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: 011-6020/2024 од 2. јула 2024. године, којим се одређује спровођење јавне расправе о Нацрту закона о информационој безбедности у периоду 3. јула до 23. јула 2024. 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 округлог стола путем видео конференцијске везе у Београду дана 17. јула 2024. године.

У току јавне расправе, прикупљене су иницијативе, коментари и сугестије од заинтересованих лица. 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, 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 унети у текст из једног од следећих разлога: опште су 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, или 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 налази се и записник са одржаног округлог стола.

Део или делови материјала на које се коментар односи	Учесник или група учесника који упућује коментар	Примљени коментар	Одговор предлагача и образложење
Члан 1.	Cedars International doo	**Коментар:** Чланом 1. се није дефинисао предмет примене, односно да ли је закон намењен искључиво институцијама у државном сектору или се ради и о јавним предузећима као и физичким лицима. Обзиром да се преостали део закона фокусира на тему сигурности ИКТ оператора од посебног значаја, савет је да се, назив закона, његов први члан или преостали садржај измене. Чак и у ситуацијама где би се закон применио искључиво на организације унутар државних структура то не би смело да искључи друштва или лица са којима ове организације раде.	**Одговор на коментар:** Чланом 1. Нацрта закона о информационој безбедности дефинисан је предмет уређивања, обухватајући све субјекте који управљају и користе информационо-комуникационе системе. Овим законским решењем није ограничен домен примене на институције државног сектора, већ се примењује и на јавна предузећа, као и на друга правна и физичка лица која спадају у оквир надлежности овог закона. Како се остатак закона фокусира на мере и поступке за унапређење општег нивоа информационе безбедности, укључујући и операторе ИКТ система од посебног значаја, закон пружа свеобухватни оквир који укључује и друштва или лица са којима наведене организације сарађују. У овом контексту, законом су

			прописани стандарди и одговорности који су обавезујући за све релевантне субјекте. Сматрамо да су назив закона и његов први члан формулисани тако да обухвате све категорије субјеката и информационо-комуникационих система на које се закон односи, омогућавајући његову правилну и свеобухватну примену. Из ових разлога, предлог за измену није прихваћен.
Члан 1.	Национална алијанса за локални економски развој	**Коментар 1**: Члан 1. став 1. – предлажемо да се реч „субјекат“ (у делу „одговорности субјеката приликом управљања…“) замени низом речи „државних субјеката и правних лица“. **Коментар 2**: Члан 1. став 1. – предлажемо да се реч „субјекат“ (у делу „као и надлежности субјекта за надзор над спровођењем овог закона“) избрише јер је сувишна реч.	**Одговор на коментар 1**: Предлог да се реч „субјекат“ замени речима „државних субјеката и правних лица“ није прихваћен, с обзиром на то да би таква измена сузила обим примене закона. Употреба термина „субјекат“ одабрана је како би се обухватили сви релевантни ентитети, укључујући државне органе, правна лица, као и физичка лица. Оваква формулација омогућава свеобухватност и флексибилност у примени закона, избегавајући потенцијалне правне празнине које би могле настати у

			случају ограничења опсега примене само на државне субјекте и правна лица. Стога, ради очувања интегритета и обухватности законског оквира, предложена измена није прихваћена. **Одговор на коментар 2:** Реч „субјекат“ је употребљена са циљем да обухвати све релевантне актере који могу имати надлежност за надзор, укључујући разне институције и органе. Брисање овог термина би могло створити неодређеност у погледу субјеката који су овлашћени за надзор, чиме би се угрозила јасност и ефикасност спровођења законских одредби. Сходно томе, ради очувања прецизности и свеобухватности законског текста, предлог није прихваћен.
Члан 2.	РАТЕЛ -Национални ЦЕРТ-	**Коментар:** Став 1. тачка 17) дефинисан је појам „управљање одговором на инцидент“ који сматрамо да је неадекватан, не само због неадекватног превода већ због радњи које дефиниција обухвата, а које се предузимају од стране различитих организација и не могу се сврстати у одговор на инцидент. У	**Одговор на коментар:** Предлог да се термин „управљање одговором на инцидент“ замени термином „управљање инцидентом“ није прихваћен, јер би таква измена била концептуално и оперативно

		пракси су у употреби појмови *incident response* и *incident handling.* Предлог је да се врати на претходну верзију појма „управљање инцидентом“. Коментар: Упоредна пракса: У хрватском закону је дефинисан појам ,.поступање с инцидентом“.	неоснована. Термин „управљање одговором на инцидент“ је одабран као најпрецизнији израз који обухвата свеобухватни скуп активности које се предузимају у контексту управљања безбедносним инцидентима у складу са међународним стандардима и најбољим праксама. Појмови „incident response“ и „incident handling“ имају различита значења и примену у пракси, где „incident response“ обухвата брз и организован одговор на инциденте са циљем минимизације штете, док „incident handling“ укључује шири спектар активности укључујући превенцију, детекцију, одговор и опоравак. Стога, коришћење термина „управљање одговором на инцидент“ прецизно одражава неопходност систематског приступа у одговору на инциденте, док предложена замена појма „управљање инцидентом“ не би адекватно обухватила све кључне аспекте који су предмет овог закона.

			Додатно, коментар који се односи на упоредну праксу са хрватским законом није од значаја будући хрватски закон има различит концептуални оквир и нормативне основе. Приликом израде овог закона, имали смо у виду специфичне потребе и контекст Републике Србије, као и релевантне међународне стандарде, како би се обезбедила највиша могућа ефикасност у управљању безбедносним инцидентима. Иако упоредна пракса може понекад бити корисна, у овом случају није пресудна. Свака држава прилагођава своје законодавство специфичним потребама и контексту, па тако и терминологија треба да одражава те специфичности. С обзиром на све наведено, предлог за измену термина није прихваћен.
Члан 2.	Национална алијанса за локални економски развој	**Коментар 1:** Тачка 11) Управљање ризиком – предлажемо да се измени делимично измени дефиниција, тако да се додају речи „идентификација“ и „успостављање система“ и да дефиниција гласи: управљање ризиком је скуп	**Одговор на коментар 1:** Предлог се усваја. **Одговор на коментар 2:** Чланом 2. тачком 12) дефинисан је појам „избегнути инцидент“:

		систематичних активности идентификације, процене и успостављање система контроле ризика који омогућава планирање, организовање и усмеравање мера заштите како би се обезбедило да ризици остану у прописаним и прихватљивим оквир. **Коментар 2:** Тачка 12) Избегнути инцидент, члан 7 тачка 9) и члан 25 – потребно је појаснити на шта се тачно мисли када се говори о избегнутом инциденту. **Коментар 3:** Члан 2 тачка 15) Инцидент – предлажемо да се редефинише појам инцидента будући да тренутна дефиниција – „догађај који угрожава“ може нашироко да се схвати. Наш 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. **Коментар 4:** Тачка 31) Безбедносна зона - Предлажемо да дефиниција безбедносне зоне обухвати зоне чије би нарушавање физичке безбедности изузетно лоше утицало на очување информационе безбедности ИКТ система	избегнути инцидент представља сваки ризичан догађај који је могао угрозити расположивост, аутентичност, интегритет или поверљивост података који се чувају, преносе или обрађују у ИКТ систему или услуга које се пружају путем ИКТ система или којима се омогућава приступ ИКТ систему, али је успешно спречен или се није остварио. Термин „избегнути инцидент“ означава ризичан догађај који је могао угрозити безбедност података или ИКТ система, али је успешно спречен или није довео до штете. То укључује ситуације као што су блокирани сајбер напади, брзо отклоњене рањивости или неуспели покушаји неовлашћеног приступа. Овај термин наглашава важност проактивног управљања безбедносним ризицима, где се претње идентификују и решавају пре него што постану стварни инциденти. **Одговор на коментар 3:** Предлог да се редефинише појам „инцидент“ у члану 2. тачка 15) није прихваћен. Тренутна

		(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.	дефиниција која обухвата сваки „догађај који угрожава“ расположивост, аутентичност, интегритет, непорецивост или поверљивост података, има за циљ да обезбеди свеобухватан приступ управљању инцидентима у ИКТ системима. Оваква дефиниција омогућава правовремену идентификацију и обраду догађаја који могу представљати потенцијалну претњу, чак и ако у првом тренутку нису довели до „стварног негативног утицаја“. Фокусирање искључиво на последице инцидента, како је предложено у коментару, могло би ограничити превентивне мере и резултирати пропуштањем важних сигнала који указују на могуће угрожавање безбедности система. Осим тога, тренутна дефиниција је усклађена са НИС2 директивом, међународним стандардима и добром праксом у области информационе безбедности, која наглашава значај проактивног приступа

			у управљању безбедносним догађајима. Сужење дефиниције на догађаје са већ остваренимнегативним утицајем не би одговарало савременим захтевима за информациону безбедност и могло би ослабити ефикасност система за управљање инцидентима. **Одговор на коментар 4:** Предлог је усвојен.
Члан 2.	А1	**Коментар :** Члан 2. став 1. тачка 12) који уређује појам избегнутог инцидента и чланом 25. став 1. који прописује обавезу достављања статистичких података о инцидентима (који укључују и избегнуте инциденте), предлажемо да се изврши прецизирање избегнутих инцидената за које постоји обавеза статистичких података на годишњем нивоу у самом закону или подзаконском акту. Коментар: Наведено прецизирање се предлаже како би се појасниле ове одредбе и обезбедила њихова уједначена примена од стране свих оператора ИКТ система од посебног значаја, имајући у виду да се у пракси може десити ситуација да постоји велики број избегнутих инцидената на дневном нивоу (нпр.phishing мејлови који добијају запослени или	**Одговор на коментар**: Предлог се усваја. Сматрамо да је најцелисходније да се ово питање детаљно уреди путем подзаконског акта, где ће бити прецизирани критеријуми за идентификацију и извештавање о избегнутим инцидентима. На овај начин ће се обезбедити флексибилност и прилагођеност регулативе стварним потребама и капацитетима оператора, уз поштовање принципа сразмерности. Узимајући у обзир важност овог питања, предложена измена ће бити размотрена у

		неких покушаја напада које сами системи спречавају у склопу примене одговарајућих техничким мера-нпр.firewall и антивирус софтвери) те је из тог разлога потребно детаљније прецизирати које врсте избегнутих инцидента потпадају под обавезу достављања података на годишњем нивоу у статистичке сврхе, при чему је потребно узети у обзир сразмерност тих обавеза у погледу ангажовања капацитета оператора ИКТ система од посебног значаја приликом достављања тих података.	оквиру израде одговарајућег подзаконског акта.
Члан 2.	Cedars International doo	**Коментар 1:** Увођење нове терминологије, допуна (велики број предлога у зависности од измене првог члана). Сајбер криминал је било која незаконита активност која се изводи преко информационо-комуникационих система. **Коментар 2:** Сајбер тероризам је коришћење информационо-комуникационих система за извршавање терористичких активности, које укључују претње или нападе на рачунарске мреже с циљем изазивања страха, економске штете или политичких притисака. **Коментар 3:** Малвер (Malicious Software) је злонамерни софтвер који је дизајниран да оштети, поремети или неовлашћено приступи информационо-	**Одговор на коментар 1 и 2:** Предлог се не прихвата, будући да се ради о појмовима који се не односе на претежну материју овог закона, већ закона из кривично-правне области. **Одговор на коментар 3:** Предлог је прихваћен, с тим што је уместо термина „малвер“употребљен термин злонамерни „софтвер“. **Одговор на коментар 4:** Предлог није прихваћен будући да је дефиниција физичке сигурности већ обухваћена постојећим законским оквиром и прописима

		комуникационим системима, укључујући вирусе, тројанце, црве, рансомware и спywаре. **Коментар 4:** Физичка сигурност обухвата све мере заштите које се односе на физичку заштиту информационо-комуникационих система, укључујући контролу приступа, заштиту опреме и сигурност објеката у којима се налази опрема. **Коментар 5:** Инцидент информационе безбедности је било који догађај који угрожава или има потенцијал да угрози поверљивост, интегритет или доступност информационо-комуникационих система. **Коментар 6:** Опоравак од катастрофе (Disaster Recovery) су планови и процедуре које се примењују за повратак информационо-комуникационих система у оперативно стање након озбиљног инцидента или катастрофе. **Коментар 7:** Оператор ИКТ система - Изменити	који регулишу област информационе безбедности. Физичка сигурност као концепт подразумева заштиту од физичких претњи, укључујући контролу приступа објектима и опреми, као и мере заштите саме опреме. Ове мере су већ обухваћене постојећим правним актима и не захтевају додатно дефинисање у овом Закону. **Одговор на коментар 5:** Сматрамо да је постојећа законска дефиниција „инцидента“ довољно прецизна и свеобухватна, те није утврђена потреба за изменама. **Одговор на коментар 6:** Предлог се одбија јер се дефинисањем овог термина у Закону може смањити флексибилност и организација у примени мера у складу са њиховим специфичним потребама. Сматрамо да је ово питање боље регулисати на нивоу подзаконских аката или интерних политика. **Одговор на коментар 7:**

			Није предложено на који начин је потребно изменити дефиницију.
Члан 3.	Cedars International doo	**Коментар:** Додати начело континуираног побољшања Увођење начела које наглашава стално побољшање мера информационе безбедности може додатно осигурати да систем остане робустан пред новим претњама.	**Одговор на коментар:** Предлог се усваја.
Члан 5.	РАТЕЛ Национални ЦЕРТ	**Коментар:** С обзиром да Нацрт садржи нове области, односно да је било допуне у односу на претходну верзију Нацрта, предлажемо да се у ИКТ системе од посебног значаја уврсти и медијски јавни сервис Србије, сматрамо да би требало да буде оператор приоритетних ИКТ система, у оквиру прве групе ових оператора и у оквиру осталих области члана 5. став 2, тачка 1) подтачка (9). Коментар: Упоредна пракса: Естонија је свој јавни сервис уврстила у ИКТ системе од посебног значаја.	**Одговор на коментар:** Предлог је детаљно размотрен и имајући у виду циљеве и начела НИС2 директиве, са којом се овај закон усаглашава, а у чијем обухвату се не налазе јавни медијски сервиси, предлог није прихваћен.
Додавање новог члана 5.	Национална алијанса за локални економски развој	**Коментар:** Додавање новог члана 5. Родна равноправност, који ће гласити: „Државни субјекти и правна лица на која се овај закон односи обезбеђују примену политика једнаких могућности и унапређења родне равноправности и доприносе уклањању родних стереотипа приликом остваривања права и обавеза лица оба пола у складу са	**Одговор на коментар:** Закон о информационој безбедности примарно је усмерен на техничке, организационе и безбедносне аспекте заштите ИКТ система, који су од критичног значаја за функционисање друштва и економије.

		законом који уређује родну равноправност у области одбране и безбедности, као и у области информационо-комуникационих технологија и информационог друштва“	Додавање одредби о родној равноправности у овај закон, иако важно у ширем друштвеном контексту, није у директној вези са основним циљевима и тематиком закона. Питања родне равноправности су већ адекватно регулисана Законом о родној равноправности, који пружа свеобухватан правни оквир за њихово остваривање и унапређење у свим секторима, укључујући и област одбране, безбедности и информационих технологија. С обзиром на то, сматрамо да би уношење овакве одредбе у Закон о информационој безбедности могло довести до правне дупликације.
Члан 5.	Српске кабловске мреже SBB	Став 8. на које конкретно управљане безбедносне услуге се мисли под ставом “пружање управљаних безбедносних услуга“? Како би се знало на које конкретно субјекте се мисли, неопходно је детаљано објашњење појма пружања безбедносних услуга.	Термин „управљане безбедносне услуге“ у члану 5, подтачка 8) , са намером је постављен широко како би обухватио различите врсте услуга које могу бити потребне у зависности од специфичних потреба оператора ИКТ система од посебног значаја. Ова флексибилност омогућава операторима да

			ангажују различите врсте безбедносних услуга, у складу са актуелним стандардима и праксама у области информационе безбедности, и да их прилагоде специфичним ризицима са којима се суочавају. Сматрамо да тренутна формулација пружа довољну јасноћу, а додатно прецизирање би могло ограничити способност оператора да у потпуности прилагоде своје мере заштите конкретним потребама и претњама. Стога, предлог за детаљно објашњење појма „управљане безбедносне услуге“ није прихваћен.
Члан 6.	А1	**Коментар:** У вези са ставовима 3.и 4. којима се уређују оператори приоритетних и важних ИКТ система од посебног значаја предлажемо да се у правни основ за доношење подзаконског акта из става 3. члана 6. којим Влада, на предлог министарства надлежног за послове информационе безбедности, ближе уређује услове, опште и секторске критеријуме и подсекторксе прагове за одређивање оператора из члана 5.и 6. овог закона, као и процедуру идентификовања и одређивања оператора ИКТ система од посебног значаја	**Одговор на коментар:** У вези са ставовима 3.и 4. члана 6. којима се уређују оператори приоритетних и важних ИКТ система од посебног значаја сматрамо да је најцелисходније да се детаљно прецизирање обави кроз подзаконске акте, који ће омогућити већу флексибилност и прилагођавање променљивим околностима у технолошком и привредном окружењу.

		допуни тако да се пропише да подзаконски акт који дефинише операторе ИКТ система од посебног значаја садржи и шифре делатности под које потпадају оператори приоритетних и важних ИКТ система од посебног значаја. Коментар: Наведена допуна члана се предлаже у циљу ближег дефинисања делатности које обављају оператори ИКТ система од посебног значаја и отклањања недоумица у примени будућег закона у погледу тумачења да ли неки правни субјект обавља делатност због које се сматра оператором ИКТ система од посебног значаја или не.	Законом је обезбеђен основни оквир за дефинисање оператора приоритетних и важних ИКТ система од посебног значаја, док ће се подзаконским актима ближе уредити услови и критеријуми за њихово одређивање. Овим приступом се омогућава да се у подзаконским актима, у зависности од потреба и развоја у различитим секторима, прецизирају све релевантне категорије и делатности без ограничења која би могла проистећи из преуских законских дефиниција. Укључивање шифри делатности директно у закон могло би ограничити прилагодљивост правног оквира, што је од кључног значаја у области информационе безбедности, где се ризици и технологије брзо развијају. Подзаконски акти ће, са друге стране, пружити могућност за ажурирање и прецизирање на начин који најбоље одговара актуелним потребама и изазовима, без потребе за изменама самог закона.

			Стога, сматрамо да је предложени правни оквир који омогућава детаљније уређење путем подзаконских аката најадекватнији приступ, те предлог за укључивање шифри делатности у сам текст закона није прихваћен.
Члан 7.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Сматрамо да је увођење обавезе приоритетним операторима ИКТ система од посебног значаја да два пута годишње врше проверу усклађености мера заштите ИКТ система није заснован на искуству из праксе и да ће ово представљати велики терет за њих. Сматрамо да је целисходније и корисније предвидети минимум мера заштите које приоритетни оператори ИКТ система од посебног значаја треба да примене. Коментар: Упоредна пракса: у Хрватској „кључни субјекти“ спроводе проверу једном у две године или када им надлежно тело затражи.	**Одговор на коментар:** Сматрамо да је обавеза спровођења провере два пута годишње неопходна и оправдана, нарочито у светлу све веће сложености и динамике сајбер претњи. Примарни разлог за ову обавезу је потреба за сталним одржавањем и ажурирањем мера заштите, како би се осигурало да приоритетни ИКТ системи од посебног значаја остају отпорни на нове и еволуирајуће сајбер претње. Сајбер претње се развијају брзо, а промене у технолошком свету захтевају континуирано прилагођавање безбедносних мера. Додатно, одлука о фреквенцији провера заснива се на најбољим праксама у области

			информационе безбедности, које препоручују редовно и систематско проверавање примене безбедносних мера, како би се благовремено уочили и отклонили евентуални пропусти. Примена оваквог приступа омогућава не само реактивно, већ и проактивно управљање ризицима, што је од кључног значаја за очување стабилности и сигурности критичних инфраструктура. Минимум мера заштите, иако важан као полазна основа, сам по себи није довољан за осигурање свеобухватне безбедности. Без редовних и детаљних провера усклађености, постоји ризик да ове мере не буду адекватно имплементиране, што би могло довести до озбиљних последица по функционисање система. Потреба за честим провером усклађености такође произлази из обавезе да се осигура високи ниво поузданости и интегритета ових система, који имају кључну улогу у одржавању критичних друштвених и

			економских активности. С обзиром на све наведено, сматрамо да је задржавање обавезе двоструке годишње провере усклађености оправдано и неопходно ради осигурања континуитета и ефикасности мера заштите. Стога, предлог за смањење учесталости провера није прихваћен, јер би могао угрозити сигурност и стабилност ИКТ система од посебног значаја.
Члан 7.	Српске кабловске мреже SBB	**Коментар:** У ставу 5. предлаже се да вршење провере усклађености мера заштите ИКТ система које се примењује актом о безбедности ИКТ система и то најмање: -једном годишње ако је оператор приоритетног ИКТ система од посебног значаја; - једном у две године ако је оператор важног ИКТ система од посебног значаја.	**Одговор на коментар:** Чланом 7. ставом 1. тачком 5) подтачком (1) и (2) предвиђено је да оператор ИКТ система од посебног значаја, сходно овом закону, у обавези је да 5) врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система и то најмање: (1) два пута годишње ако је оператор приоритетног ИКТ система од посебног значаја (2) једном годишње ако је оператор важног ИКТ система од посебног значаја;

			Учесталост провера, како је дефинисана у закону, осигурава да су безбедносне мере увек усклађене са најновијим стандардима и ризицима. За приоритетне ИКТ системе, чешће провере два пута годишње су неопходне због њиховог критичног значаја. Смањење учесталости провера могло би угрозити способност ових система да се адекватно одбране од све сложенијих сајбер претњи. Стога, задржавање предложене учесталости провера у закону сматрамо неопходним за очување високог нивоа информационе безбедности, и предлог за њихово смањење није прихваћен.
Члан 7.	А1	**Коментар 1:** Преформулисати тачку 7) став 1. тако да гласи: “7) доставља обавештења, без одлагања, о сваком инциденту који значајно нарушава безбедност ИКТ система од посебног значаја“, а из разлога дефинисања члана 13.закона и како би у потпуности било јасно шта се доставља од података. **Коментар 2:** Тачка 8) став 1. предвиђа да оператор ИКТ система од посебног значаја доставља	**Одговор на коментар 1:** Предлог се усваја. **Одговор на коментар 2:** Дефиниција озбиљне претње, како је већ предвиђена чланом 2. ставом 1. тачком 14), довољно је прецизна и свеобухватна да омогући правилну примену закона. Дефиниција озбиљне претње већ обухвата кључне елементе,

		обавештења о озбиљним претњама за ИКТ систем од посебног значаја. Ова новоуведена обавеза за операторе ИКТ система од посебног значаја ствара недоумицу за операторе ИКТ система од посебног значаја шта се стварно сматра озбиљном претњом да би се пријавило, те предлажемо детаљније дефинисање кроз закон или подзаконски акт увођењем квалитативног или квантитативног критеријума.	укључујући техничка својства претње и њен потенцијал да изазове значајне негативне последице по ИКТ систем, оператора или кориснике услуга, укључујући материјалну и нематеријалну штету. Овај опис пружа довољно јасноће да оператори могу идентификовати и пријавити претње које испуњавају наведене критеријуме. Увођење квалитативних или квантитативних критеријума могло би довести до непотребне крутости у примени закона и ограничити способност оператора да процене и реагују на различите и брзо променљиве претње у сајбер простору. Закон је намерно оставио простор за флексибилност у тумачењу и пријављивању озбиљних претњи, омогућавајући операторима да примене најбоље праксе у процени ризика. Стога, сматрамо да је постојећа дефиниција адекватна и да омогућава правилну примену закона, те предлог за детаљније дефинисање озбиљне

			претње није прихваћен.
Члан 8.	Национална алијанса за локални економски развој	**Коментар:** Став 1 тачка 4) – предлажемо да се дефинише максимални период у ком је потребно извршити бар једну проверу, па би реченица требало да гласи: „врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система у складу са сопственим правилима за проверу усклађености мера заштите, а најмање једном годишње“	**Одговор на коментар:** Предлог се усваја.
Члан 10.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Нема јасне одредбе да су оператори ИКТ система од посебног значаја у обавези да примене мере заштите.	**Одговор на коментар:** Обавеза оператора ИКТ система од посебног значаја да примене мере заштите већ је јасно дефинисана чланом 7. став 1. тачка 2) којим је прописано да је оператор ИКТ система од посебног значаја дужан да предузме одговарајуће техничке, оперативне, организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидената, као и чланом 10. ставом 1. којим се изричито наводи да оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и

			предузимање мера заштите ИКТ система. Ова формулација недвосмислено указује на обавезу примене мера заштите у складу са законом. Додатно, мере заштите које су наведене у члану 10. обухватају широк спектар активности које оператори морају предузети како би осигурали безбедност својих ИКТ система. У том смислу, сматрамо да нема потребе за додатним прецизирањем, јер је обавеза примене мера заштите јасно наглашена. Стога, предлог за додатно појашњење није прихваћен.
Члан 10.	Национална алијанса за локални економски развој	**Коментар 1:** Став 3. Предлажемо да се код мера заштите ИКТ система од посебног значаја дода и мера која ће гласити: „обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу“ **Коментар 2:** Став 3 тачка 1) предлажемо да се у наведену меру заштите додају речи „знања, компетенција и искуства“, па би онда цела реченица гласила: „успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством и одговорностима запослених, којом се остварује управљање информационом	**Одговор на коментар 1:** Предлог се усваја. **Одговор на коментар 2:** Предлог се усваја. **Одговор на коментар 3:** Предлог се усваја. **Одговор на коментар 4:** Предлог се усваја.

		безбедношћу у оквиру оператора ИКТ система“. **Коментар 3:** Став 3 тачка 4) Предлажемо да се у наведену меру заштите дода још један део који се тиче обучавања запослених, тако да гласи: „обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност, односно да обезбеди одржавање основних и по потреби напредних информатичких обука за све запослене и ангажована лица која имају приступ ИКТ системима, као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедности ради обезбеђивања континуиране едукације.“ **Коментар 4:** Став 3 тачка 25) Предлажемо брисање ове тачке, јер сматрамо да није у складу са НИС2 директивом. Уколико брисање није могуће, предлажемо да се она преформулише на следећи начин како би била у складу са ISO стандардом 27001 (2022) контролним циљем A8.34 : „обезбеђивање заштите ИКТ система приликом спровођења ревизорског тестирања“.	
Члан 10.	Удружење интерних ревизора Србије	**Коментар 1:** Како бисмо избегли потенцијално погрешно тумачење члана 10, тачке 25. у предлогу закона, на начин да се тумачи као основ за одбијање сарадње са	**Одговор на коментар 1:** Предлог се усваја. **Одговор на коментар 2:**

		интерним и екстерним ревизорима, што би могло негативно утицати на квалитет и ефикасност ревизорских процеса унутар организација, предлажемо прецизирање ове тачке. Ради унапређења рада интерне и екстерне ревизије и обезбеђивања транспарентности и одговорности у пословању наших компанија, сматрамо да је неопходно изменити формулацију члана 10, тачка 25 предлога закона, на начин да гласи: „Обезбеђивање заштите информационог система током ревизорског тестирања.“ Овај предлог је у складу са најбољом праксом и међународним стандарима, као што су ИСО 27001:2022 А8.34, који наглашавају значај заштите информационих система и безбедности података током ревизорских активности. **Коментар 2:** Такође, предлажемо додавање новог члана у Закон о информационој безбедности, који ће јасно дефинисати улогу интерне ревизије информационих система. Нови члан би могао гласити: „Интерна ревизија информационог система треба да се спроводи редовно и у складу са Глобалним Стандардима интерне ревизије, како би се обезбедила ефикасност, безбедност и усклађеност информационих система са регулативом, интерним актима и најбољим праксама	Начин вршења ревизије биће регулисан подзаконским актом.

		у области интерне ревизије информационих система.“ Коментар: С обзиром на савремене услове пословања и сталне промене у окружењу, ризици информационих система постају све израженији и кључни за одржавање високог нивоа безбедности и поузданости информација. Наше Удружење, као афилијација Међународног института интерних ревизора (IIA) и чланица Европске конфедерације интерних ревизора (ECIIA), прати водеће светске праксе у области интерне ревизије и сматра да је ова измена неопходна за унапређење укупне информационо-безбедносне инфраструктуре и усклађивање са међународним стандардима. Ове измене ће омогућити интерним ревизорима да ефикасно спроводе своје активности, у складу са међународно признатим стандардима и најбољим праксама, без препрека и ризика погрешног тумачења, док ће истовремено обезбедити да послодавци испуњавају своје обавезе у складу са законом и међународним стандардима.	
Члан 10.	“Advanced Cyber Security doo”, Београд Бранислав Добросављевић	**Коментар:** Мере заштите ИКТ система од посебног значаја, треба допунити текстом који ће, у складу са НИС2 директивом, обухватити и прецизно дефинисање интерне одговорности за спровођење мера заштите, што се експлицитно односи на директора, односно	**Одговор на коментар:** У вези са предлогом за допуну мера заштите ИКТ система у складу са НИС2 директивом, конкретно прецизно дефинисање интерне одговорности за спровођење мера заштите која обухвата

		највише руководиоце оператера („management body“ у Директиви). Предлог члана: За спровођење мера заштите ИКТ система, односно за управљање безбедносним ризицима ИКТ система, у складу са овим законом, одговорни су директори, односно чланови највиших органа управљања Оператора приоритетних и важних ИКТ система од посебног значаја, односно руководиоци органа државне управе, других државних органа и извршних органа локалне и регионалне самоуправе. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Мере заштите ИКТ система се односе на: 1) успостављање организационе структуре, ... итд, без измена Коментар: Текст би се могао убацити и на друго место, на пример после 2. става или на сам крај овог члана Закона.	највише руководиоце, сматрамо да је овај предлог у основи усклађен са принципима побољшања безбедности. Међутим, треба имати у виду да је постојећи правни оквир (други важећи пропис који регулишу одговорности у случају већ обухватио одговорност руководства кроз дефинисане мере и процедуре које осигуравају безбедност ИКТ система. Допуњавање текста на предложени начин могло би додатно осигурати јасније утврђивање одговорности, али је важно да се при уношење оваквих измена обезбеди њихова хармонизација са већ постојећим правним прописима и организационим структурама.
Члан 11. и 12.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Остаје нејасан однос Акта о процени ризика и Акта о безбедности, односно требало би јасно указати да Акт о процени ризика претходи Акту о безбедности, односно да се	**Одговор на коментар:** Предлог се усваја.

		примена мера заштите заснива на процењеном ризику.	
Члан 12.	Национална алијанса за локални економски развој	**Коментар:** Став 5 - предлажемо да се дода део реченице којим ће се оператори обавезати да достављају извештаје надлежном органу (Канцеларији за информациону безбедност). У том случају реченица би требала да гласи: „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, а један примера извештаја достави надлежном органу“. Став 6 – уколико се коментар изнад прихвати, онда би требало изменити и став 6 тако да гласи: „Подзаконски акт којим се уређује ближе садржај акта о безбедности, начин провере ИКТ система од посебног значаја и садржај извештаја о провери, као и достављање извештаја надлежном органу, доноси Влада на предлог Министарства“.	**Одговор на коментар:** Закон већ предвиђа механизме контроле и надзора над операторима кроз редовне провере и извештавање које су примерене безбедносном ризику. Увођење додатне обавезе достављања извештаја би дуплирало већ постојеће процедуре, што није неопходно.
Члан 13.	РАТЕЛ Национални ЦЕРТ	**Коментар:** С обзиром да се у члану 13. разрађују обавезе оператора ИКТ система од посебног значаја да доставе обавештење и о избегнутим инцидентима, а не само о инцидентима који значајано нарушавају информациону безбедност, прикладнији назив члана је „обавеза извештавања о инцидентима“. Коментар:	**Одговор на коментар:** Након детаљног разматрања, одлучено је да се не прихвати предлог о промени назива члана 13. Назив „Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност“ остаје

		Упоредна пракса: у Хрватској се избегнути инциденти пријављују на добровољној основи.	примерен и усклађен са међународним стандардима и најбољим праксама у управљању информационом безбедношћу. Међународни стандарди као што су ISO/IEC 27001 и ISO/IEC 27005 наглашавају важност пријављивања инцидената који могу угрозити интегритет, доступност и поверљивост информационих система. Обавеза пријављивања избегнутих инцидената има значајну улогу у управљању ризицима, јер омогућава рано идентификовање претњи и слабих тачака које би могле довести до озбиљнијих последица у будућности. У складу са НИС 2 директивом Европске уније, која поставља строге захтеве за информациону безбедност, државе чланице су дужне да осигурају да оператери основних услуга и провајдери дигиталних услуга пријављују инциденте који имају значајан утицај на услуге које пружају. НИС 2 директива такође предвиђа јачање

			превентивних мера и увођење обавеза пријављивања избегнутих инцидената, јер они могу бити индикатори нових претњи или слабости у системима. Овај приступ повећава ниво свести и безбедности на нивоу целог система, што је и сврха овог члана. Док је у неким државама, као што је Хрватска, пријављивање избегнутих инцидената на добровољној основи, Република Србија се определила за другачији приступ. Ово усклађивање са НИС 2 директивом и међународним стандардима представља кључни корак ка јачању националног оквира за информациону безбедност и смањење ризика од будућих инцидената. Из тих разлога, назив члана 13. који наглашава значајне инциденте је адекватан и покрива целокупан спектар инцидената који могу утицати на информациону безбедност, укључујући и обавезу пријављивања избегнутих инцидената као важан

			део превентивне стратегије.
Члан 14.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Сматрамо да ће примена одредбе члана 14. став 8. бити веома проблематична у пракси јер је реч о тајним подацима што захтева дефинисање безбедних начина коришћења, размене и чување ових података, као и довољан број запослених у свим релевантним институцијама који су сертификовани за приступ тајним подацима.	**Одговор на коментар:** Члан 14. нема став 8.
Члан 17.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Сматрамо да је потребно предвидети стално усавршавање чланова оперативног тима и дефинисати да ће Канцеларија донети критеријуме за именовање у овај тим.	**Одговор на коментар:** Усвојен је предлог који се односи на дефинисање критеријума за именовање чланова у оперативни тим. У вези са предлогом да се предвиди обавеза сталног усавршавања чланова оперативног тима указујемо да је законом већ предвиђен оквир за континуирано и професионално усавршавање чланова оперативних тимова кроз постојеће прописе и интерне процедуре оператора. Обавеза сталног усавршавања је већ имплицитно укључена као део одговорности оператора за одржавање и унапређење информационе безбедности.

Члан 18.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Влада доноси План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности, али нема дефинисаног рока у ком ће Влада донети овај План. Коментар: Упоредна пракса: хрватски закон предвиђа да Влада донесе и Акт о стратешком планирању, док се за управљање кризама доноси национални програм за управљање кризама информационе безбедности.	**Одговор на коментар:** Желимо да истакнемо да министарство пажљиво прати упоредно-правну праксу у области информационе безбедности, укључујући примере добре праксе из других земаља. У овом контексту, већ смо у Нацрту закона о информационој безбедности предвидели механизам који осигурава да Влада донесе План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности у разумном року. Тиме се обезбеђује ефикасност и благовременост у реаговању на потенцијалне кризне ситуације, у складу са најбољим праксама и примерима из упоредног права. Поред тога, министарство је посвећено континуираном унапређењу законодавства, узимајући у обзир специфичности нашег правног система и потребе Републике Србије. Усвајањем најбољих примера праксе, настојимо да обезбедимо висок

			ниво информационе безбедности и да адекватно одговоримо на све изазове који могу настати у овој области. Имајући у виду да је овај аспект већ адекватно регулисан у Нацрту закона, сматрамо да није потребно уносити додатне измене у овом правцу.
Члан 19.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Предлажемо да се предвиди доношење подзаконског акта о поступању по пријему обавештења о инциденту јер је неопходно детаљније уредити поступање по пријави, као и класификацију инцидената према нивоу опасности, односно критеријума, као и класификацију инцидената.	**Одговор на коментар:** Нацртом закона о информационој безбедности је већ предвиђено доношење подзаконског акта којим се уређује поступак обавештавања о инцидентима, обрасци за обавештавање, листа инцидената према врстама и класификација инцидената према нивоу опасности доноси Влада, на предлог Министарства. Уједно указујемо да закон већ предвиђа детаљне процедуре и одговорности Канцеларије за информациону безбедност у случају пријема обавештења о инциденту, укључујући обавезу анализе, утврђивања нивоа опасности, као

			и предузимања мера које укључују обавештавање јавности и других надлежних органа. У закону је ћ предвиђено да се Канцеларија за информациону безбедност приликом управљања одговором на инциденте руководи постојећим прописима и међународним стандардима, као што је TLP (Traffic Light Protocol) протокол, што обезбеђује да су процедуре у складу са најбољим праксама
Чл. 19.-25.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Потребно је јасно дефинисати да су ово надлежности Националног ЦЕРТ-а.	**Одговор на коментар:** Законом су већ прецизно и недвосмислено дефинисане надлежности Канцеларије за информациону безбедност, укључујући и Национални ЦЕРТ, у управљању инцидентима информационе безбедности. Додатно наглашавање и прецизирање тих надлежности би могло довести до дуплирања правних одредби, што би само по себи могло да умањи јасноћу и концизност закона, стварајући простор за потенцијалне правне недоумице и

			противречности. Такође, овакав приступ би могао угрозити доследност и координацију у примени закона, јер би се увело непотребно раздвајање надлежности у оквиру једног органа, што није у складу са принципима доброг законодавства. Због свих наведених разлога, сматрамо да је текст закона већ оптимално формулисан и да додатно прецизирање није потребно, те се коментар одбија.

Члан 19. став 3. и Члан 24	Слободан Марковић	**Коментар:** Наведене одредбе требало оснажити тако што би се законом превидела обавезност објављивања тзв. blameless post-mortem извештаја, са циљем развијања културе учења на грешкама у оквиру шире заједнице.	**Одговор на коментар:** Указујемо да је обавеза објављивања података о инцидентима већ утврђена чланом 31. Нацрта закона којим се уређују надлежности Националног ЦЕРТ-а, а које обухватају и обавештавање јавности о инцидентима у ИКТ системима у Републици Србији.
Члан 19.став 6 и 33.став 4	Cedars International doo	**Коментар:** TLP (Traffic Light Protocol) протокол није дефинисан у оквиру закона TLP протокол се појављује у оквиру ова два члана, а да није претходно јасно дефинисано шта тај протокол представља	**Одговор на коментар:** Предлог се усваја.
Чл. 22. и 23.	РАТЕЛ	**Коментар:**	**Одговор на коментар:**

	Национални ЦЕРТ	Поступање у случају инцидента нивоа опасности „висок“ и „веома висок“, нема учешћа оперативног тима, нестали су ставови из претходног Нацрта о сазивању састанка оперативног тима, па остаје нејасно у коју сврху се дефинише и образује.	Предлог се одбија будући да је учешће оперативног тима у случају инцидената нивоа опасности „висок“ и „веома висок“, већ предвиђено чланом 17. Нацрта закона. Наиме, правним тумачењем члана 17. став 1, јасно се закључује да се стални оперативни тим образује управо у циљу координисане реакције на инциденте високог и веома високог нивоа. Улога овог тима је кључна у осигурању да се на такве инциденте реагује брзо и ефикасно, у складу са надлежностима које су тиме предвиђене. Додатно, одредбе које омогућавају Канцеларији за информациону безбедност да укључи друге органе и представнике посебних ЦЕРТ-ова у рад оперативног тима потврђују да је тим формиран за реаговање на најозбиљније инциденте. Ово обезбеђује свеобухватну и координисану реакцију, што је од суштинске важности за очување информационе безбедности на националном нивоу.

			С обзиром на то да је улога оперативног тима у овом контексту већ јасно дефинисана и регулисана чланом 17, сматрамо да није потребно уносити додатне измене.
Члан 30.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Нема међународне сарадње која се касније разрађује чланом 34.	**Одговор на коментар:** Предлог се усваја.
Члан 30.	Национална алијанса за локални економски развој	**Коментар 1:** Тачка 7) – предлажемо да се избаци реч на крају „у органима“, како се обуке не би ограничавале само на лица у органима, и да цела реченица гласи: „у сарадњи са надлежним органима и другим субјектима из јавног, академског, привредног и невладиног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности“. **Коментар 2:** Предлажемо да су у члан 30. или 31, додају као области рада Канцеларије за информациону безбедност: <u>Област софтвери и алати</u> 1)Агенција ће бити задужена за валидацију софтвера/алата који се могу користити на пословима имплементације/увођења и одржавања стандарда и имплементације информационо безбедносних процеса (ISMS). <u>Област контрола и ревизија</u> Агенција ће бити задужена за сертификацију и валидацију ревизора (auditors) који се могу	**Одговор на коментар 1:** Предлог се усваја. **Одговор на коментар 2:** Коментар 2 је одбијен јер би проширење надлежности Канцеларије за информациону безбедност на валидацију софтвера, сертификацију консултаната и ревизора значајно оптеретило пројектоване капацитете и функције Канцеларије. Овакав задатак би захтевао значајне додатне ресурсе и могао би довести до потенцијалног конфликта интереса у вези са независношћу консултантских и ревизорских процеса. Поред тога, ове активности су већ регулисане постојећим националним и међународним стандардима и сертификатима, што

		бавити ревизијом имплементације законских аката и правилника дефинисаних на нивоу агенције, као и имплементације дефинисаних стандарда од стране агенције, као што су *ISO 27001* или слични. 2) Агенција ће бити задужена за сертификацију и валидацију консултаната (consultants) за послове имплементације дефинисаних стандарда, као и одређивање правила и нивоа њихове компетентности кроз поседовање међународно признатих сертификата (*CISSP*, *CISM* и сл.) 3) Агенција ће бити задужена за валидацију консултаната (*consultants*) за послове имплементације дефинисаних стандарда у оквиру организација класификованих као Оператор ИКТ система од посебног значаја ("критична инфраструктура"), односно одређивање правила за учествовање на пројектима кроз различите провере прошлости („*background check*").	би довело до преклапања надлежности и могло би створити конфузију у примени и спровођењу ових стандарда. Уместо тога, сматра се да је приоритетно да Канцеларија остане фокусирана на своје основне надлежности, како би обезбедила ефикасну заштиту и управљање безбедносним ризицима у оквиру ИКТ система од посебног значаја.
Члан 31.	Национална алијанса за локални економски развој	**Коментар 1:** Став 1 тачка 13) – предлажемо да се избрише или јасније дефинише шта се тачно мисли под „Канцеларија промовише усвајање“. Предлажемо да се користе адекватнији термини за послове Националног ЦЕРТ-а, која превазилазе промовисање. Тренутно није баш најјасније ко промовише и	**Одговор на коментар 1:** Предлог се усваја. **Одговор на коментар 2:** Чланом 12. Закона о родној равноправности предвиђена је обавеза разврставања

		ко је циљана јавност којој се промовише. **Коментар 2:** Став 2 – предлажемо да се, у делу који говори о подацима за које је Канцеларија за информациону безбедност овлашћена да обрађује, дода и информација о полу подносиоца пријаве, а у складу са чланом 12. Закона о родној равноправности.	статистичких података по полу и старосној доби у органима јавне власти и код послодаваца, што је важан аспект за праћење и унапређење родне равноправности. Међутим, ова обавеза се односи на области у којима се директно спроводе мере родне равноправности, као што су запошљавање, образовање и слично. У контексту управљања инцидентима у ИКТ систему, примарни фокус је на брзом и ефикасном одговору на инциденте који угрожавају информациону безбедност. Обрада података о полу у овом контексту не доприноси ефикасности управљања инцидентима. Иако Закон о родној равноправности има свој значај и примену, у случају ИКТ безбедности је важно задржати фокус на безбедносним аспектима, а не на подацима који нису директно повезани са проценом и управљањем безбедносним ризицима. Стога, сматрамо да се коментар 2 може оправдано одбити

			како би се омогућила ефикаснија примена мера информационе безбедности.
Члан 31.	РАТЕЛ Национални ЦЕРТ	**Коментар 1:** Нема услова које је потребно испунити да би се обезбедио континуитет рада Националног ЦЕРТ-а, ставови 5.и 6. члана 15. важећег закона, а исто је дефинисано и чланом 11. НИС2 Директиве. Предлог је да се уведу ставови од 1-3 НИС2 Директиве. **Коментар 2:** Став 1.тачка 3) изменити тако да гласи:“ пружа рана упозорења, узбуне и најаве и информише релевантна лица о претњама, рањивостима и инцидентима.“ Као у тачки 1). Сматрамо да је потребно јасно дефинисати надлежности Националног ЦЕРТ-а кроз више чланови како би се обезбедио континуитет и смањио ризик од премештања из институције у институцију, у складу са начелом савести и оспособљености овог Нацрта.	**Одговор на коментар 1 и 2:** Предлог се усваја.
Члан 32.	РАТЕЛ Национални ЦЕРТ	**Коментар:** Назив тзв. владиног ЦЕРТ-а је сувише рогобатан и требало би задржати важећи ЦЕРТ органа власти јер је због иначе „тешке“ терминологије коришћене у закону доста појмова нејасно, што је довело до нових колоквијалних појмова који уносе додатну забуну.	**Одговор на коментар:** Предлог је прихваћен и унет је назив „ЦЕРТ органа власти“. Уједно напомињемо да, иако је овај предлог прихваћен, није коришћен колоквијални појам будући да је термин Јединствена информационо-комуникационе мреже електронске управе већ дефинисан и

			утврђен другим прописом (Закон о електронској управи).
Чланови од 39. до 42.	Cedars International doo	**Коментар:** Наведене казне у документу не усклађују са штетом коју би могао data leak проузроковати. Ако оператор ИКТ система зна да њихов систем није безбедан посто нису поштовали закон, али су га продали држави са тим знањем на уму, то је прекршај државног закона. Пенали би требали да се дефинишу на суду који ће одредити колико штете се било и колико казна треба да буду, као сваки други прекршај дозваног закона. Са овим казнама, има шансе да оператори ИКТ система неће поштовати овај закон.	Наведени коментар не одговара садржају чланова 39, 40 и 41, јер ови чланови регулишу техничке мере у области криптографске безбедности и заштите од компромитујућег електромагнетног зрачења (КЕМЗ). Они се не баве питањем санкција и одговорности за пропусте у спровођењу информационе безбедности. Предложени коментар се фокусира на питање казни за могуће пропусте и злоупотребе од стране оператора ИКТ система, што је тема која треба да буде разматрана у оквиру делова закона који се баве санкцијама и правним последицама кршења прописа. Стога, овај коментар је непримењив на наведене чланове и не може се усвојити у овом контексту.
Члан 46.	Cedars International doo	**Коментар:** Није јасно дефинисано ко постављања Инспекторе за информациону безбедност, као ни ко врши обуку и припрему Инспектора.	**Одговор на коментар:** Предлог није усвојен, будући да је другим прописима (Законом о инспекцијском надзору, Законом о

		У оквиру члана 46. је наведено да Канцеларија спроводи послове инспекције преко инспектора, али није јасно наведено ко поставља и обучава инспекторе.	државној управи и другим релевантним прописима) одређено на који начин орган врши послове из своје надлежности, као и обуке запослених, што се односи и на послове инспекције за информациону безбедност.
Члан 47.	Cedars International doo	**Коментар:** Овлашћење инспектора би требало проширити, тако да укључи и остале врсте прегледа по потреби, а не само скенирања ИКТ система. Коментар: Скенирање ИКТ система, у свакодневној терминологији, подразумева скенирање мреже на рањивости, а могуће је у складу са проценом и идентификовањем одређених ризика, да је потребно спровести и друге врсте прегледа (преглед конфигурација, penetration тестирање..)	**Одговор на коментар:** Предлог се усваја.
Члан 47.	Cedars International doo	**Коментар:** Проширити/дефинисати овлашћења инспектора, те у иста и додати могућност кажњавања. Тренутно није дефинисано ко кажњава операторе ИКТ система од посебног значаја.	**Одговор на коментар:** Није потребно додавати овлашћења инспектора за кажњавање у Закон о информационој безбедности, јер су та овлашћења већ прописана Законом о инспекцијском надзору и односе се и на примену Закона о информационој безбедности.
Члан 47.	A1	**Коментар:** Став 1. тачка 3) предвиђа да: „Инспектор за	**Одговор на коментар:**

		информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђеним законом: 3) захтева од оператора ИКТ система од посебног значаја да изврши скенирање ИКТ система у циљу утврђивања евентуалних безбедносних рањивости, а у складу са проценом ризика;“ Коментар: Овакво навођење овлашћења инспектора сматрамо неодређеним, те предлажемо прецизирање случајева у којима се додељује овакво овлашћење инспектору ради избегавања несигурности.	Сматрамо да предлог за додатно прецизирање овлашћења инспектора за информациону безбедност није неопходан. Инспектор већ има довољно прецизна овлашћења дефинисана законом, укључујући и Законом о инспекцијском надзору. Ова овлашћења обухватају право инспектора да, у случају постојања процене ризика или сумње на безбедносне рањивости, наложи скенирање ИКТ система. Прецизирање додатних услова за коришћење овог овлашћења могло би непотребно да ограничи делотворност инспекцијског надзора и створи правне несигурности. Због тога сматрамо да је потребно да се постојећа формулација задржи.
Члан 48.	Национална алијанса за локални економски развој	**Коментар:** Предлажемо да се у казнене одредбе дода и 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. Премда је ово	**Одговор на коментар:** Сматрамо да предложене измене у виду додавања казнене одредбе за неовлашћено обелодањивање поверљивих информација оператора ИКТ система нису неопходне у оквиру овог закона. Овакво

		поступање кажњиво применом других закона из области кривичног и казненог права, сматрамо да га треба нагласити и у Закону о информационој безбедности.	казнено дело је већ уређен кроз постојеће законске оквире који регулишу заштиту поверљивих података и информација, као што су Закон о заштити података о личности и Кривични законик. Увођење додатних казнених одредби у Закону о информационој безбедности би довело до преклапања правних норми и потенцијалних правних несигурности. Такође, предлог за увођење казнене одредбе за неадекватно управљање информационом безбедношћу није сврсисходан јер је одговорност оператора већ детаљно регулисана постојећим казненим одредбама које предвиђају казне за непоштовање одредби о информационој безбедности. Инциденти и њихове последице се већ разматрају у складу са овим законом, а додатне казнене одредбе би могле довести до дуплирања обавеза и конфузије у примени закона.
Чланови од 48. до 51.	Cedars International doo	**Коментар 1:** Приликом имплементације сигурносних мера у систем управљања организацијом, одговорност за преузимање	**Одговор на коментар 1**: Сматрамо да је потребно одбити предлог да се

		свих ризика и последица мора бити на највишем надређеном лицу, попут генералног директора (ЦЕО). Директори сектора и менаџмент не могу бити директно одговорни за непоштовање стандарда због организационе структуре, јер њихове функције немају извршну контролу над целокупном организацијом. **Коментар 2:** Износ казни је несразмеран стварним губицима у случају експлоатације ризика. **Коментар 3:** Не постоје казне за сајбер тероризам/криминал.	одговорност за ризике и последице пребаци искључиво на највише надређено лице, попут генералног директора (CEO). Организациона структура привредних субјеката подразумева да се одговорности деле на различитим нивоима управљања, у зависности од природе послова и функција. Директори сектора и менаџмент су одговорни за примену стандарда у својим областима деловања, иако можда немају извршну контролу над целокупном организацијом. Преношење одговорности само на једну позицију може довести до непотпуне примене мера безбедности и умањити ефикасност укупног система управљања информационом безбедношћу. **Одговор на коментар 2**: Одбија се предлог да се измене износи казни на основу тврдње да су несразмерни стварним губицима у случају експлоатације ризика. Износи казни су утврђени с обзиром на превентивну природу и значај очувања

			информационе безбедности, као и са циљем да се оператери ИКТ система подстакну да предузму све неопходне мере заштите. Прекомерно смањење казни могло би ослабити правни систем заштите и довести до мање озбиљног приступа примени мера безбедности. Напомињемо и да су предвиђене казне у оквиру општих лимита који су прописани Законом о прекршајима и који не могу бити промењени Законом о информационој безбедности. **Одговор на коментар 3**: Предлог за увођење казни за сајбер тероризам/криминал такође се одбија, јер је ова област већ регулисана у оквиру кривичног законодавства Републике Србије.
Члан 52.	Службени гласник	**Коментар:** Потребно је дефинисати у ком року је Национални ЦЕРТ (тј. орган који обавља послове Националног ЦЕРТа) дужан да донесе/предложи методологију за процену ризика у ИКТ системима од посебног значаја. Коментар: Формално гледано, није у питању подзаконски акт, те	**Одговор на коментар:** Предлог се усваја.

		не подлеже роковима из Члана 52. Ово питање је важно и са становишта органа који ће донети ову методологију – да ли ће то бити РАТЕЛ или Канцеларија за ИТЕ? Треба узети у обзир и то да се рокови из Члана 52 поклапају са преузимањем права, обавеза, запослених, предмета, опреме, средстава за рад и архиве из РАТЕЛа у Канцеларију за ИТЕ (Члан 54).	
Члан 53.	Службени гласник	**Коментар:** Рок у којем су Оператори ИКТ система од посебног значаја дужни да донесу Акт о процени ризика за ИКТ системе којима управљају и Акт о безбедности ИКТ система треба да буде везан за датуме ступања на снагу одговарајућих подзаконских аката из Члана 6 и Члана 12, односно доношења методологије из Члана 11, а не за датум ступања Закона на снагу (12 месеци). Ово посебно имајући у виду да и до 6 месеци по доношењу закона поједини Оператори још увек неће ни знати да ли спадају у Операторе ИКТ система од посебног значаја, као ни којег су приоритета/важности, а да је у року од 6 месеци потребно донети 12 подзаконских аката. Такође, није прецизиран рок за доношење методологије из Члана 11 (видети ставку 2).	**Одговор на коментар:** Коментар није прихваћен, с обзиром да је рок за доношење акта којим ће се одредити оператори 6 месеци. Сматрамо да су рокови за доношење акта о процени ризика адекватни и да оператори имају довољно времена да их припреме.
Члан 54.	Службени гласник	Чланом 136. Закона о државним службеницима, прописано је да ако део делокруга државног органа преузме други државни орган, он преузима и државне службенике који	Прихваћено.

		раде у преузетом делокругу. У том смислу сматрам да одредбе Члана 54 Нацрта којима Канцеларија за ИТЕ преузима права, обавезе, предмете, опрему, средства за рад и архиву од Министарства насталу у обављању послова инспекције за информациону безбедност, а НЕ преузима запослене који у Министарству обављају послове инспекције за информациону безбедност - нису у складу са прописима којим се уређује положај државних службеника. Коментар: Општи утисак са тачке гледишта Оператора ИКТ система од посебног значаја: највећу забуну доноси вишеструко преношење делокруга рада Националног ЦЕРТа (РАТЕЛ – Канцеларија за ИТЕ – Канцеларија за ИБ) и инспекције за ИБ (Министарство – Канцеларија за ИТЕ – Канцеларија за ИБ) и то што се „прелазне тачке“ за ЦЕРТ преклапају са роковима везаним за доношење подзаконских аката, а за инспекцију се преклапају са роковима везано за обавезе Оператора да донесу акте у складу са новим ЗИБом.	
Члан 55.	Национална алијанса за локални економски развој	**Коментар:** Предлажемо додавање додатног, новог, става 9 „Приликом преузимања запослених потребно је да се обезбеде минимално исти услови рада који су имале пре преузимања“.	**Одговор на коментар:** Предложено додавање става којим би се прописала обавеза задржавања минимално истих услова рада за запослене приликом њиховог преузимања

			је непотребно, јер је то питање већ регулисано важећим Законом о раду Републике Србије. Закон о раду предвиђа да у случају преноса запослених из једног правног лица у друго, нови послодавац има обавезу да обезбеди исте или боље услове рада који су важили код претходног послодавца. Додатно укључивање такве одредбе у овај закон би представљало дуплирање правних норми, што није неопходно и могло би довести до конфузије у примени закона. Због тога, овај коментар се не усваја.
Члан 56.	А1	С обзиром на свеобухватност промена које доноси нови Нацрт закона и време за доношење подзаконских аката који ће детаљније уредити неке области, као и значајне обавезе за операторе ИКТ система од посебног значаја, што ће захтевати и додатне развоје на системима, предлажемо да се примена закона одложи, те да члан 56. Нацрта закона гласи: „Овај закон ступа на снагу осмог дана од дана објављивања у Службеном гласнику Републике Србије, а примењује се од 01. јула 2025. године.“	Предлог није прихваћен, с обзиром да је за знатан број обавеза оператора ИКТ система (упис у евиденцију, доношење акта о процени ризика и акта о безбедности) предвиђен извесни транзициони период на основу више норми закона.

Прилог: Извештај са округлог стола одржаног у Београду дана 17. јула 2024. године

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

одржаног дана 17. јула 2024. године с почетком у 10:00 часова путем видео конференцијске везе

Милан Војводић, шеф Одсека за регулативу у области информационе безбедности Министарства информисања и телекомуникација отворио је јавну расправу поводом Нацрта закона о информационој безбедности (у даљем тексту: Закон) и захвалио се свим присутнима на интересовању за учешће. Указао је да је било неопходно опет презентовати Закон на јавној расправи с обзиром да је Закон претрпео одређене промене у односу на претходни нацрт закон иако је иста већ одржана 2023. године. Подсетио је да је Министарство информисања и телекомуникација 2023. године формирало Радну групе за израду Нацрта закона о информационој безбедности и у којој је учествовао велики број представника из државних органа, привреде, образовних институција, као и представници организација које се баве питањима информационе безбедности.

Истакао је као главни разлог доношења новог закона 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. 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 су приоритетни оператори ИКТ системи од посебног значаја дужни да проверу обављају два пута годишње. Даље је представљена категоризација субјеката према напред наведене две категорије, као и 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).

Указао је да одредбе 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, а које се између осталог односе на процедуре за скенирање мреже, информације о рањивостима

ИКТ система, ограничење приступа интернет страницама и којих свеукупно има тридесет четири. Указао је да једна од битних новина које Закон о информационој безбедности предвиђа увођење обавезе доношења Акта о процени ризика. Такође, поред Акта о процени ризика остала је обавеза доношења Акта о безбедности ИКТ система.

Оператори ИКТ система од посебног значаја дужни су да доставе обавештење о инциденту који може да има значајан утицај на нарушавање информационе безбедности, без одлагања, а најкасније у року од 24 сата од када су сазнали за инцидент. Оператори ИКТ система од посебног значаја дужни су да обавештења о инцидентима доставе у јединствени систем за пријем обавештења о инцидентима који одржава Канцеларија за информациону безбедност. 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 нивоу опасности (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 Влада 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, а то значи да надлежни орган за информациону безбедност остаје Министарство информисања и телекомуникација, које припрема прописе, планска документа, води Евиденцију ИКТ система од посебног значаја, врши међународну сарадњу, а промена која је овим законом предвиђена односи се вршење инспекцијског надзора. Планирано је да инспекцијски надзор врши Министарство информисања и телекомуникација годину дана од дана ступања на снагу овог закона, а потом би се инспекцијски надзор пренео најпре Канцеларији за информационе технологије и електронску управу, а потом Канцеларији за информациону безбедност.

Законом се од 1. јуна 2027.године успоставља Канцеларија за информациону безбедност која би имала улогу да удружи постојеће ресурсе у области информационе безбедности и тиме побољша одговор Републике Србије на изазове у области информационе безбедности. Канцеларија за информациону безбедност би вршила послове ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе, послове Националног ЦЕРТ-а, послове међународне сарадње, послове јединствене тачке контакта у међународној сарадњи, послове одговора на инциденте, прописивање мере заштите органа као и многе друге у складу са законом. Законом је предвиђено да до образовања Канцеларије за информациону безбедност ове послове врши Канцеларија за информационе технологије и електронску управу.

Послови Националног ЦЕРТ-а, проширени су у складу са НИС2 Директивом. Проширене надлежности између осталог подразумевају да на захтев оператора ИКТ система од посебног значаја Националног ЦЕРТ је дужан да пружа помоћ у праћењу стања безбедности ИКТ система у реалном времену или приближном реалном времену,

врши проактивно скенирање ИКТ система, поступа као координатор за потребе координираног откривања рањивости као и да води базу рањивости ИКТ производа и ИКТ услуга.

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.

Нове одредбе које се односе на инспекцију за информациону безбедност јесу да послове инспекције за информациону безбедност обавља Канцеларија за информациону безбедност. Прописано је да до успостављања Канцеларије за информациону безбедност првих годину дана од дана ступања на снагу Закона о информационој безбедности послове обавља Министарство информисања и телекомуникација. Након истека тог периода послове инспекције преузеће Канцеларија за информационе технологије и електронску управу, а од 1. јуна 2027. године послове инспекцијског надзора вршиће Канцеларија за информациону безбедност.

Такође проширена су овлашћења инспектора за информациону безбедност у поступку спровођења надзора који уз овлашћења утврђеним Законом о инспекцијском надзору може и да захтева од оператора ИКТ система од посебног значаја да изврши скенирање ИКТ система у циљу утврђивања евентуалних безбедносних рањивости, затим да наложи да надзирани субјект учини доступним јавности информације које се тичу непоштовања одредби овог Закона и да наложи да надзирани субјект одреди лице са тачно утврђеним овлашћењима које ће у утврђеном временском периоду надзирати и пратити усаглашеност са одредбама овог Закона и наложеним мерама.

Нове одредбе које се односе на непоштовање овог Закона односно казнене одредбе јесте виши износ новчане казне за операторе приоритетног ИКТ система од посебног значаја.

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.

Подзаконски акти који регулишу ову област биће донети у року од шест месеци од дана ступања на снагу овог Закона.

Након завршене презентације одредби новог Закона о информационој безбедности позвао је све присутне да поставе питања.

Маја Лакушић, Национални ЦЕРТ, указала је да сматра да је потребно кориговати одредбе члана 31. које се односи на послове Националног ЦЕТ-а, а све у складу са чланом 11. НИС2 Директиве како би се додали услови и надлежности који недостају, а

прописани су наведеном Директивом и који би омогућили неометан рад Националног ЦЕРТ-а и јасно утврђене надлежности. Везано за члан 17. који се односи на улогу оперативног тима за реаговање на инциденте истакла је потребу за сталним усавршавањем чланова истог као и улоге оперативног тима у поступању у случају инцидената нивоа опасности означен као висок и веома висок. Поставила је питање везано за члан 14. који се односи на достављање обавештења о инцидентима како ће орган који је примио обавештење о инциденту знати да ли је реч о ИКТ систему од посебног значаја који је одређен као критична инфраструктура. Указала је на потребу усклађивања терминологије и да не би требало да се мења назив ЦЕРТ-а органа власти. Везано за члан 54. који се односи на пренос надлежности мишљења је да би било корисније да се Канцеларији за информациону безбедност додели надлежност ревизије или стручног надзора која би представљала помоћ постојећем инспекцијском надзору. Такође истакла је да би пружање стручне и техничке помоћи операторима ИКТ система од посебног значаја много више значило него да се уводи инспекцијски надзор у нову институцију као и да би требало размотрити мере и обавезе истих.

Соња Суботић, психолог, поставила је питање како и коме да у својству физичког лица пријави проблем уколико доживи напад на сајт као и да ли су напади такве природе кривична дела.

Ана Златановић, Службени гласник, поставила је питање коме и када у прелазном периоду се обраћају оператори ИКТ система од посебног значаја у случају проблема као и питања услова запошљавања, стручности и мотивисаности стручног кадра за рад у Канцеларији за информациону безбедност како би се избегло поверавање послова трећим лицима.

Ана Миловановић из Националне алијансе за локални економски развој, истакла је да би било добро да се у самом тексту закона експлицитно наведу услови запослених у Канцеларији за информациону безбедности и да се обезбеде минимални услови које имају у националном ЦЕРТ-у. Поставила је питање да ли капацитети у државном дата центру који би се могли искористити за чување приоритетних скупова података локалних самоуправа. Истакла је да с обзиром на Закон о критичној инфраструктури, а ради избегавања дуплирања сектора који су већ препознати као критична инфраструктура наведеним законом, да се наведу они који нису обухваћени тим законом ради избегавања дуплирања норми из различитих прописа.

Сања Кекић, Women4Cyber, изнела је мишљење да би било добро да се члан 1. Закона преформулише како би се јасно видело коме је намењен Закон. Такође мишљења је да би запосленима који се пребацују требало заштитити статус приликом преласка из једне институције у другу. Везано за спровођење програма обука и стручног усавршавања лица који раде на пословима информационе безбедности истакла је да наведене обуке би требало да се прошире и на остала лица и категорије, а не само лица која раде у органима.

Додала је да је потребно преформулисати члан 2. тачку 11) и допунити са речима „идентификација ризика“ као и да је потребно додати члан који би истакао родну равноправност и инклузију.

Слободан Марковић дао је коментар на члан 19. који уређује поступање по пријему обавештења о инциденту односно ситуацију када је неопходно да јавност буде упозната

са инцидентом или када је инцидент од интереса за јавност да сматра да би наведене одредбе требало оснажити тако што би се законом предвидела обавезност објављивања blameless post-mortem извештаја, пре свега мислећи на високопрофилне инциденте са последицама по пружање јавних услуга.

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 и на постављеним питањима и датим сугестијама и коментарима. Такође, још једном је истакао да је јавна расправа отворена до 23. јула и позвао све заинтересоване да доставе своје коментаре, мишљења и предлоге.

Округли сто завршен је у 12 часова.

Записник саставила:

Дијана Поповић