акт о безбедности ИКТ система од посебног значаја – Потребно је допунити члан тако што ће се прописати рок у ком је оператор дужан да донесе предметни акт.	ПРИХВАЋЕН Рок унет у прелазне и завршне одредбе.
Члан 13	Партнери Србија	Члан 13. Обавештавање о инцидентима – Потребно је допунити став 7. члана, тако што ће након: „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“ додати: „без одлагања, а најкасније у року од 24 сата од пријема обавештења о инциденту“. Потребно је допунити став 8. члана, тако што ће се након: „Ако је инцидент повезан са	ПРИХВАЋЕН

		значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање одбране или националне безбедности Републике Србије, орган коме је упућено обавештење о инциденту обавештава органе који су надлежни за послове одбране или националне безбедности“ додати: „без одлагања, а најкасније у року од 24 сата од пријема обавештења о инциденту“. Потребно је допунити став 9 члана, тако што ће се након: „Орган коме је у складу са овим законом упућено обавештење о инциденту, уколико је реч о ИКТ систему од посебног значаја који је одређен као критична инфраструктура, то обавештење прослеђује Министарству унутрашњих послова и министарствима надлежним за секторе критичне инфраструктуре у складу са законом који уређује критичну инфраструктуру“ додати: „без одлагања, а најкасније у року од 24 сата од пријема обавештења о инциденту“. Прописивањем предложених рокова обезбедиће се већа сигурност и оперативност приликом реаговања на инциденте, а овај пропис ће се додатно ускладити са директивама Европске уније.	
	Национална алијанса за локални	Члан 13. став 10. – Претходним законским решењем је било неопходно	НИЈЕ ПРИХВАЋЕН НИС2 директива користи израз који је најближи

	економски развој (НАЛЕД)	да се јавност информише о инцидентима а стручна лица о рањивостима. Могуће је да се уместо „саветовања“ предложи „усаглашавања“ јер подразумева и усаглашавање екстерне комуникације.	изразу саветовање па се предлагач определио да задржи ово решење.
	РАТЕЛ	У члану 13: став 2. додати и операторе ИКТ система из члана 6. став 1. тачка 1) алинеја прва тако гласи: „Изузетно од става 1. тачка 2) овог члана, оператори ИКТ система из чл. 5. став 2. тачка 1) подтачка (3) алинеја прва, друга пета 6 став 1. тачка 1) алинеја прва овог закона су дужни да обавештење о инциденту доставе Народној банци Србије, а оператори ИКТ система из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа обавештење о инциденту достављају регулаторном телу за електронске комуникације и поштанске услуге“. Предлог: је да и оператори поштанских услуга достављају обавештења о инциденту Регулатору, с обзиром да исто и обавља регулаторне послове у области електронских комуникација и поштанских услуга, као и да су оператори поштанских услуга дефинисани као оператори важних ИКТ система од посебног значаја који имају обавезу достављања обавештења о инцидентима	ПРИХВАЋЕН

		који могу да имају значајан утицај на нарушавање информационе безбедности, у складу са чланом 13. Нацрта закона.	
		став 3: изменити тако да гласи: „Народна банка Србије и Регулаторно тело за електронске комуникације и поштанске услуге обавештење из претходног става прослеђују у јединствени систем за пријем обавештења о инцидентима“. Предлог: преформулисати став 3. Нацрта закона јер смо мишљења да члан 13. не дефинише услове које обавештење о инциденту треба да испуни, те брисање предлажемо јер сматрамо да је целисходније да се сва обавештења која приме секторски ЦЕРТ-ови прослеђују Националном ЦЕРТ-у, који ће након анализе обавештења о инциденту извршити адекватну класификацију. Такође, с обзиром да је реч о називу институције, неопходно је да почетно слово у називу Регулаторног тела за електронске комуникације и поштанске услуге исправи у целом тексту Нацрта закона о информационој безбедности.	ПРИХВАЋЕН
		Став 10. изменити тако да гласи: „Приликом управљања инцидентом Национални	ДЕЛИМИЧНО ПРИХВАЋЕН Сугестија да се речи „пријем обавештења о

		ЦЕРТ, Народна банка Србије и Регулаторно тело за електронске комуникације и поштанске услуге означавају обавештење о инциденту, односно информације о инциденту, у складу са прописима и TLP (енг „Traffic Light Protocol").“ Поред обавештења о инциденту, у поступку управљања долази се и до других информација које су везане за ознаку пријаве, као што су додатна обавештења или извештаји из овог члана (13.) Нацрта закона, те сматрамо да је неопходна примена TLP-а на цео процес управљања инцидентом и на све информације о инциденту, као што и Протокол дефинише.	инциденту“ замене речима „управљање инцидентом“ није прихваћен јер предлагач сматра да управљање инцидентом није адекватан превод incident handling на српски језик јер има конотацију да заправо национални ЦЕРТ стоји иза инцидента па њиме и управља. У том смислу се предлагач определио да га преводи на различитим местима у закону у складу са интенцијом у контексту те конкретне употребе у недостатку израза који представља апсолутни превод овог појма.
	SHARE фондација	Када је реч о обавештавању јавности о инцидентима, члан 13. став 6. Нацрта предвиђа да Национални ЦЕРТ може уз консултацију са оператором ИКТ система објавити информације о инциденту „када је неопходно да јавност буде упозната са инцидентом или када је инцидент такав да је од интереса за јавност“. Сматрамо да би било ефектније да се ова одредба прецизира и више прилагоди тексту из НИС2 директиве (члан 23) који предвиђа обавештавање јавности у случају где је „неопходна свест јавности да би се реаговало на	ПРИХВАЋЕН

		активан значајни инцидент", „како би се значајни инцидент спречио" или „ако је објављивање информација о значајном инциденту на други начин у јавном интересу". Нацртом би могло да се подстакне проактивно објављивање post mortem анализа инцидента, без откривања осетљивих техничких информација о самом ИКТ систему, која би садржала информације од значаја за друге ИКТ системе зарад превенције будућих инцидената: индикаторе компромитације, уочене тактике и технике нападача, савете за заштиту од сличних напада и митигацију и томе слично.	
	Српске кабловске мреже (СББ)	Члан 13. став 6. Када је неопходно да јавност буде упозната са инцидентом или када је инцидент такав да је од интереса за јавност, Национални ЦЕРТ може објавити информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио. Коментар: Ко у овом случају доноси финалу одлуку – Национални ЦЕРТ или Оператор ИКТ система од посебног значаја? Неопходно је појаснити.	ПРИХВАЋЕН
	Друштво за информатику Србије	Члан 13. допунити прецизном одредбом ко је обавезан и у ком случају да доставља коментаре о инциденту.	НИЈЕ ПРИХВАЋЕН Коментар је размотрен и утврђено је да је одредба довољно прецизна.

Члан 14	Српске кабловске мреже (СББ)	Члан 14. став 1. тачка 2) инциденте који утичу на велики број корисника услуга, или трају дужи временски период; Коментар: Термин „велики број“ и „дужи временски период“ потребно је појаснити, није јасно шта се подразумева под тим.	НИЈЕ ПРИХВАЋЕН Реч је о уобичајеним правним стандардима.
	Удружење банака Србије	Задњи параграф: У вези са коментаром на Члан 2. дефиниција Озбиљне претње. По нашем мишљењу отвара се место за раличита тумачње појма озбиљна претња што би могло довести до неконзистентности у пријављивању инцидената.	НИЈЕ ПРИХВАЋЕН Како је раније објашњено, реч је о термину из НИС2.
Члан 15	Друштво за информатику Србије	Неусклађеност члана 15 и члана 19. Нацрта закона о информационој безбедности Наиме у чл. 15. су набројане надлежности Канцеларије, а тек у чл. 19. се наводи да се у Републици Србији оснива Канцеларија. Радом Канцеларије руководи Директор кога именује Влада, а који мора бити лице одговарајуће стручности са најмање 5 година искуства на пословима руковођења (чл. 19. став 3. Нацрта). Није наведено шта је то „одговарајућа стручност“ (степен и која школска спрема) и на којим пословима руковођења, што би било неопходно	НИЈЕ ПРИХВАЋЕН Ништа од наведеног није материја овог закона већ прописа који се сходно примењују.

		имајући у виду сложеност и обим послова Канцеларије за информациону безбедност. Канцеларија има заменика директора за кога нису наведени никакви стручни услови ни радно искуство (чл. 19. став 4 Нацрта). С обзиром да се формира ново тело (Канцеларија), није наведено да ли су и који финансијски инструменти потребни за извршење Нацрта и ко их обезбеђује.	
	РАТЕЛ	Члан 15. ставови 3. и 4. уместо Канцеларија за информациону безбедност – Национални ЦЕРТ Коментар: Имајући у виду да Канцеларија послове Националног ЦЕРТ-а неће обављати до 2026. године, сматрамо да је ради јасније и прецизније дефиниције делокруга послова потребно извршити ову измену, нарочито јер од 01.01.2026. године Канцеларија за информациону безбедност обавља послове Националног ЦЕРТ-а.	НИЈЕ ПРИХВАЋЕН Интенција је да Канцеларија за информациону безбедност буде институционално овлашћена за поступање у ситуацијама из члана 15. а не само кроз своју организациону јединицу тј. Национални ЦЕРТ.
	Америчка привредна комора у Србији (AmCham)	Члан 15. Потребно је Законом прописати критеријуме, процедуру и надлежни орган за одређивање нивоа опасности инцидената у ИКТ системима од посебног значаја.	ПРИХВАЋЕН Предлагач ће финално формулисати одредбу у току интерне процедуре усвајања у консултацији са другим надлежним органима.
	А1	У вези са чланом 15. став 5. Нацрта Закона, предлажемо да се изврши измена тако да управљање инцидентима ниског и средњег нивоа	ПРИХВАЋЕН Предлагач ће финално формулисати одредбу у току интерне процедуре усвајања у консултацији

		врши самостално оператор ИКТ система од посебног значаја уз могућност остваривања сарадње са Канцеларијом за информациону безбедност, министарством надлежним за послове информационе безбедности, Телом за координацију информационе безбедности и другим надлежним органима по потреби. Образложење: Предложена измена омогућава ефикасније реаговање у случају инцидената ниског и средњег нивоа, у складу са сопственим капацитетима оператора ИКТ система од посебног значаја, а уз могућност остваривања сарадње са Канцеларијом за информациону безбеедност и другим надлежним органима по потреби. Уколико би Канцеларија за информациону безбедност одговорна за управљање инцидентима ниског, средњег и високог нивоа, и то код свих оператора од посебног значаја у Републици Србији то би могло да доведе до преоптерећења њених капацитета и да успори и учини сложенијим поступак поступања у вези са инцидентима ниског и средњег нивоа које би оператор ИКТ система од посебног значаја могао на ефикасан и брз начин да реши са сопственим капацитетима и на тај	са другим надлежним органима.

		начин предузме одговарајуће мере за реаговање на инцидент и спречавање даље штете. Предлажемо да се задрже одребе из Нацрта Закона тако да Канцеларија за информациону безбедност управља инцидетима високог нивоа, а Влада Републике Србије инцидентима веома високог нивоа, чиме би се обезбедила заштита интереса Републике Србије код инцидената од већег значаја.	
	Савет страних инвеститора	Наслов члана 15 : Значај инцидента према нивоу опасности Предлог измене: Значај инцидента према нивоу претње Релевантни члан: члан 15 став 2 Инциденти у ИКТ системима од посебног значаја могу се сврстати у следеће нивое опасности: 1) веома висок; 2) висок; 3) средњи; 4) низак. Коментар: недостаје криза информационе безбедности као највиши ниво претње по информациону безбедност Републике Србије.	НИЈЕ ПРИХВАЋЕН Интенција је да фокус буде на материјализованим инцидентима радије него на сајбер претњама, у том смислу предлагач сматра да је овај израз адекватнији.
Члан 16	А1	У вези са чланом 2. став 1. тачка 13) који уређује појам „избегнутог инцидента” и чланом 16. став 1. прописује обавезу достављања статистичких података о инцидентима (који укључују и избегнуте инциденте), предлажемо да	НИЈЕ ПРИХВАЋЕН Ово питање ће бити регулисано подзаконским актом и у том смислу овај коментар ће свакако бити узет у разматрање том приликом.

		се изврши прецизирање избегнутих инцидената за које постоји обавеза достављања статистичких података на годишњем нивоу.	
Члан 17	Национална алијанса за локални економски развој (НАЛЕД)	Пре члана 17. уметнути наслов Организација система за управљање информационом безбедношћу у Републици Србији, а тренутни наслов уметнути пре члана 5.	НИЈЕ ПРИХАВЋЕН Не сматрамо да је предложени назив адекватан јер није реч о систему за управљање информационом безбедношћу у Републици Србији већ о надлежности органа у области информационе безбедности.
Члан 18	Партнери Србија	Члан 18. Тело за координацију послова информационе безбедности – Потребно је допунити став 1. члана 18, тако што ће се набројаним органима чији представници улазе у састав Тела за координацију послова информационе безбедности додати и Повереник за информације од јавног значаја и заштиту података о личности. Укључивањем Повереника у Тело за координацију, осигурава се присуство стручњака из области права на заштиту података о личности, посебно имајући у виду да је ово право међу првима на удару у случају инцидената, те да су последице по права и слободе лица у оваквим случајевима далекосежне. Такође, представници Службе Повереника могу додатно допринети раду Тела својим разумевањем	ДЕЛИМИЧНО ПРИХВАЋЕН Приликом успостављања Тела за координацију постојећим законом предложено је да Повереник буде у иницијалном саставу међутим ова институција се изјаснила да не сматра да треба да буде члан Тела за координацију јер је то тело Владе Републике Србије, а Повереник је независан орган. Представници Повереника били су чланови Радне групе за израду Нацрта закона и сви њихови коментари су уважени и уврштени у Нацрт текста. Током рада Радне групе нису исказали став супротан ранијем у погледу састава Тела за координацију. Наравно, у рад Тела, по потреби могу да се укључују и представници других

		баланса између заштите информација и права на слободан приступ информацијама од јавног значаја. Такође, укључивање Повереника олакшава размену информација између органа надлежних за управљање информацијама. Ово би довело до ефикаснијих решења и боље координације у случају потребе за реаговањем на инциденте који угрожавају информациону безбедност.	органа и организација и појединци који могу да допринесу реализацији појединачних задатака.
	Савет страних инвеститора	Релевантни члан: Члан 18 / тело за координацију послова информационе безбедности У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности Влада оснива Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију), као координационо тело Владе, у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије за информациону безбедност, Канцеларије Савета за националну	НИЈЕ ПРИХВАЋЕН Представници Канцеларије за ИТ и еУправу јесу у саставу Тела за координацију само под ресорним називом институције, а не тренутним називом („органа надлежног за пројектовање, усклађивање, развој и функционисање система електронске управе“) да би се избегла потреба за мењањем закона уколико она промени име или правни статус. Што се тиче дела о Поверенику погледати образложење на коментар у пољу изнад.

		безбедност и заштиту тајних података, органа надлежног за пројектовање, усклађивање, развој и функционисање система електронске управе, Генералног секретаријата Владе, Народне банке Србије и регулаторног тела за електронске комуникације и поштанске услуге. Предлог: Потребно је допунити и Канцеларијом за ИТ и еУправу, као ЦЕРТ-ом државних органа, као и Повереника за заштиту података о личности. Независно од тога што Канцеларија за ИТ и еУправу неће бити ЦЕРТ државних органа велик је њен значај.	
Члан 19	Српске кабловске мреже (СББ)	Члан 19. став 3. Радом Канцеларије руководи директор кога именује Влада, а који мора бити лице одговарајуће стручности које има најмање 5 година искуства на пословима руковођења. Коментар: Како ће се дефинисати неопходна стручност? „послови руковођења“ су шири појам – није исто руководити пословима информационе безбедности у компанијама од 10 запослених и од 10.000 запослених. Требало би строжије дефинисати критеријуме.	НИЈЕ ПРИХВАЋЕН Предлагач се определио за уобичајен правни стандард приликом одређивања законом прописаних квалификација руководиоца посебне организације, имајући у виду да се прецизнија одређења углавном врше интерним актима, условима конкурса и сл.
	Америчка привредна комора у Србији (AmCham)	Експлицитно прописати да лице које руководи канцеларијом поседује стручност и области	НИЈЕ ПРИХВАЋЕН Предлагач се определио за уобичајени правни стандард „одговарајућа стручност“ јер имајући у

		информационе безбедности.	виду да је реч о Закону о информационој безбедности то би била стручност у вези са пословима информационе безбедности. Прецизније одређење би значајно сузило круг лица која би испуњавала услове јер је реч о области у којој у целом свету још нису развијени кадрови за различите улоге које спровођење политика и мера сајбер безбедности подразумева. Сматрамо да је, у том смислу, одговарајућа стручност и лице које је радило на пословима у вези са информационо-комуникационим технологијама.
	SHARE фондација	Оснивање Канцеларије за информациону безбедност (КИБ) у оквиру које ће бити и Национални ЦЕРТ отвара питања у вези са могућношћу политичког утицаја, транспарентношћу рада КИБ и обезбеђивањем довољно стручног кадра за адекватан ниво капацитета. У погледу унапређења транспарентности, могуће је предвидети обавезу да КИБ објављује детаљан годишњи извештај о раду који би укључивао статистичке податке, али и детаљне техничке анализе најзначајнијих инцидената, без навођења одговорности и конкретног ИКТ система од посебног значаја где се инцидент догодио. Ово би омогућило праћење	НИЈЕ ПРИХВАЋЕН Запажања истакнута овде свакако представљају одређене ризике у примени којих је и предлагач свестан. Међутим, то су општи ризици који не могу да се уклоне појединачним законом. Канцеларија за ИБ је посебна организација на коју се примењују општи закони који уређују рад државне управе и они садрже одредбе које гарантују транспарентност, елиминисање нежељеног политичког утицаја, извештавање о раду и слично. Претпоставка је да ће се постојеће законске одредбе

		трендова на дужи рок када је реч о инцидентима, како на секторском, тако и националном нивоу. Члан 19 Нацрта закона предвиђа да Канцеларијом за информациону безбедност руководи директор, кога именује Влада. Као услов наведено је да лице које се именује за директора мора бити лице "одговарајуће стручности" са радним искуством од најмање 5 година на пословима руковођења. Имајући у виду комплексност задужења и широк спектар надлежности КИБ, као и све напредније изазове са којима се суочавамо у дигиталном окружењу, сматрамо да је од изузетне важности да се законом пропише да именовано лице додатно поседује знања, искуство и компетенције у области безбедности информационих технологија.	поштовати, а не супротно. У вези са делом који се односи на одговарајућу стручност руководиоца, указујемо на образложење изнето у одговорима на коментаре изнад.
Члан 21	Саша Милашиновић	Члан 21. Надлежности канцеларије 5) послове стандардизације и сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга Ингеренције Института за стандардизацију Србије, АТС-а, сертификационих кућа… Никако не треба преузимати ингеренције за које већ постоје овлашћена тела од стране Републике Србије. Посебно је упитна	ДЕЛИМИЧНО ПРИХВАЋЕН Уклоњена је реч стандардизација јер заиста није адекватна у овом контексту. Конкретна одредба представља транспозицију Акта ЕУ о сајбер безбедности који говори о сертификацији ИКТ производа, услуга, процеса и система.

		компетентност и акредитације које су за такве послове неопходне.	
		7) у сарадњи са надлежним органима учествује у развоју и спровођењу програма обука и стручног усавршавања Компетентност канцеларије (Министарство просвете, Национална академија за јавну управу, акредитације, компетентност за едукацију…)	НИЈЕ ПРИХВАЋЕНО Одредба је формулисана тако да је комплементарна раду других надлежних институција.
		8) извештава Министарство на кварталном нивоу о предузетим активностима И јавност!!! Транспарентност рада, основна функција ЦЕРТ-а, Закон о приступу јавним информацијама	НИЈЕ ПРИХВАЋЕН Овде је реч о обавези извештавања према ресорно надлежном органу. Транспарентност у раду и обавештавање јавности регулисано је на другим местима у закону и другим законима који уређују рад органа државне управе.
	SHARE фондација	Такође, чланом 21. ст. 1. тач. 7) Нацрта закона предвиђено је да Канцеларија у оквиру њене надлежности „у сарадњи са надлежним органима учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности у органима”. Сматрамо да би речи „у сарадњи са надлежним органима” требало искључити из наведене тачке, имајући у виду значај сарадње са свим заинтересованим актерима на едукацији и подизању нивоа знања, пре свега цивилним сектором и академском заједницом.	ДЕЛИМИЧНО ПРИХВАЋЕН Прихваћено да се сарадња обавља и са другим актерима поред надлежних органа.

Члан 22	Саша Милашиновић	6) на захтев оператора ИКТ система од посебног значаја, врши проактивно скенирање ИКТ система у циљу утврђивања рањивости које могу да потенцијално знатно наруше безбедност ИКТ система, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора; Не сме да ради никакво скенирање. Није и не треба да буде у надлежности Националног ЦЕРТ-а. Компетентност Националног ЦЕРТ-а, Ресурси… Потенцијално велики проблеми технике природе и велике могућности за злоупотребу организационе и правне природе.	НИЈЕ ПРИХВАЋЕН Одредба представља транспозицију одредбе НИС2 директиве.
	Национална алијанса за локални економски развој (НАЛЕД)	Члан 22. тачка 11 - Предлог да се обрише реч "усвајање" или да се уместо речи "промовише" користи термин адекватнији за овлашћења Националног ЦЕРТ-а, која превазилазе промовисање. Како је дефинисано није јасно ко промовише и ко је циљана јавност којој се промовише, нарочито ако се промовише усвајање прописа и процедура.	НИЈЕ ПРИХВАЋЕН Одредба се односи на подстицање коришћења прописаних процедура код оних субјеката који на то нису обавезни законом, али који би било пожељно да примењују прописане процедуре у циљу развоја свести и унапређења свеукупне информационе безбедности.
	РАТЕЛ	Члан 22. став 1. Додати као посебне тачке: „води Евиденцију посебних ЦЕРТ-ова“ и „води базу рањивости“.	ПРИХВАЋЕН
		Члан 22. став 1. тачка 1) Изменити тако да гласи: „Прикупља и размењује информације о претњама, рањивостима и	ПРИХВАЋЕН

		инцидентима и пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији као и јавност“. Сматрамо да је употреба појмова претње, рањивости и инцидената целисходнија, као и да је потребно брисати догађаје, нарочито имајући у виду да Нацрт закона не прописује дефиницију догађаја.	
		Члан 22. став 2. тачка 1) изменити тако да гласи: „управљање инцидентима“.	НИЈЕ ПРИХВАЋЕН Из раније наведених разлога, предлагач сматра да управљање инцидентом није адекватан превод incident handling из НИС2.
		Члан 22. став 2. тачка 2) изменити тако да гласи: „класификацију информација о инцидентима, односно класификацију према нивоу опасности инцидената“. Мишљења смо да је предложена измена примеренија од одредби НИС 2 Директиве.	ПРИХВАЋЕН
	Нафтна индустрија Србије (НИС)	Члан 22. став 1. тачка 5) потребно је брисати речи: „у реалном времену или приближно реалном времену“. Предлог је да се измена изврши на начин да се део „у реалном времену или приближном реалном времену“ избрише. Није јасно шта се подразумева под термином „приближно реално време“.	НИЈЕ ПРИХВАЋЕН Одредба је транспозиција одредбе НИС2 директиве. Одредница је одатле преузета.
	Бранислав Добросављевић	Ово ће по мени бити најсложенији (од многих сложених) задатака у	ДЕЛИМИЧНО ПРИХВАЋЕНО

		разради и реализацији овог закона. Наиме, нови Закон је предвидео да Национални ЦЕРТ пређе из РАТЕЛ-а у нову Канцеларију од 1.1.2026. године. Реално претпостављајући да ће нови Закон бити донет крајем ове године, прелазни период (док је овај ЦЕРТ још у РАТЕЛ-у) трајаће целе две године, од чега у првих шест месеци треба да буду донета сва подзаконска акта. С друге стране, закон је предвидео значајно повећање обима и сложености посла Националног ЦЕРТ-а, с тим што ове обавезе треба да почну да се остварују одмах по доношењу закона. Да би се видело колико су те обавезе сложене, треба погледати члан 22. „Послови Националног ЦЕРТ-а", посебно став 1, тачке 1) 4-8. (Ко год је радио у масовној ИТ подршци, дићи ће му се коса на глави од овога!) Имајући искуство у решавању оваквих питања у низу српских закона у претходном периоду, веома сам забринут да ће са овим у пракси бити великих проблема ако му се већ у подзаконским актима не посвети одговарајућа пажња.	Предлагач је узео у разматрање да предвиди доношење појединих подзаконских аката у року од годину дана од дана ступања на снагу.
Члан 24	Партнери Србија	Члан 24. Сарадња на националном нивоу - Потребно је допунити став 1. и став 2. овог члана, тако што ће се међу органе са	НИЈЕ ПРИХВАЋЕН Реч је о члану који уређују сарадњу између органа који су одређени као надлежни за потребе

		којима Национални ЦЕРТ непосредно сарађује, односно одржава састанке, навести и Повереник за информације од јавног значаја и заштиту података о личности, из разлога наведених у предлогу за допуну члана 18.	Закона о информационој безбедности. Повереник није један од надлежних органа за област безбедности информационих система и мрежа. Наравно, општи прописи који уређују питање међу институционалне сарадње примењују се и у случају органа надлежних по ЗИБ.
Члан 25	Америчка привредна комора Србије (AmCham)	Овај члан није у складу са Законником о кривичном поступку, имајући у виду: - Недостатак појма „кривична дела која се гоне по службеној дужности“ (дакле, не односи се на сва кривична дела, односно кривична дела која се гоне по приватној тужби, већ само на кривична дела која се гоне по службеној дужности од стране надлежног јавног тужилаштва и/или полиције уколико то одлучи надлежно јавно тужилаштво) и - Недостатак појма „надлежног јавног тужилаштва“, као државног органа који је надлежан да квалификује да ли одређени инцидент уопште има елементе кривичног дела, а после тога да ли се гони по службеној дужности, те да након тога покрене и руководи кривичним поступком. Стога, предлажемо следећу формулацију члана 25. тако да гласи: „Уколико је инцидент у вези са извршењем	ПРИХВАЋЕНО

		кривичног дела које се гони по службеној дужности, Канцеларија ће о томе обавестити надлежно јавно тужилаштво, које ће самостално или преко министарства надлежног за унутрашње послове у званичној процедури проследити пријаву у складу са потврђеним међународним уговорима.“	
Члан 27	РАТЕЛ	Члан 27. став 2 тачка 2) изменити тако да гласи: „Податке о рањивим ИКТ производима и ИКТ услугама“. Сматрамо да је прецизније дефинисати као рањиви ИКТ производи и ИКТ услуге јер се већ користе у нашем језику.	ПРИХВАЋЕН
	Саша Милашиновић	Члан 27. База рањивости Ово би требао да буде подзаконски акт, а не да се налази у закону.	НИЈЕ ПРИХВАЋЕН Питања везана за базу рањивости биће уређена подзаконским актом тј. актом Националног ЦЕРТа како и пише у последњем ставу овог члана. Подзаконски акт може се донети само у ситуацијама где закон дозвољава да се одређено питање уреди на тај начин у том смислу законски основ за подзаконски акт мора да постоји у закону.
	Српске кабловске мреже (СББ)	Члан 27. став 1. Ово је профитабилан посао и на добровољној бази нико неће пријавити нешто што може наплатити. Треба направити „bug bount program" који плаћа награде за откривене рањивости, како би	НИЈЕ ПРИХВАЋЕН Реч је о транспозицији одредбе НИС2 директиве.

		ово имало икаквог смисла.	
	SHARE фондација	Члан 27. Нацрта закона јесте добар пример размене информација и транспарентности, али је Нацрт ипак предвидео да она буде на добровољној бази.	НИЈЕ ПРИХВАЋЕН Реч је о транспозицији одредбе НИС2 директиве.
Члан 28	Национална алијанса за локални економски развој (НАЛЕД)	Члан 28. став 5. – У став 5. је потребно унети и информације о полу, у складу са чланом 12. Закона о родној равноправности.	НИЈЕ ПРИХВАЋЕН Податак о полу се не тражи за потребе евидентирања пријаве већ само подаци наведени у закону. У том смислу не постоји ни његова обрада.
		Члан 28. став 7. – Потребно је додати тачку 4. у став 7. која гласи „обезбеди континуирану обуку о родно заснованом насиљу запослених који раде на систему за пријем пријава“.	ПРИХВАЋЕН
		Члан 28. Уколико из навода пријаве проистиче основана сумња да је извршено неко од кривичних дела које се гони по службеној дужности, пријава ће бити прослеђена надлежном јавном тужилаштву. Уколико из навода пријаве проистиче да се ради о кривичном делу које се гони по приватној тужби, подносилац пријаве би требао да буде поучен и упућен од стране службеника јединственог места за пружање савета и пријем пријава у вези безбедности деце на интернету, да лично поднесе приватну тужбу надлежном суду, јер код кривичних дела која се гоне по приватној тужби није	НИЈЕ ПРИХВАЋЕН Питање је већ уређено Уредбом о безбедности и заштити деце при коришћењу информационо-комуникационих технологија "Службени гласник РС", број 13 од 14. фебруара 2020.

		предвиђена надлежност и поступање државних органа по службеној дужности (тужилаштво и полиција, пре свега). Мишљења смо да би овакво поступање службеника требало регулисати у интерном акту којим се регулише процедура пријема и обраде пријава у јединственом месту за пружање савета и пријем пријава у вези безбедности деце на интернету. Стога, предлажемо следећу допуну члана 27. става 3. тако да гласи: „У случају да наводи из пријаве упућују на постојање кривичног дела које се гони по службеној дужности, на повреду права, здравственог статуса, добробити и/или општег интегритета детета, на ризик стварања зависности од коришћења интернета, пријава се прослеђује надлежном органу ради поступања у складу са утврђеним надлежностима“.	
	Партнери Србија	Члан 28. - Потребно је допунити став 3. члана, тако што ће се након: „У случају да наводи из пријаве упућују на постојање кривичног дела, на повреду права, здравственог статуса, добробити и/или општег интереса детета, на ризик стварања зависности од коришћења интернета, пријава се прослеђује	НИЈЕ ПРИХВАЋЕН Питање је већ уређено Уредбом о безбедности и заштити деце при коришћењу информационо-комуникационих технологија "Службени гласник РС", број 13 од 14. фебруара 2020.

		надлежном органу раду поступања у складу са утврђеним надлежностима“ додати: „без одлагања, а најкасније у року од 24 сата од пријема пријаве“.	
	Саша Милашиновић	Члан 28. би требао да буде подзаконски акт, а не да се налази у закону.	НИЈЕ ПРИХВАЋЕН Питање је већ уређено Уредбом о безбедности и заштити деце при коришћењу информационо-комуникационих технологија "Службени гласник РС", број 13 од 14. фебруара 2020.
	SHARE фондација	Члан 28. Нацрта који се бави заштитом деце при коришћењу ИКТ предвиђа јединствено место за пружање савета и пријем пријава у вези безбедности деце на интернету, где је наведено да се подаци о лицима која подносе пријаве чувају у роковима предвиђеним прописима који уређују канцеларијско пословање. Како канцеларијско пословање уређују подзаконски акти, напомињемо да се питања обраде и заштите података о личности морају уредити законом, те да би наведену одредбу требало преформулисати на начин да се не позива на акте ниже правне снаге.	НИЈЕ ПРИХВАЋЕН Представници Повереника за заштиту података о личности били су чланови Радне групе и доставили своје коментаре који су сви уважени. Уколико током процедуре прибављања мишљења надлежни орган не сугерише да се ово питање уреди другачије, предлагач ће задржати постојеће решење које је на снази и по постојећем закону.
Члан 29	Савет страних инвеститора	Министарство надлежно за послове одбране је надлежно за послове информационе безбедности који се односе на одобравање криптографских производа, дистрибуцију	У ОБРАДИ Коментар ће бити прослеђен предлагачу овог дела закона на разматрање.

		криптоматеријала и заштиту од компромитујућег електромагнетног зрачења и послове и задатке у складу са законом и прописима донетим на основу закона. Коментар: Опасно је дефинисати надлежност МО за комплетан јавни и приватни сектор, којим се намеће примена Закона о тајности података на све податке како је дефинисано чланом 32. На овај начин излази се из надлежности МО како је дефинисано Законом о министарствима. Поред тога, оправдано сумњамо у капацитете МО да надзире и сертификује све ИКТ системе од посебног значаја у овој области, што би за последицу имало огромне административне баријере и неусаглашеност са Законом о информационој безбедности огромног броја субјеката. Коришћење криптографије регулисано је овим законом кроз дефинисане мере заштите ИКТ система и процену ризика по информациону безбедност ИКТ система. Такође, примена криптографских контрола и управљање криптографским кључевима спроводиће се у складу са проценом ризика по информациону безбедност ИКТ система.	

		Предлог: Предлажемо да се ово поглавље избаци из Закона о информационој безбедности.	
Члан 32 и 33	SHARE фондација	Дугорочно гледано, законом би требало омогућити да се слично одредбама НИС2 директиве (чланови 32 и 33) које се односе на мере надзора над операторима ИКТ система од посебног значаја усвоје мере које би потенцијално допринеле да обвезници имају повећану свест о спровођењу надзора. У зависности од капацитета и ресурса министарства као надлежног органа, те мере могу бити теренске посете, насумичне контроле, редовне безбедносне ревизије система, ад хоц ревизије система и томе слично.	НИЈЕ ПРИХВАЋЕНО Применом општег прописа који уређује питање инспекцијског надзора дозвољено је да инспектори поступају на наведене начине и предлагач је става да то не ма потребе дупло прописивати и посебним законом.
Члан 36	Национална алијанса за локални економски развој (НАЛЕД)	Члан 36. став 2. у складу са чланом 12. став 1. и 4. Закона о родној равноправности укључити и пол лица која обављају послове криптозаштите.	НИЈЕ ПРИХВАЋЕН Прихваћен је предлог да се у уводном члану закону напише да све што је изражено у мушком роду односи се на оба пола и предлагач сматра да не мора да понавља ту одредбу на осталим местима у закону.
Члан 38	Саша Милашиновић	Члан 38. Овлашћења инспектора за информациону безбедност 3) захтева од оператора ИКТ система од посебног значаја да изврши скенирање мреже у циљу утврђивања евентуалних безбедносних рањивости, а у складу са проценом ризика;	НИЈЕ ПРИХВАЋЕНО Реч је о транспозицији одредбе из НИС2 директиве

		Ако Канцеларија за ИКТ безбедност и Национални ЦЕРТ врше скенирање ИКТ система од посебног значаја, зашто се налаже ИКТ систему од посебног значаја да ради послове које им нису у ингеренцији и да се излажу трошку ангажовања пенетратион тестера. У сваком случају, треба избацити улогу тестирања и издавања налога за пенетрационе тестове. Посебно, треба јасно разграничити и направити разлику између „Vulnerability“ и „Penetration“ тестирања.	
Члан 38	SHARE фондација	Иако су чланом 38. Нацрта инспекторима додељена три додатна овлашћења, што је веома значајно, седам година од усвајања првог закона број инспектора за информациону безбедности је и даље недовољан и недопустиво мали, што се донекле може разумети услед ограничених капацитета и ресурса (налажење, запошљавање и задржавање довољно стручног кадра) и интерних процедура у јавном сектору. Мера која би Канцеларији омогућила да има ширу слику стања од старта била би обавеза да оператори ИКТ система од посебног значаја Канцеларији достављају акте о безбедности и акте о процени ризика, што би такође министарству као надлежном органу	ДЕЛИМИЧНО ПРИХВАЋЕН Предлагач не може тренутно да омогући реализацију ове препоруке имајући у виду да се КИБ тек оснива овим законом и да треба да развије капацитете. Предлог ће бити узет у разматрање у припреми подзаконских аката и припреми измена и допуна закона, или се може разматрати у смислу измене општих прописа којима се уређује инспекцијски надзор.

		омогућило да ефикасније спроводи инспекцијски надзор.	
Члан 39	Национална алијанса за локални економски развој (НАЛЕД)	Члан 39 - У казнене одредбе потребно је унети неовлашћено обелодањивање поверљивих информација оператора ИКТ система. Потребно је размотрити и казнену одредбу за оператора ИКТ система од посебног значаја када не управља информационом безбедношћу на начин да обезбеди да не дође до инцидента.	НИЈЕ ПРИХВАЋЕН То је већ кажњиво поступање применом других закона из области кривичног и казненог права.
	Бранислав Добросављевић	Мислим да казна од 2.000.000 динара за највеће пропусте за гиганте у критичним областима (енергетика, телеком оператери) унапред дезавуише важност овог закона током будуће примене. Хитном изменом Закона о прекршајима треба омогућити да горња граница казне, специјално за поједине случајеве (информациона безбедност, екологија и видети шта још) буде вишеструко већа. У вези са овим је и потреба да се током примене новог закона значајно унапреди рад инспекцијске службе, о чему је сигурно било пуно коментара других учесника јавне дискусије.	НИЈЕ ПРИХВАЋЕН Овим законом не може да се одступи од општег режима прекршајног права.
Члан 39,40,41 и 42	Партнери Србија	Требало би детаљније регулисати висине новчане казне за специфична кршења, имајући у виду да су тренутно прописани казнени распони за низ	ПРИХВАЋЕН/ У ОБРАДИ Током процеса интерних процедура и прибављања мишљења, предлагач ће у сарадњи са надлежним

		различитих чињења и нечињење веома високи (нпр. члан 39. предвиђа новчану казну у распону од 50.000 до 2.000.000 динара). Додатно прецизирање би обезбедило виши ниво предвидљивости и правне сигурности, а омогућило надлежним органима да брже и ефикасније доносе одлуке о казнама, јер имају јасне смернице о томе које казне су примерене за које врсте кршења.	институцијама формулисати евентуално разликовање према озбиљности преступа.
Члан 43	РАТЕЛ	Члан 43. Додати став 2. да гласи: „Подзаконски акт предвиђен чланом 27.овог закона донеће се у року од 12 месеци од дана ступања на снагу овог закона“. Сматрамо да доношење подзаконског акта којим ће се прописати база рањивости изискује више времена, која укључује између осталог и анализу решења у уз упоредне праксе, нарочито земаља чланица ЕУ које тренутно раде на развоју својих решења.	ПРИХВАЋЕН/ У ОБРАДИ У складу са више сугестија овог типа, предлагач ће приступити изради овог члана на начин да се одређени акти доносе у року од 6 месеци, а други у року од 12 месеци зависно од релевантности за очување постојећег система.
Уопштено	Нафтна индустрија Србије (НИС)	У закону нису дефинисани појмови ИКТ добро, ИКТ сервис, IT ресурс ИКТ сервис: функционалност и погодност коју Корисник добија од Провајдера ИКТ сервиса, коришћењем ИКТ добара и ИКТ услуга, у оквиру дефинисаног система квалитета ИКТ сервиса, како би корисницима ИКТ сервиса	НИЈЕ ПРИХВАЋЕН Нацрт закона израђен је са циљем усклађивања са НИС2 директивом. Како овај пропис ЕУ не садржи дефиниције ових појмова, нити се они појављују у закону, предлагач је мишљења да не треба посебно да их дефинише за потребе примене и тумачења

		омогућило креирање, управљање и оптимизација или приступ информацијама и пословним процесима. По својој природи ИКТ сервиси се могу поделити на две основне групе и то: сервисе који су доступни корисницима (ITIL: customer faced services) и техничке сервисе (ITIL: supporting services); ИКТ добро - хардвер/софтвер у оквиру ког се врши обрада података и/или пренос података и/или се омогућава приступ подацима (модем, рутер, свич, рачунар, сервер, конзола, фајервол, штампач, оперативни систем, апликација, софтверска решења, мобилни телефон) IT ресурс - ИКТ добро + ИКТ сервис + периферија (миш, тастатура, монитор, слушалице) Наведени термини су употреби у процедурама оператора ИКТ система и њихово дефинисање би олакшало рад у смислу тумачења закона и интерних процедура.	закона о информационој безбедности.
Уопштено	SHARE Фондација	Овим путем такође позивамо Министарство информисања и телекомуникација да са Министарством правде покрене консултације о изменама Закона о прекршајима, како би се кроз изузетке прописале више казне за кршење	ПРИХВАЋЕНО Министарство ће свакако када за то буде била прилика, у смислу иницијативе да се Закон о прекршајима измени, предложити одредбе за потребе усклађивања са казненом политиком НИС2 директиве.

		Закона о информационој безбедности. Највиша казна прописана Нацртом закона је 2.000.000 динара, што јесте максимум одређен Законом о прекршајима, али из позиције великих корпоративних система који послују у Србији то није износ који ће деловати одвраћајуће на операторе и навести их да уложе ресурсе у адекватну примену мера заштите и других обавеза прописаних законом.	

Прилог 1: Извештај са округлог стола одржаног у Београду дана 18. августа 2023. године

ЗАПИСНИК СА ПРВОГ ОКРУГЛОГ СТОЛА У ОКВИРУ ЈАВНЕ РАСПРАВЕ ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

одржаног дана 18. августа 2023. године с почетком у 10:00 часова у Свечаној сали Градске општине Стари град, Београд (Македонска 42)

Јелена Мићић, представница Националне алијансе за економски развој (НАЛЕД) свечано је отворила прву јавну расправу поводом Закона о информационој безбедности и

захвалила се свим присутнима на великом интересовању за учешће. Истакла је да у изради Нацрта закона о информационој безбедности у оквиру Радне групе за израду Нацрта Закона о информационој безбедности (у даљем тексту: Радна група) учествовао велики број представника из државних органа, привреде, образовних институција, као и представници организација које се баве питањима информационе безбедности. Главни разлог доношења новог Закона о информационој безбедности јесте приближавање домаћег закона правном оквиру Европске уније, односно усклађивање са НИС 2 директивом (2555/2022), усклађивање са Актом о сајбер безбедности ЕУ (2019/881) у делу који се односи на сертификацију у области сајбер безбедности, унапређење институционалног и организационог оквира и капацитета, као и сва даља унапређења текста стечена на темељима досадашњих искуства у примени Закона о информационој безбедности. Такође, истакла је да поред овог округлог стола који се одржава у Београду, биће одржан и други округли сто у Крагујевцу, као и да је јавна расправа је отворена до 30. августа и позвала све заинтересоване да доставе своје коментаре, мишљења и предлоге.

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, пожелио је добродошлицу свим присутнима и искористио прилику да се захвали представницима НАЛЕД-а на подршци која је пружена током рада на изради Закона о информационој безбедности. Уједно је истакао да му је веома драго што види велику заинтересованост за учешће на јавној расправи поводом Закона о информационој безбедности. Како би на што бољи начин презентовао које су то измене које се предвиђају новим Законом о информационој безбедности прво је представио је рад Радне групе која се бавила израдом овог Нацрта закона. Наиме, првобитна идеја била је доношење измена и допуна постојећег Закона о информационој безбедности, али се ипак услед промене већег броја одредби Закона приступило изради новог Закона. Представио је НИС 2 директиву, као и новине у односу на претходну НИС 2 директиву, а које се пре свега односе на класификацију оператора ИКТ система од посебног значаја, јачање улоге ЦЕРТ-ова, јачање казнене политике, увођење нових појмова, израда Националног плана деловања у случају великих инцидената, дељење информација о претњама и инцидентима. Такође, представио је и основна начела новог Закона о информационој безбедности – начело управљања ризиком, начело свеобухватне заштите, начело стручности и добре праксе и начело савести и оспособљености. Указао је да се новим Законом уводи нова подела оператора ИКТ система од посебног значаја и то на приоритетне операторе ИКТ система од посебног значаја и на важне операторе ИКТ система од посебног значаја, која је усаглашена са поделом из НИС 2 директиве. Државни органи, укључујући органе локалне самоуправе и аутономне покрајине, потпадају под приоритетну категорију, као и сви субјекти којима су поверена јавна овлашћења. Нагласио је да је главна разлика између напред наведене две категорије оператора ИКТ система од посебног значаја у динамици ревизије ИКТ система. С тим у вези, важни оператори ИКТ система од посебног значаја дужни су да врше проверу усклађености својих система једном годишње, док приоритетни оператори ИКТ системи од посебног значаја дужни су да проверу обављају два пута годишње. Даље је представљена категоризација субјеката према напред наведене две категорије, као категоризација органа који потпадају под самосталне операторе ИКТ система и њихове обавезе. Указао је да новим Законом предвиђено да ће оператори ИКТ система од посебног

значаја имати дужност да при упису у Евиденцију ИКТ систем од посебног значаја достављају и податке о својим адресама опсега интернет протокола – IP адресе (то је новина коју уводи НИС 2 директива).

Што се тиче одредби које се односе на мере заштите које су оператори ИКТ система од посебног значаја дужни да спроводе није дошло до већих промена, али су уведене неке нове контроле информационе безбедности на основу ИСО 27000 стандарда (који је допуњен крајем прошле године), а које се између осталог односе процедуре за скенирање мреже, информације о рањивостима ИКТ система, ограничење приступа интернет страницама и којих свеукупно има 34. Указао је да једна од битних новина које Закон о информационој безбедности предвиђа увођење обавезе доношења Акта о процени ризика. Заправо идеја је да Канцеларија за информациону безбедност донесе модел акта, који ће послужити операторима приликом доношења својих аката. Такође, поред Акта о процени ризика остала је обавеза доношења Акта о безбедности ИКТ система.

Обавештење о инцидентима који угрожавају информациону безбедност – уведена је обавеза операторима да пријаве инциденте који угрожавају информациону безбедност Националном ЦЕРТ-у, али не пријављују се сви инциденти који се догоде (од овога су изостављене финансијске институције, Кредитни биро и пружаоци услуга повезаних са дигиталном имовином који достављају Народној банци, као и оператори електронских комуникација који то достављају РАТЕЛ-у). У случају да је инцидент везан за кривична дела извештај се доставља МУП-у и јавном тужилаштву, док у случају да је угрожена национална безбедност извештај се доставља Министарству одбране. Законом се јасно наводи које инциденте треба пријавити, али пре свега оне које утичу на велики број корисника, који утичу на рад других оператора ИКТ система, као и оне који доводе до прекида у раду вршења послова и пружања услуга. Нацртом закона о информационој безбедности уводи се и подела инцидената према степену кризе информационе безбедности (веома висок, висок, средњи и низак), при чему се наводи и институција која је надлежна за сваки степен кризе (у случају да је ризик низак, средњи и висок надлежна је Канцеларија за информациону безбедност, а у случају да је веома висок ризик онда је надлежна Влада Републике Србије која проглашава кризу информационе безбедности и задужује органе да поступају у складу са мерама које буде донела). Статистички подаци о инцидентима оператори ИКТ система од посебног значаја достављају податке Националном ЦЕРТ-у најкасније до 28. фебруара текуће године за претходну годину и то инциденте по типовима, при чему се достављају подаци о свим инцидентима, али не детаљно објашњене већ само бројчано и према типу, степену инцидента.

Новим Законом промењен је институционални оквир, то значи да надлежни орган остаје Министарство информисања и телекомуникација, док послове ЦЕРТ-а државних органа, Националног ЦЕРТ-а (од 1. јануара 2026. године, а до тада их обавља РАТЕЛ) преузима нови орган - Канцеларија за информациону безбедност (јединствена контакт тачка, управља инцидентима, минималним мерама заштите органа), док Министарство одбране остаје надлежно за одобравање криптографских производа који се користе за руковање тајним подацима, дистрибуцију криптоматеријала и заштите од КЕМЗ-а. Представљена је улога Канцеларије за информациону безбедност (у даљем тексту: Канцеларија) која је дефинисана као орган државне управе и која ће обављати послове у складу са прописима

које уређују државну управу, а са циљем обављања послова превенције и заштите од безбедносних ризика и инцидената у ИКТ системима у Републици Србији. Надлежност Канцеларије је управљање инцидентима који значајно угрожавају информациону безбедност, обавља послове Националног ЦЕРТ-а (од 1. јануара 2026. године, до тада их обавља РАТЕЛ), обављање послова ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе, обавља сарадњу на националном нивоу у области информационе безбедности, врши послове јединствене тачке контакта, послове стандардизације и сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, прописује минималне мере заштите ИКТ система органа, у сарадњи са надлежним органима учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности у органима, извештава Министарство на кварталном нивоу о предузетим активностима, као и друге послове у складу са овим законом. Такође, биће задужена и за вођење Базе рањивости ИКТ производа и ИКТ услуга – она ће садржати податке о рањивости и податке о ИКТ производима или ИКТ услугама на које рањивост утиче (ближе ће бити регулисано подзаконским актом). Поред заштите мреже електронске управе, Канцеларија ће вршити проактивно скенирање мреже, остваривати међународну сарадњу у области безбедности ИКТ система итд.

Део одредби Закона о информационој безбедности односи се и на безбедност деце на интернету – Национални контакт центар за безбедност деце на интернету који остаје да функционише у оном облику у коме је и деловао до сада. Министарство одбране остаје надлежно за криптобезбедност и заштиту од КЕМЗ-а, а представљене су његове функције у овој области попут вршења функције националног органа за одобравање криптопроизвода и заштиту од КЕМЗ-а, развоја, имплементирања, верификације и класификације криптографске производе и алгоритме и производе и решења заштите од КЕМЗ-а итд. Део нацрта Закона који дефинише шта су тајни подаци у ИКТ системима, уз навођење изузетка, самосталних оператора, који имају опште овлашћење и није им потребна дозвола. Инспекција за информациону безбедност остаје у саставу Министарства информисања и телекомуникација, али с обзиром да већ постоји Закон о инспекцијском надзору, Закон не уводи неке новине, већ само прецизира и појашњава одређене одредбе. Једна од новина у овом домену јесте могућност да инспектори наложе да надзирани субјекат учини доступним јавности информације које се тичу непоштовања одредби овог Закона. Подзаконски акти који регулишу ову област биће донети у року од шест месеци од дана ступања на снагу овог Закона. На крају указао је да даном ступања на снагу овог закона престаје да важи Закон о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19), изузев одредби које се односе на обавезе оператора ИКТ система од посебног значаја које важе до доношења подзаконског акта из члана 6. овог закона. Након завршене презентације одредби новог Закона о информационој безбедности позвао је све присутне да поставе питања.

Ана Вушковић, Службени гласник Републике Србије, поставила је питање везано за предложени Нацрт закона о информационој безбедности – зашто је објављивање Службеног гласника подведено под категорију важних, а не приоритетних оператора ИКТ система од посебног значаја, јер је Службени гласник једини пружалац услуге објављивања гласила, и по Уставу и по закону, те самим тим би требало, на основу тог

својства, да буде подведен под категорију приоритетних оператора ИКТ система од посебног значаја. Такође, Нацртом закона не регулише се питање вођења правно-информационог система Републике Србије, што би такође требало да буде својство које карактерише приоритетне операторе ИКТ системе од посебног значаја.

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, захвалио се на коментару и истакао је да је било доста разматрања око тога које установе, односно области/делатности подвести под коју категорију, и истакао да је наведени коментар веома важан и да ће свакако бити узет у разматрање.

Соња Суботић, психолог, поставила је питање везано за навођење приоритетних ИКТ система од посебног значаја, а који се односи пружање услуга од поверења и пружање услуга ДНС-а, мобилне операторе и интернет тачке размене садржаја, да ли овај део нацрта Закона односи и на кабловске операторе? Такође, поставила је питање везано за неопходне стручњаке који би се бавили овим захтевним пословима у домену информационе безбедности, који ће бити део Канцеларије за информациону безбедност.

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да се тај део Закона, који се односи на приоритетне ИКТ системе од посебног значај, односи и на кабловске операторе. Канцеларија за информациону безбедност објединиће послове који су сада подељени између више институција. У претходном периоду велики број људи је оспособљен у овој области, па су спремни да одговоре на изазове информационе безбедности.

Горан Јагодић, представник Градске општине Палилула - Београд, поставио је питање - Како обезбедити да управљачка структура у локалним самоуправама приушти људска и материјална средства, посебно у ситуацији где су потребе све веће, а средстава је све мање. Такође, поред напред наведеног указао је да постоји велики проблем око кадрова, па се поставља питање како то превазићи? Осим тога поставио је питање почињања рада Канцеларије за информациону безбедност, и указао да је неопходно да локалне самоуправе смање потребу за обављањем послова информационе безбедности код себе, с обзиром да већ постоје Државни дата центри, па се поставља питање да ли локалне самоуправе могу да користе њихове услуге и да се они баве заштитом података у локалним самоуправама?

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је Министарство свесно да не постоји свуда у Републици Србији једнака свест о значају информационе безбедности, као и о средствима које је потребно уложити у ову област. Управо због тога потребно је представити све негативне последице које могу да се догоде и наштете локалним самоуправама, ако се догоди неки инцидент. Министарство није надлежно и не може наредити локалним самоуправама колико средстава ће расподелити. Међутим, нова Канцеларија за информациону безбедност треба да помогне локалним самоуправама у овом домену – тако што ће вршити проактивно скенирање мрежа, откривати рањивости, инцидентима. Канцеларија за информациону безбедност уложиће све напоре да помогне локалним самоуправа, а оне ће се успоставити чим се Закон донесе, крајем године. Када је

реч о чувању и заштити података локалне самоуправе, истакао је иде се у том правцу, али нема информације о тренутним плановима у овој области.

Гордана Предић, представница Градске општине Чукарица – Београд, навела је да би било добро да подаци локалних самоуправа буду чувани у Државним дата центрима. Такође, многи прописи из других области задиру у поље информационе безбедности (попут Плана интегритета за борбу против корупције), па је потребно усагласити сва та документа које стварају различите обавезе локалним самоуправама. Такође, потребно је прецизирати део који се тиче пријава инцидената – да ли то односи и на нпр. фишинг мејлове?

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да, уколико оператор ИКТ система има свој пропис о мерама информационе безбедности, није у обавези да се доноси нови. Такође, када је реч о обавештењу о инцидентима, биће организоване радионице како би се појасниле одређене појединости и нејасноће.

Томислав Ункашевић, представник Фондације Мрежа за сајбер безбедност, истакао је да би дефинисање појма безбедности, циљева и нивоа безбедности требало прецизирати, и сходно томе, класификацију типова безбедносних инцидента (тренутно нема атрибута који ближе описују те појмове, па би требало то појаснити). Напоменуо је да у праски других европских земаља постоје агенције и канцеларије сличне Канцеларији за информациону безбедност које имају оперативну улогу и активност, док у Републици Србији још увек нема. Поставио је питање везано за обављање инспекцијских послова, орган који врши контролу треба да поседује исти или већи степен знања од онога кога контролише, па се поставља питање да ли Република Србија има довољне капацитете за инспекторе и да ли постоји могућност аутсорсовања?

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да питање инспекција представља проблем на нивоу целе државе, али да предложени закон не препознаје могућност аутсорсовања инспекција. Постоји само могућност тражења неког стручног мишљења са стране, али не и ангажовања људи за те потребе.

Андреј Петровски, представник SHARE Фондације, поздравио је напоре министарства са усклађивањем са правним оквиром Европске уније. Поставио је питање везано за капацитете и питање везано за поверење у мере које институције предузимају, па самим тим и када је реч о предложеној Канцеларији за информациону безбедност. Какви су капацитети за инспекцијски надзор у овој области и да ли је некоме до сада изречена казна због непоштовања одредби тренутно важећег Закона? Који је био разлог се одредбе о инспекцијског надзора унесу ако није до сада ништа урађено у овој области?

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да су капацитети инспекције за информациону безбедност повећани ове године, али постоје изазови на нивоу целе државе, не само на пољу информационе безбедности. Током претходних године, инспекција је изрекла више мера ИКТ операторима да исправе одређене ствари, али

инспекција нема право да изриче новчане казне (нити је било сличних пресуда прекршајних судова). Институције су радиле свој посао најбоље што су могле.

Никола Марковић, представник Друштва за информатику Србије, истакао је да се предложеним мерама ствара доста озбиљнији правни оквир за развој информационе безбедности, посебно имајући у виду нове ризике који се свакодневно јављају. Поставио је питање за статус самосталних оператора – који су критеријуми да би имао неко тај статус?

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да статус самосталних оператора постоји за оне институције које се баве пословима јавне и националне безбедности. Њихово пословање је другачије у односу на остале органе, и није згодно да Министарство информисања и телекомуникација врши надзор над њима. Опис послова је био главни критеријум за својство самосталних оператора.

Милан Секулоски, Фондација Мрежа за сајбер безбедност, искористио је прилику да похвали уложени напор и рад при изради овог Закона, јер је сам процес био веома инклузиван и укључио је велики број релевантних субјеката и стручњака. Истакао је да имплементација овог прописа остаје отворено питање – основно питање је управљање људским ресурсима (првенствено финансирања стручњака који ће радити у новом телу – Канцеларији за информациону безбедност). Такође, важно је да ново тело буде отворено за сарадњу са локалним стручњацима и изграђује поверење међу грађанима, као и да сарађује са сличним телима у иностранству.

Дарко Шеховић, Удружење банака Србије, поставио је питање о Акту о процени ризика – да ли ће акт бити обавезујући и да ли ће методологија бити обавезна? Истакао је да постоје одређене нејасноће у домену обавештавања (озбиљна претња, инцидент итд).

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да ће акт о процени ризика бити обавезан за све операторе ИКТ система од посебног значаја, али уколико већ постоји неки сличан акт оператори неће бити у обавези да доносе нови (како се не би дуплирао процес). Планирано је доношење уредбе која ће дефинисати шта ће све садржати и обухватати провера ИКТ система. Уколико постоје предлози за прецизирање одређених термина, Министарство је отворено за све предлоге и сугестије.

Ненад Поповић, представник Addiko банке, истакао је да је главна мана предложеног Нацрта закона ограничење које је постављено у погледу инспекције. Улога инспекције не треба да се огледа у само у промовисању коришћења стандарда и процедура, односно у праћењу усклађивања закона, већ и инспекција треба да строжије интервенише. Да ли је могуће прописати минималан ниво стандарда заштите ИКТ система који се мора обезбедити?

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да је предвиђено да се такве мере пропишу само за органе јавне власти. Тренутно слични систем односно минимални

ниво стандарда заштите ИКТ система постоји у неким секторима (финансијском), али може се размотрити да ли исте треба прописати и за још неку област.

Даљих питања није било, те је Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација искористило прилику да се захвали свима који су присуствовали јавној расправи, као на постављеним питањима и датим сугестијама и коментарима. Такође, још једном је истакао да је јавна расправа отворена до 30. августа и позвао све заинтересоване да доставе своје коментаре, мишљења и предлоге.

Округли сто завршен је у 12 часова

Записник саставила:

_____

Невена Антонијевић

Прилог 2: Извештај са округлог стола одржаног у Београду дана 21. августа 2023. године

ЗАПИСНИК СА ДРУГОГ ОКРУГЛОГ СТОЛА У ОКВИРУ ЈАВНЕ РАСПРАВЕ ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

одржаног дана 21. августа 2023. године с почетком у 11:00 часова у Конференцијској сали предузећа eKG Info Data, Краља Петра Првог 23, Крагујевац

Зоран Ђоровић, директор eKG Info Data, пожелео је добродошлицу и захвалио се присутним учесницима округлог стола у оквиру јавне расправе Закона о информационој безбедност испред eKG Info Data и пожелео успешан рад.

Проф. др Анђелка Стојковић, заменица председника Скупштине града Крагујевца, поздравила је присутне у име Града Крагујевца и захвалила се на великом интересовању за овако важну тему. Истакла је да јој је велико задовољство што се други округли сто одржава у Крагујевцу, чиме је посебно истакнута улога Крагујевца у процесу дигитализације и развоја нових ИКТ технологија, Државног дата центра и планиране изградње Иновационог дистрикта.

Јелена Мићић, представница Националне алијансе за економски развој (НАЛЕД) свечано је отворила прву јавну расправу поводом Закона о информационој безбедности при чему је искористила прилику да се захвали свим присутним на великом интересовању за учешће. Истакла је да у изради Нацрта закона о информационој безбедности у оквиру Радне групе за израду Нацрта Закона о информационој безбедности (у даљем тексту: Радна група) учествовао велики број представника из државних органа, привреде, образовних институција, као и представници организација које се баве питањима информационе безбедности. Главни разлог доношења новог Закона о информационој безбедности јесте приближавање домаћег закона правном оквиру Европске уније, односно усклађивање са НИС 2 директивом (2555/2022), усклађивање са Актом о сајбер безбедности ЕУ (2019/881) у делу који се односи на сертификацију у области сајбер безбедности, унапређење институционалног и организационог оквира и капацитета, као и сва даља унапређења текста стечена на темељима досадашњих искуства у примени Закона о информационој безбедности.

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, искористио је прилику и посебно се захвалио представницима Града Крагујевца и предузећа eKG Info Data, као и представницима НАЛЕД-а на подршци која је пружена приликом израде овог Закона. Указао је да је Град Крагујевац изабран са намером, с обзиром на значај и улогу коју има у на овом пољу у Републици Србији и истако је веома драго што види велику заинтересованост за учешће на јавној расправи поводом Закона о информационој безбедности. Како би на што бољи начин презентовао које су то измене које се предвиђају новим Законом о информационој безбедности представио је рад Радне групе која се бавила израдом овог Нацрта закона. Наиме, првобитна идеја била је доношење измена и допуна постојећег Закона о информационој безбедности, али се ипак услед промене већег броја одредби Закона приступило изради новог Закона. Представио је НИС 2 директиву, као и новине у односу на претходну НИС 2 директиву, а које се пре свега односе на класификацију оператора ИКТ система од посебног значаја, јачање улоге ЦЕРТ-ова, јачање казнене политике, увођење нових појмова, израда Националног плана деловања у случају великих инцидената, дељење информација о претњама и инцидентима. Такође, представио је и основна начела новог Закона о информационој безбедности – начело управљања ризиком, начело свеобухватне заштите, начело стручности и добре праксе и начело савести и оспособљености. Указао је да се новим Законом уводи нова подела оператора ИКТ система од посебног значаја и то на приоритетне операторе ИКТ система

од посебног значаја и на важне операторе ИКТ система од посебног значаја, која је усаглашена са поделом из НИС 2 директиве. Државни органи, укључујући органе локалне самоуправе и аутономне покрајине, потпадају под приоритетну категорију, као и сви субјекти којима су поверена јавна овлашћења. Нагласио је да је главна разлика између напред наведене две категорије оператора ИКТ система од посебног значаја у динамици ревизије ИКТ система. С тим у вези, важни оператори ИКТ система од посебног значаја дужни су да врше проверу усклађености својих система једном годишње, док приоритетни оператори ИКТ системи од посебног значаја дужни су да проверу обављају два пута годишње. Даље је представљена категоризација субјеката према напред наведене две категорије, као категоризација органа који потпадају под самосталне операторе ИКТ система и њихове обавезе. Указао је да новим Законом предвиђено да ће оператори ИКТ система од посебног значаја имати дужност да при упису у Евиденцију ИКТ систем од посебног значаја достављају и податке о својим адресама опсега интернет протокола – IP адресе (то је новина коју уводи НИС 2 директива).

Што се тиче одредби које се односе на мере заштите које су оператори ИКТ система од посебног значаја дужни да спроводе није дошло до већих промена, али су уведене неке нове контроле информационе безбедности на основу ИСО 27000 стандарда (који је допуњен крајем прошле године), а које се између осталог односе процедуре за скенирање мреже, информације о рањивостима ИКТ система, ограничење приступа интернет страницама и којих свеукупно има 34. Указао је да једна од битних новина које Закон о информационој безбедности предвиђа увођење обавезе доношења Акта о процени ризика. Заправо идеја је да Канцеларија за информациону безбедност донесе модел акта, који ће послужити операторима приликом доношења својих аката. Такође, поред Акта о процени ризика остала је обавеза доношења Акта о безбедности ИКТ система.

Обавештење о инцидентима који угрожавају информациону безбедност – уведена је обавеза операторима да пријаве инциденте који угрожавају информациону безбедност Националном ЦЕРТ-у, али не пријављују се сви инциденти који се догоде (од овога су изостављене финансијске институције, Кредитни биро и пружаоци услуга повезаних са дигиталном имовином који достављају Народној банци, као и оператори електронских комуникација који то достављају РАТЕЛ-у). У случају да је инцидент везан за кривична дела извештај се доставља МУП-у и јавном тужилаштву, док у случају да је угрожена национална безбедност извештај се доставља Министарству одбране. Законом се јасно наводи које инциденте треба пријавити, али пре свега оне које утичу на велики број корисника, који утичу на рад других оператора ИКТ система, као и оне који доводе до прекида у раду вршења послова и пружања услуга. Нацртом закона о информационој безбедности уводи се и подела инцидената према степену кризе информационе безбедности (веома висок, висок, средњи и низак), при чему се наводи и институција која је надлежна за сваки степен кризе (у случају да је ризик низак, средњи и висок надлежна је Канцеларија за информациону безбедност, а у случају да је веома висок ризик онда је надлежна Влада Републике Србије која проглашава кризу информационе безбедности и задужује органе да поступају у складу са мерама које буде донела). Статистички подаци о инцидентима оператори ИКТ система од посебног значаја достављају податке Националном ЦЕРТ-у најкасније до 28. фебруара текуће године за претходну годину и то

инциденте по типовима, при чему се достављају подаци о свим инцидентима, али не детаљно објашњене већ само бројчано и према типу, степену инцидента.

Новим Законом промењен је институционални оквир, то значи да надлежни орган остаје Министарство информисања и телекомуникација, док послове ЦЕРТ-а државних органа, Националног ЦЕРТ-а (од 1. јануара 2026. године, а до тада их обавља РАТЕЛ) преузима нови орган - Канцеларија за информациону безбедност (јединствена контакт тачка, управља инцидентима, минималним мерама заштите органа), док Министарство одбране остаје надлежно за одобравање криптографских производа који се користе за руковање тајним подацима, дистрибуцију криптоматеријала и заштите од КЕМЗ-а. Представљена је улога Канцеларије за информациону безбедност (у даљем тексту: Канцеларија) која је дефинисана као орган државне управе и која ће обављати послове у складу са прописима које уређују државну управу, а са циљем обављања послова превенције и заштите од безбедносних ризика и инцидената у ИКТ системима у Републици Србији. Надлежност Канцеларије је управљање инцидентима који значајно угрожавају информациону безбедност, обавља послове Националног ЦЕРТ-а (од 1. јануара 2026. године, до тада их обавља РАТЕЛ), обављање послова ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе, обавља сарадњу на националном нивоу у области информационе безбедности, врши послове јединствене тачке контакта, послове стандардизације и сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, прописује минималне мере заштите ИКТ система органа, у сарадњи са надлежним органима учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности у органима, извештава Министарство на кварталном нивоу о предузетим активностима, као и друге послове у складу са овим законом. Такође, биће задужена и за вођење Базе рањивости ИКТ производа и ИКТ услуга – она ће садржати податке о рањивости и податке о ИКТ производима или ИКТ услугама на које рањивост утиче (ближе ће бити регулисано подзаконским актом). Поред заштите мреже електронске управе, Канцеларија ће вршити проактивно скенирање мреже, остваривати међународну сарадњу у области безбедности ИКТ система итд.

Део одредби Закона о информационој безбедности односи се и на безбедност деце на интернету – Национални контакт центар за безбедност деце на интернету који остаје да функционише у оном облику у коме је и деловао до сада. Министарство одбране остаје надлежно за криптобезбедност и заштиту од КЕМЗ-а, а представљене су његове функције у овој области попут вршења функције националног органа за одобравање криптопроизвода и заштиту од КЕМЗ-а, развоја, имплементирања, верификације и класификације криптографске производе и алгоритме и производе и решења заштите од КЕМЗ-а итд. Део нацрта Закона који дефинише шта су тајни подаци у ИКТ системима, уз навођење изузетка, самосталних оператора, који имају опште овлашћење и није им потребна дозвола. Инспекција за информациону безбедност остаје у саставу Министарства информисања и телекомуникација, али с обзиром да већ постоји Закон о инспекцијском надзору, Закон не уводи неке новине, већ само прецизира и појашњава одређене одредбе. Једна од новина у овом домену јесте могућност да инспектори наложе да надзирани субјекат учини доступним јавности информације које се тичу непоштовања одредби овог Закона. Подзаконски акти који регулишу ову област биће донети у року од шест месеци

од дана ступања на снагу овог Закона. На крају указао је да даном ступања на снагу овог закона престаје да важи Закон о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19), изузев одредби које се односе на обавезе оператора ИКТ система од посебног значаја које важе до доношења подзаконског акта из члана 6. овог закона. Након завршене презентације одредби новог Закона о информационој безбедности позвао је све присутне да поставе питања.

Ненад Филиповић, ректор Универзитета у Крагујевцу, поставио је питање у вези улоге академске заједнице у процесу имплементације Закона о информационој безбедности, односно каква је улога академске заједнице у делу едукације?

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација, истакао је да су научно-истраживачке организације оператори ИКТ од посебног значаја, али потребно је донети уредбу која ће ближе дефинисати критеријуме и њихову улогу. Научно-истраживачке институције и академска заједница имају веома важну улогу, претходних година је била организовано такмичење „Сајбер херој“, министарство ће у наредном периоду организовати сличне активности.

Даљих питања није било, те је Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација искористило прилику да се захвали свима који су присуствовали јавној расправи, као на постављеним питањима и датим сугестијама и коментарима. Такође, још једном је истакао да је јавна расправа отворена до 30. августа и позвао све заинтересоване да доставе своје коментаре, мишљења и предлоге.

Округли сто завршен је у 12 часова.

Записник саставила:

_____

Невена Антонијевић