



Република Србија
Републички секретаријат
за јавне политике
Број: 011-00-00038/2019-02
7. мај 2019. године
Влајковићева 10
Београд

МИНИСТАРСТВО ТРГОВИНЕ, ТУРИЗМА И ТЕЛЕКОМУНИКАЦИЈА

БЕОГРАД
Немањина 22-26

ПРЕДМЕТ: Мишљење на Нацрт закона о изменама и допунама Закона о информационој безбедности

У вези са вашим дописом број: 011-00-00139/2019-12 од 16. априла 2019. године којим сте Републичком секретаријату за јавне политике доставили на мишљење Нацрт закона о изменама и допунама Закона о информационој безбедности (у даљем тексту: Нацрт закона) са анализом ефеката Нацрта закона и Образложењем Нацрта закона, обавештавамо вас о следећем:

Члан 9. којим се у важећем Закону о информационој безбедности ("Сл. гласник РС", бр. 6/2016 и 94/2017) предвиђа доношење новог члана 11а. који у ставу 1. тачка 2) предвиђа да је оператор ИКТ система од посебног значаја дужан да поред осталог пријави инциденте који утичу на велики број корисника услуга или трају дужи временски период, а који могу да имају значајан утицај на нарушување информационе безбедности.

Сматрамо да је у наведеној законској одредби, имајући у виду нарочит значај ове категорије инцидената, потребно ближе дефинисати (прецизирати) термине као што је „велики број корисника“ и „дужи временски период“ како би се смањило дискреционо овлашћење оператора ИКТ система приликом доношења одлуке о томе да ли ће се пријавити одређени инциденти који могу да имају значајан утицај на нарушување информационе безбедности. Такође сматрамо да је у наведеној предложенју законској одредби потребно прецизирати и критеријуме на основу којих је могуће адекватно проценити да је наступио услов који се односи на то да је дошло до потенцијалног значајног утицаја на нарушување информационе безбедности.

Имајући у виду садржну достављеног текста Нацрта закона, Републички секретаријат за јавне политике је становишта да извештај о спроведеној анализи ефеката прописа, у вези са чланом 8. Уредбе о методологији управљања јавним политикама, анализи ефеката јавних политика и прописа и садржају појединачних докумената јавних политика („Службени гласник РС“, бр. 8/19, у даљем тексту: Уредба), треба да садржи образложене одговоре на питања из прилога 2-10. Уредбе, те стога у даљем тексту упућујемо на недостатке достављене анализе ефеката прописа.

У оквиру кључних питања из прилога 2. Уредбе која се односе на анализу постојећег стања и правилно дефинисање промене која се предлаже, указујемо да је предлагач пропустио да представи резултате спровођења релевантног документа јавних политика у овој области (Стратегије развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године („Службени гласник РС“ бр. 53/17)) и

Акционог плана за 2018. и 2019. годину за спровођење Стратегије развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године („Службени гласник РС“ бр. 76/18)). Такође предлагач није навео ни да ли је приликом израде текста Нацрта закона разматрао и искуства других држава у остваривању промена које се желе постићи овим законом (упоредно-правна анализа).

У оквиру кључних питања из прилога 3. Уредбе која се односе на утврђивање циљева предлагач је пропустио да наведе на основу којих показатеља учинка ће бити могуће утврдити да ли је дошло до остваривања општих, односно посебних циљева који се желе постићи доношењем овог закона.

У оквиру кључних питања из прилога 4. Уредбе која се односе на кључна питања за идентификовање опција јавних политика предлагач није дао одговор. С тим у вези, било је потребно доставити образложене одговоре на питања која се односе на то које релевантне опције за остваривање циља су разматране, да ли је разматрана опција „status quo“ (уз бољу имплементацију постојеће регулативе) и да ли су поред регулаторних разматране и друге опције за постизање жељене промене, с обзиром да је предлагач у извештају о спроведеној Анализи ефеката прописа навео да је важећи Закон о информационој безбедности већ био у значајној мери усклађен са директивом о мерама за висок ниво безбедности мрежних и информационих система у Европској унији број 2016/1148 (НИС директиве), која је усвојена у јулу 2016. године.

У оквиру кључних питања из прилога 6. Уредбе која се односе на анализу економских ефеката предлагач је навео да ће предложена законска решења створити потенцијално нове трошкове одређеним привредним субјектима и да није могуће прецизно израчунати додатне трошкове за испуњење законских обавеза који се огледају у евентуалном додатном технолошком опремању, обуци запослених, ангажовању нових стручњака и остало. Стoga, истичемо да је било потребно на конкретном примеру применом методом стандардног трошка (*eng. standard cost model*) показати колико ће додатно административно оптерећење привредним субјектима проузроковати обавеза увођења тзв. ИКТ система од посебног значаја и у област *производње и снабдевања хемикалијама*, имајући у виду да члан 5. Нацрта закона којим се мења важећи члан 6. важећег Закона о информационој безбедности, проширује домен примене новог информационог система и на ову област пословања.

Такође указујемо предлагачу да нови трошкови за привредне субјекте могу настати и на основу члана 19. Нацрта закона који уводи нови члан 19а. у важећи Закон о информационој безбедности у делу који се односи на став 3, као последица прописивања обавезе за оператора електронских комуникација који пружа јавно доступне телефонске услуге да омогући свим претплатницима услугу бесплатног позива према јединственом месту за пружање савета и пријем пријава у вези са безбедношћу на интернету.

У оквиру кључних питања из прилога 9. Уредбе која се односе на анализу управљачких ефеката, предлагач је требало да наведе какви су постојећи капацитети јавне управе (кадровски, технички, организациони) за спровођење изабране опције и да ли је с тим у вези потребно предузети одређене мере за побољшање тих капацитета. Ту мислимо конкретно на капацитете надлежног министарства (надлежни орган), с обзиром да члан 6. Нацрта закона којим се уводи нови члан 6б. у важећем Закону о информационој безбедности прописује обавезу Министарства да успостави и води ажуруну евиденцију ИКТ система од посебног значаја. Наводимо да је потребно навести и које конкретно активности је потребно предузети у циљу спровођења *превентивних* мера за безбедност и заштиту на интернету у складу са чланом 19. Нацрта закона који уводи нови члан 19а. у важећи Закон о информационој безбедности.

Такође потребно је навести које конкретно активности је неопходно да спроведу и оператори ИКТ система од посебног значаја како би били у могућности да врше обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности преко портала надлежног органа или националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима, у складу са чланом 8. Нацрта закона којим се мења члан 11. важећег Закона о информационој безбедности.

На крају наводимо и да је у овом сегменту извештаја о спроведеној анализи ефеката прописа потребно навести и које све подзаконске акте је потребно донети (или изменити) како би се у потпуности имплементирала нова законска решења у области информационе безбедности.

Имајући у виду све наведено, у складу са чланом 37. и чланом 41. став 3. Закона о планском систему Републике Србије („Службени гласник РС“ бр. 30/2018) и чл. 47, 48 и 49. Уредбе о методологији управљања јавним политикама, анализи ефеката јавних политика и прописа и садржају појединачних докумената јавних политика („Службени гласник РС“, бр. 8/2019), Републички секретаријат за јавне политике је мишљења да Нацрт закона садржи **недовољну** анализу ефеката и позива предлагача да поступи у складу са наведеним примедбама и унапреди текст Нацрта закона и извештај о спроведеној анализи прописа.

