И З В Е Ш Т А Ј

о резултатима спроведених јавних консултацијама о Нацрту правилника о безбедности и интегритету јавних електронских комуникационих мрежа и услуга и терминалне опреме

На основу члана 37. Закона о електронским комуникацијама („Службени гласник РС”, број 35/23, у даљем тексту: Закон), Регулаторно тело за електронске комуникације и поштанске услуге (у даљем тексту: Регулатор) објављује Извештај о резултатима спроведених јавних консултација о Нацрту правилника о безбедности и интегритету јавних електронских комуникационих мрежа и услуга и терминалне опреме (у даљем тексту: Нацрт правилника).

Нацрт правилника је припремљен у складу са одредбом члана 157. став 7. Закона којом је прописано, између осталог, да Регулаторно тело за електронске комуникације и поштанске услуге (у даљем тексту: Регулатор) ближе уређује примену адекватних техничких и организационих мера примерених постојећим ризицима, а посебно мера за превенцију и минимизацију утицаја безбедносних инцидената по кориснике и међуповезане мреже, мера за обезбеђивање континуитета рада јавних комуникационих мрежа и услуга, мера заштите за спречавање неовлашћеног коришћења терминалне опреме која омогућава приступ интернету, поступак обавештавања корисника када постоји посебан ризик од повреде безбедности и интегритета јавних електронских комуникационих мрежа и услуга и поступак обавештавања Регулатора о свакој повреди безбедности и интегритета јавних електронских комуникационих мрежа и услуга која је значајно утицала на рад привредног субјекта.

У складу са чл. 36. и 37. Закона, Регулатор је спровео јавне консултације о Нацрту правилника у периоду од 30. априла до 14. јуна 2024. године, како би све заинтересоване стране биле благовремено и правилно информисане о предложеним решењима, чиме би се омогућило да дају и свој допринос даљем унапређењу предложених решења.

Текст Нацрта правилника објављен је на званичној веб презентацији Регулатора https://www.ratel.rs/cyr/blog/javne-konsultatsije-o-natsrtu-pravilnika-o-bezbednosti-i-integritetu-javnikh-elektronskikh-komunikatsionikh-mrezha-i-usluga-i-terminalne-opreme, као и на порталу Е-консултације, а сва заинтересована лица била су у могућности да своја мишљења доставе у писаном облику или електронским путем.

Као резултат спроведених јавних консултација, Регулатору су достављена мишљења од стране A1 Srbija d.o.o. Beograd у (даљем тексту: A1) и CETIN d.o.o. Beograd (у даљем тексту: CETIN).

У наставку, Регулатор даје одговоре на пристигла мишљења.

Мишљење, предлог, примедба, коментар	Одговор Регулатора

А1:

1. У Нацрту правилника у члану 2. који се односи на значење појединих појмова, у последњој одредби наведеног члана наводи се да појмови који се употребљавају у овом правилнику имају значење прописано законима којима се уређују електронске комуникације и информациона безбедност. Сходно наведеном, у Закону о информационој безбедности дефинисан је појам „инцидент“ на начин да је инцидент сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система. Међутим, из наведене дефиниције није јасно да ли се под инцидентом подразумевају негативни утицаји на безбедност мрежних и информационих система који настају као последица више силе (нпр. елементарне непогоде), фактора људске грешке, нестанка струје и сл. те молимо за појашњење.	**Примедба је размотрена и предлог се не прихвата** Закон о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19, у даљем тексту: ЗИБ) утврђује појам „инцидент“ као „сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система”. Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Службени гласник РС”, број 11/20), у члану 4. и Прилогу 1, прецизира врсте инцидената у информационо-комуникационим системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности, у које, између осталог, спадају прекид у функционисању система или дела система и остали инциденти. Наведени инциденти могу да настану као последица више силе (нпр. елементарне непогоде), фактора људске грешке, нестанка струје и сл.
2. Нацрт Правилника у члану 3. став 4, „Обавезе привредних субјеката“, предвиђа да привредни субјект примењује техничке смернице о безбедносним мерама и претњама у области електронских комуникација Агенције за сајбер безбедност Европске уније (ЕНИСА) и српске стандарде за спровођење техничких и организационих мера безбедности. Наведена одредба не прецизира да ли смернице ЕНИСА и српски стандарди наведени у Прилогу 1 представљају	**Примедба је размотрена и предлог се делимично прихвата** Члан 3. Нацрта правилника ближе уређује обавезе привредних субјеката које су прописане чланом 157. став 1. Закона, па у складу са тим, све што је прописано у овом члану представља обавезу за привредне субјекте, а између осталог, и примена техничких смерница о безбедносним мерама и претњама у

препоруку или обавезу примене истих у пословању привредног субјекта, те молимо за појашњење. Такође, наведени Правилник, иако упућује на смернице ЕНИСА, не наводи конкретне документ(е) ЕНИСА за разлику од Прилога 1 који садржи листу конкретних српских стандарда те предлажемо да предметни Правилник буде допуњен односно да упућује на конкретне смернице ЕНИСА о безбедносним мерама и претњама у области електронских комуникација.	области електронских комуникација Агенције за сајбер безбедност Европске уније (ENISA) и српских стандарда за спровођење техничких и организационих мера безбедности. Прилог 1. Нацрта правилника је допуњен навођењем конкретне смернице Агенције за сајбер безбедност Европске Уније (ENISA) о безбедносним мерама и претњама у области електронских комуникација.
3. У члану 5, „Обавештавање Регулатора о безбедносним инцидентима“, у последњем ставу овог члана наводи се да је привредни субјект дужан да на захтев Регулатора достави статистичке податке о свим безбедносним инцидентима у претходној години. Овако формулисан став не прецизира јасно које податке о инцидентима треба доставити на захтев РАТЕЛ-а те предлажемо да се овај став допуни тако да јасно произлази да је на захтев РАТЕЛ-а потребно доставити оне податке о инцидентима који су у претходном периоду већ достављени РАТЕЛ-у у складу са квантитативним и квалитативним критеријумима за обавештавање. Предлог допуњеног става гласи: „Привредни субјект је дужан да, на захтев Регулатора, достави статистичке податке о свим безбедносним инцидентима у претходној години, у складу са квантитативним и квалитативним критеријумима за обавештавање наведеним у Прилогу 2. Правилника.“	**Примедба је размотрена и предлог се не прихвата** Привредни субјект дужан је да, на захтев Регулатора, достави статистичке податке о **свим** безбедносним инцидентима у претходној години, **без обзира на испуњеност критеријума за обавештавање наведених у Прилогу 2**. Нацрта правилника и/или критеријуме из прописа којим се уређује поступак обавештавања о инцидентима у информационо - комуникационим системима од посебног значаја, све у складу са чл. 157. и 34. став 1. тачка 10) Закона, који, између осталог, уређују достављање података потребних за процену безбедности и интегритета мрежа и услуга.
4. У члану 6. став 1, „Обавештавање корисника о посебним ризицима односно претњама повреде безбедности и интегритета“, предвиђено је да је привредни субјект дужан да без одлагања у случају постојања посебног ризика, односно претње	**Примедба је размотрена и предлог се делимично прихвата** Члан 6. Нацрта правилника је измењен и сада гласи:

повреде безбедности и интегритета јавних електронских комуникационих мрежа и/или услуга или терминалне опреме која омогућава приступ интернету, о том ризику односно претњи обавести кориснике на јасан и документован начин путем своје веб презентације, међутим Правилник не дефинише детаљније шта се подразумева под термином „посебан ризик“ те предлажемо да се дефиниција „посебан ризик“ дефинише у оквиру члана 2. овог Правилника.	„Привредни субјект је дужан да, без одлагања, у случају постојања претње која доводи до значајног повећања ризика повреде безбедности и интегритета јавних електронских комуникационих мрежа и/или услуга или терминалне опреме која омогућава приступ интернету (неовлашћени приступ, значајан губитак података, угрожавања тајности комуникација, безбедности података о личности и друго) о тој претњи, обавести кориснике на јасан и документован начин, путем своје веб презентације и на друге погодне начине. У случају да претња из става 1. овог члана захтева мере које су ван опсега мера које је привредни субјект дужан да примени, привредни субјект је у обавези да обавести кориснике на које би таква претња могла да утиче, о могућим мерама заштите које корисник може да примени, као и о евентуалним трошковима везаним за примену тих мера.“
5. Такође предлажемо да се члан 6. став 1, допуни тако да буде усклађен са чланом 5. став 1. који дефинише рок у којем је привредни субјект у обавези да обавести РАТЕЛ те да се иста временска одредница користи и за обавезу обавештавања корисника, чиме се уједно уважавају и техничке могућности привредног субјекта везано за покретање поступка постављања обавештења на своју веб презентацију. Предлог допуне члана 6. став 1. гласи: „Привредни субјект је дужан да, без одлагања, а најкасније наредног радног дана од дана сазнања о постојању посебног ризика, односно претње повреде безбедности и	**Примедба је размотрена и предлог се не прихвата** С обзиром на законско овлашћење, дато Регулатору ради ближег уређивања поступка обавештавања из члана 157. став 3, као и примену техничких и организационих мера из става 1. истог члана, сматрамо да је неопходно да се предметно обавештавање корисника од стране привредног субјекта учини без одлагања, имајући у виду потребу да се у највећој могућој мери предупреди настанак безбедносних инцидената.

интегритета јавних електронских комуникационих мрежа и/или услуга или терминалне опреме која омогућава приступ интернету, о том ризику односно претњи (неовлашћен приступ, значајан губитак података, угрожавање тајности комуникација, безбедности података о личности и друго), обавести кориснике на јасан и документован начин, путем своје веб презентације.“	
6. Имајући у виду следеће: - Примену смерница ЕНИСА и српских стандарда по питању безбедносних мера, - Да члан 4. став 1, „Провера усклађености примењених мера заштите“, наводи да је привредни субјект у обавези да самостално или уз ангажовање спољних експерата, спроведе процену ризика и проверу усклађености примењених мера заштите у складу са законом којим се уређује област информационе безбедности те да постојећи Закон о информационој безбедности ("Службени гласник РС", бр. 6/16 , 94/17 и 77/19) предвиђа искључиво процену ризика од неовлашћеног приступа тајним подацима путем КЕМЗ-а (компромитујуће електромагнетно зрачење), - Да се очекује израда и усвајање новог Закона о информационој безбедности који би детаљније уредио израду Акта о процени ризика, предлажемо да се члан 7, „Завршна одредба“, преформулише тако што ће се предвидети дужи период за усаглашавање пословања привредних субјеката са овим Правилником. На овај начин би се постигла већа транспарентност процеса и омогућило привредним субјектима да обавезе предвиђене овим Правилником уврсте у своје годишње пословне планове и обезбеде буџет за њихову реализацију. Сходно свему наведеном реално је очекивати да се наведене измене и буџет	**Примедба је размотрена и предлог се не прихвата** Нацрт правилника не уводи значајан број додатних обавеза за привредне субјекте у односу на постојеће обавезе које имају према позитивним прописима, те по нашем мишљењу, нема потребе за померањем рока за примену.

планирају за пословну 2026. годину те предлажемо да члан 7. гласи: „Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије“ а примењује се од 1. децембра 2026. године.“	

CETIN:

1. Нацртом правилника се уређује област информационе безбедности у сектору електронских комуникација, што је већ на исти или сличан начин уређено Законом о информационој безбедности и пратећим подзаконским актима, па је питање који акти имају примат у примени у случају међусобних неусаглашености, као и где су границе надлежности Регулатора из Закона и Националног ЦЕРТ-а из Закона о информационој безбедности. Ово додатно може компликовати ефективну примену Нацрта правилника након планиране измене Закона о информационој безбедности, која је најављена за крај године.	**Примедба је размотрена и предлог се не прихвата** У изради Нацрта правилника узете су у обзир надлежности Регулатора, из члана 11. ЗИБ-а и чл. 7. став 4. тачка 4), 9. став 1. тачка 28), 34. став 1. тачка 10), 157. и 161. Закона. ЗИБ јасно прописује надлежности Националног ЦЕРТа, а Закон надлежности Регулатора у области безбедности и интегритета јавних електронских комуникационих мрежа и услуга и терминалне опреме. Измене и допуне или доношење нових закона захтевају измену и допуну или доношење новог подзаконског акта.
2. Чланом 157. став 5. Закона прописано је да привредни субјект обавештава Регулатора о свакој повреди интегритета и безбедности јавних електронских комуникационих мрежа и услуга у складу са прописима којима се уређује информациона безбедност, што обухвата и критеријуме за обавештавање. Ставом 7. истог члана Закона прописано да Регулатор само ближе уређује поступак обавештавања из става 3. и 5. Стога сматрамо да овим правилником не треба прописивати критеријуме за	**Примедба је размотрена и предлог се не прихвата** Одредбом члана 34 . став 1. тачка 10) Закона прописано је да је привредни субјекат дужан да на захтев Регулатора достави све потребне податке и информације које су неопходне за процењивање безбедности и интегритета електронских комуникационих мрежа и услуга укључујући, између осталог,

обавештавање о инцидентима, односно да треба из правилника искључити Прилог 2.	обезбеђивање континуитета рада. Такође, одредбом става 7. члана 157. Закона, осим ближег уређивања поступка обавештавања Регулатора о свакој повреди интегритета и безбедности јавних електронских комуникационих мрежа и услуга у складу са прописима којима се уређује информациона безбедност, такође је прописна надлежност Регулатора да ближе уреди примену адекватних техничких и организационих мера из члана 157. став 1. Закона, а посебно мера за превенцију и минимизацију утицаја безбеднсних инцидента по кориснике и међуповезане мреже, као и мере за обезбеђивања континуитета рада јавних комуникационих мрежа и услуга. Наведене мере су у директној вези са критеријумима за обавештавање о инцидентима у области електронских комуникација из Прилога 2. Нацрта правилника. Квантитативни и квалитативни критеријуми за обавештавање из Прилога 2. Нацрта правилника су засновани на ENISA документу„ Tehnical Guidline on incident reporting under the EECC ", из марта 2021. године који је у примени у Европској Унији.
3. У члану 3. став 3. тачка 1) Нацрта правилника помиње се „информационо-комуникациони систем од посебног значаја", који Нацртом правилника није ближе дефинисан, а Закон о информационој безбедности познаје појам „оператор информационо-комуникационог система" и „информационо-комуникациони систем". Предлажемо да се појмови ускладе ради уједначеног тумачења и ефективне примене оба прописа.	**Примедба је размотрена и предлог се не прихвата** ИКТ системи од посебног значаја су регулисани одредбама члана 6. ЗИБ-а и у Нацрту правилника се наводе у мери у којој Закон упућује на усклађеност са прописима којима се уређује информациона безбедност.
4. Чланом 4. Нацрта правилника прописано је да је, у циљу провере усклађености	**Примедба је размотрена и предлог се делимично прихвата**

примењених мера заштите, привредни субјект у обавези да, самостално или уз ангажовање спољних експерата, спроведе процену ризика и проверу усклађености примењених мера заштите из члана 3. овог правилника у складу са законом којим се уређује област информационе безбедности, узимајући при том у обзир резултате претходних провера усклађености. Осим тога, прописано је да је привредни субјект у обавези да, на захтев Регулатора, достави процену ризика и извештај о провери усклађености примењених мера заштите из члана 3. овог правилника, заједно са планом третирања ризика и планом уклањања уочених недостатака. С друге стране, члан 8. став 4. Закона о информационој безбедности прописује да је оператор ИКТ система од посебног значаја дужан да самостално или уз ангажовање спољних експерата врши проверу усклађености примењених мера ИКТ система са актом о безбедности ИКТ система од посебног значаја најмање једном годишње и да о томе сачини извештај. Ни према члану 157. став 7. Закона се као предмет Нацрта правилника не помиње процена ризика, па предлажемо да се изостави текст који се односи на процену ризика, односно на план третирања ризика. Наглашавамо да је процена ризика интерни акт који је означен као пословна тајна. Регулатор у складу са својим надлежностима које се односе на стручни надзор може да добије процену ризика на увид, како би се уверио да је овај интерни акт донет.	Одредбом чл. 157. став 8. тачка 1) и 34. став 1. тачка 10) Закона, између осталог, уређују се обавезе достављања података Регулатору од стране привредног субјекта, потребних за процену безбедности и интегритета мрежа и услуга. Акт о процени ризика и извештај о провери усклађености примењених мера заштите из члана 3. Нацрта правилника, као и план третирања ризика и план уклањања уочених недостатака су акти потребни за процену безбедности и интегритета мрежа и услуга. Одредбом члана 161. став 2. Закона, између осталог, прописано ја да је Регулатор, ради обављања послова стручног надзора, овлашћен да тражи од привредних субјеката и других лица потребне податке и информације. Даље, у складу са одредбом члана 35. Закона, Регулатор је у обавези да чува тајност прикупљених података који су означени као пословна тајна у складу са законом којим се уређује тајност података, односно који су означени као пословна тајна актом власника податка или уговором, у складу са законом. У складу са наведеним, Регулатор има овлашћење да захтева достављање акта о процени ризика без обзира да ли је наведени акт интерни акт који је означен као пословна тајна од стране привредног субјекта.