

На основу члана 157. став 7. Закона о електронским комуникацијама („Службени гласник РС”, број 35/23),

Савет Регулаторног тела за електронске комуникације и поштанске услуге, на 36. седници четвртог сазива одржаној 26. 4. 2024. године, доноси

ПРАВИЛНИК

о безбедности и интегритету јавних електронских комуникационих мрежа и услуга и терминалне опреме

Предмет примене

Члан 1.

Овим правилником ближе се уређује примена 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 Регулаторног тела за електронске комуникације и поштанске услуге (у даљем тексту: Регулатор) о свакој повреди безбедности и интегритета јавних електронских комуникационих мрежа и услуга која је значајно утицала на рад привредног субјекта.

Значење појединих појмова

Члан 2.

Поједини појмови који се употребљавају у овом правилнику имају следеће значење:

- 1) аутентичност је својство које значи да је могуће проверити и потврдити да је информацију створио или послао онај за кога је декларисано да је ту радњу извршио;
- 2) безбедносна политика је скуп правила који дефинишу на који начин средства и ресурси информационе технологије треба да се користе и штите, као и начин на који се њима

управља, односно акта које је привредни субјект дужан да донесе у складу са законом који уређује област информационе безбедности;

3) доступност (распољивост) је својство којим се обезбеђује приступачност и употребљивост јавних електронских комуникационих мрежа и/или услуга или терминалне опреме која омогућава приступ интернету на захтев лица или процеса;

4) интегритет је својство које обезбеђује да подаци или информације који се стварају, обрађују, преносе или чувају путем јавних електронских комуникационих мрежа и/или услуга, јавне комуникационе мреже и/или услуге и делови од којих се састоје нису промењени или уништени на неовлашћени начин;

5) поверљивост је својство којим се обезбеђује да су информације и функције јавних електронских комуникационих мрежа и/или услуга или терминалне опреме која омогућава приступ интернету доступне само овлашћеним лицима;

6) претња представља сваку околност, догађај или радњу која може да угрози, поремети или на други начин штетно утиче на јавне електронске комуникационе мреже и/или услуге или терминалну опрему која омогућава приступ интернету, кориснике и друга лица;

7) рањивост представља слабост или недостатак у јавним електронским комуникационим мрежама и/или услугама или терминалној опреми који се могу искористити за реализацију једне или више претњи;

8) ризик је постојање услова за нарушавање безбедности јавних електронских комуникационих мрежа и/или услуга, односно исправног функционисања јавних електронских комуникационих мрежа и/или услуга или терминалне опреме која омогућава приступ интернету, чији се ниво одређује проценом вероватноће да се догоди одређена последица по ниво информационе безбедности и проценом обима те последице.

Други појмови који се употребљавају у овом правилнику имају значење прописано законима којима се уређују електронске комуникације и информациона безбедност.

Обавезе привредних субјеката

Члан 3.

Привредни субјект је дужан да, ради обезбеђивања безбедности и интегритета својих мрежа и услуга, тајности комуникација, заштите података о личности, саобраћају и локацији, примени адекватне техничке и организационе мере, примерене постојећим ризицима, што обухвата и енкрипцију у одговарајућим случајевима, а посебно мере за превенцију и минимизацију утицаја безбедносних инцидената на кориснике и међуповезане мреже и услуге, као и мере за обезбеђивања континуитета рада јавних комуникационих мрежа и услуга.

Техничке и организационе мере из става 1. овог члана, привредни субјект је дужан да примени и за спречавање неовлашћеног коришћења терминалне опреме која омогућава приступ интернету и која је дата на коришћење кориснику.

У спровођењу техничких и организационих мера из става 1. овог члана привредни субјект примењује мере:

- 1) заштите информационо-комуникационих система од посебног значаја у складу са законом којим се уређује област информационе безбедности;
- 2) мере које се односе на обраду податка о личности у складу са законом којим се уређује област заштите података о личности.

У предузимању мера из ст. 1. и 3. овог члана, привредни субјект примењује техничке смернице о безбедносним мерама и претњама у области електронских комуникација Агенције за сајбер безбедност Европске Уније (ENISA) и српске стандарде за спровођење техничких и организационих мера безбедности (у даљем тексту: српски стандарди).

Српски стандарди су наведени у Прилогу 1, који је одштампан уз овај правилник и чини његов саставни део.

Привредни субјект је дужан да на захтев Регулатора достави све потребне податке и информације о примени мера из ст. 1. и 3. овог члана, укључујући и документа која се односе на безбедносну политику.

Регулатор надзире примену мера из ст. 1. и 3. овог члана и може да предложи привредном субјекту примену додатних мера заштите у складу са одговарајућим нивоом безбедности.

Провера усклађености примењених мера заштите

Члан 4.

Привредни субјект је 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.

Привредни субјект је 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.

У случају да се план уклањања уочених недостатака из става 2. овог члана не оцени примереним за спречавање и умањење утицаја безбедносних инцидената на кориснике услуга и/или за обезбеђивање безбедности мрежа и услуга, Регулатор може привредном субјекту да одреди додатне мере.

Ако Регулатор у поступку обављања стручног надзора утврди неправилности, недостатке или пропусте у примени мера, а нарочито мера у сврху спречавања безбедносних инцидената када се утврди значајна претња, за уклањање последица безбедносног инцидената и заштите у циљу отклањања откривених рањивости о томе обавештава привредног субјекта и одређује му рок у коме је дужан да их отклони.

Обавештавање Регулатора о безбедносним инцидентима

Члан 5.

Привредни субјект је дужан, да без одлагања, а најкасније наредног радног дана од дана сазнања о настанку безбедносног инцидента, обавести Регулатора о сваком безбедносном инциденту, који је значајно утицао на његов рад, а који испуњава квантитативне и квалитативне критеријуме за обавештавање (у даљем тексту: критеријуми за обавештавање), при чему прво проверава испуњеност квантитативних критеријума, а уколико они нису испуњени проверава испуњеност квалитативних критеријума.

У случају настанка безбедносног инцидента који испуњава критеријуме из прописа којим се уређује поступак обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, привредни субјект је у обавези да Регулатору достави обавештење о наведеном инциденту, без одлагања, а најкасније наредног радног дана од дана сазнања о настанку безбедносног инцидента, без обзира да ли безбедносни инцидент испуњава критеријуме за обавештавање.

Критеријуми за обавештавање дати су у Прилогу 2, који је одштампан уз овај правилник и чини његов саставни део.

Привредни субјект доставља Регулатору обавештење о безбедносном инциденту из ст. 1. и 2. овог члана путем портала за пријем обавештења о безбедносним инцидентима у области електронских комуникација.

У случају хитности, обавештење о инциденту из ст. 1. и 2. овог члана пријављује се и телефоном или електронским путем.

Приликом пријаве безбедносног инцидента, привредни субјект је у обавези да наведе податке о контакт особи ради брзе размене информација о безбедносним инцидентима и пружања потребних техничких информација Регулатору.

У случају да дође до нарушавања редувантности система привредног субјекта, односно испада бар једног од редувантних елемената електронске комуникационе мреже, привредни субјект је дужан да наведени безбедносни инцидент пријави као инцидент који има утицаја на редувантност.

Привредни субјект је дужан да Регулатору, након пријаве инцидента, достави:

- 1) обавештења о битним догађајима у вези са инцидентом и активностима које предузима до престанка инцидента, у случају безбедносног инцидента из става 1. овог члана, уколико је инцидент и даље у току;
- 2) обавештења и извештаје током и након инцидента, који су предвиђени законом којим се уређује област информационе безбедности, у случају безбедносног инцидента из става 2. овог члана;
- 3) обавештење о престанку инцидента из ст. 1. и 2. овог члана, најкасније у року од једног сата од када је инцидент отклоњен;
- 4) завршни извештај о безбедносном инциденту из ст. 1. и 2. овог члана, у року од 15 дана од дана његовог престанка, који мора да садржи детаљне податке о врсти и опису безбедносног инцидента, времену настанка и трајању, последицама које је изазвао, евентуалном прекограничном дејству, предузетим активностима ради отклањања последица и друге информације од значаја за евидентирање и статистичку обраду безбедносног инцидента.

Регулатор може да тражи додатна обавештења ради прецизирања детаља насталог безбедносног инцидента из ст. 1. и 2. овог члана, као и додатна обавештења о битним догађајима у вези са безбедносним инцидентом који је и даље у току и активностима које се предузимају до престанка тог инцидента.

У случају пријављеног безбедносног инцидента из ст. 1. и 2. овог члана, Регулатор може да наложи евентуалну допуну извештаја, предузимање других мера за спречавање или отклањање безбедносног инцидента и мера за отклањање последица безбедносног инцидента, укључујући и давање одређених препорука, смерница и упозорења о безбедносним претњама и покретање одговарајућег поступка из надлежности Регулатора.

Привредни субјект може да обавести Регулатора и о другим претњама и безбедносним инцидентима које сматра значајним, а који нису уређени ст. 1. и 2. овог члана.

Привредни субјект је дужан да, на захтев Регулатора, достави статистичке податке о свим безбедносним инцидентима у претходној години.

**Обавештавање корисника о посебним ризицима односно претњама повреде
безбедности и интегритета**

Члан 6.

Привредни субјект је дужан да, без одлагања, у случају постојања посебног ризика, односно претње повреде безбедности и интегритета јавних електронских комуникационих мрежа и/или услуга или терминалне опреме која омогућава приступ интернету, о том ризику односно претњи (неовлашћени приступ, значајан губитак података, угрожавања тајности комуникација, безбедности података о личности и друго), обавести кориснике на јасан и документован начин, путем своје веб презентације.

У случају да је ризик односно претња из става 1. овог члана ван опсега мера које је привредни субјект дужан да примени, привредни субјект је у обавези да обавести кориснике на које би такав ризик односно претња могла да утиче, о могућим мерама заштите које корисник може да примени, као и о евентуалним трошковима везаним за примену тих мера.

Завршна одредба

Члан 7.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”, а примењује се од 1. децембра 2025. године .

Број 1-01-_____

У Београду, _____ 2024. године

ПРЕДСЕДНИК САВЕТА

Драган Ковачевић

**СПИСАК СРПСКИХ СТАНДАРДА ЗА СПРОВОЂЕЊЕ
ТЕХНИЧКИХ И ОРГАНИЗАЦИОНИХ МЕРА БЕЗБЕДНОСТИ**

Назив референтног стандарда	Ознака референтног стандарда
Безбедност информација, сајбер безбедност и заштита приватности – Системи менаџмента безбедношћу информација	SRPS ISO/IEC 27001
Безбедност информација, сајбер безбедност и заштита приватности – Контроле безбедности информација	SRPS ISO/IEC 27002
Безбедност информација, сајбер безбедност и заштита приватности – Упутство за управљање ризицима по безбедност информација	SRPS ISO/IEC 27005
Сајбер безбедност – Односи са испоручиоцима – Део 3: Смернице за безбедност ланца снабдевања хардвером, софтвером и услугама	SRPS ISO/IEC 27036-3
Безбедност и отпорност - Системи менаџмента континуитетом пословања	SRPS EN ISO 22301

КВАНТИТАТИВНИ И КВАЛИТАТИВНИ КРИТЕРИЈУМИ ЗА ОБАВЕШТАВАЊЕ**I КВАНТИТАТИВНИ КРИТЕРИЈУМИ ЗА ОБАВЕШТАВАЊЕ**

Утицај на доступност (расположивост)	Минимални број корисника на који утиче безбедносни инцидент	Трајање безбедносног инцидента (више од)
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној фиксној комуникационој мрежи	20.000	8 сати
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној фиксној комуникационој мрежи	40.000	6 сати
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној фиксној комуникационој мрежи	100.000	4 сата
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној фиксној комуникационој мрежи	200.000	2 сата
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној фиксној комуникационој мрежи	300.000	1 сат
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној мобилној комуникационој мрежи	80.000	8 сати
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној мобилној комуникационој мрежи	160.000	6 сати
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној мобилној комуникационој мрежи	400.000	4 сата
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној мобилној комуникационој мрежи	800.000	2 сата
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној мобилној комуникационој мрежи	1.200.000	1 сат

Услуге приступа интернету у јавној фиксној комуникационој мрежи	20.000	8 сати
Услуге приступа интернету у јавној фиксној комуникационој мрежи	40.000	6 сати
Услуге приступа интернету у јавној фиксној комуникационој мрежи	100.000	4 сата
Услуге приступа интернету у јавној фиксној комуникационој мрежи	200.000	2 сата
Услуге приступа интернету у јавној фиксној комуникационој мрежи	300.000	1 сат
Услуге приступа интернету у јавној мобилној комуникационој мрежи	70.000	8 сати
Услуге приступа интернету у јавној мобилној комуникационој мрежи	140.000	6 сати
Услуге приступа интернету у јавној мобилној комуникационој мрежи	350.000	4 сата
Услуге приступа интернету у јавној мобилној комуникационој мрежи	700.000	2 сата
Услуге приступа интернету у јавној мобилној комуникационој мрежи	1.000.000	1 сат
Комуникациона услуга између лица која није заснована на нумерацији	70.000	8 сати
Комуникациона услуга између лица која није заснована на коришћењу нумерације	140.000	6 сати
Комуникациона услуга између лица која није заснована на коришћењу нумерације	350.000	4 сата
Комуникациона услуга између лица која није заснована на коришћењу нумерације	700.000	2 сата
Комуникациона услуга између лица која није заснована на коришћењу нумерације	1.000.000	1 сат
Утицај на Аутентичност/Интегритет/Поверљивост		
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној фиксној комуникационој мрежи	20.000	Независно од трајања
Комуникациона услуга између лица заснована на коришћењу нумерације у јавној мобилној комуникационој мрежи	80.000	Независно од трајања
Услуге приступа интернету у јавној фиксној комуникационој мрежи	20.000	Независно од трајања
Услуге приступа интернету у јавној мобилној комуникационој мрежи	70.000	Независно од трајања

Комуникациона услуга између лица која није заснована на нумерацији	70.000	Независно од трајања
--	--------	----------------------

II КВАЛИТАТИВНИ КРИТЕРИЈУМИ ЗА ОБАВЕШТАВАЊЕ

<p>Безбедносни инцидент се односи на:</p> <ul style="list-style-type: none"> - Комуникациону услугу између лица засновану на коришћењу нумерације у јавној фиксној комуникационој мрежи - Комуникациону услугу између лица засновану на коришћењу нумерације у јавној мобилној комуникационој мрежи - Услугу приступа интернету у јавној фиксној комуникационој мрежи - Услугу приступа интернету у јавној мобилној комуникационој мрежи - Комуникациону услугу између лица која није заснована на нумерацији - Услугу комуникације између машина - Услугу дистрибуције медијских садржаја 	<p>Утицај на :</p> <p>Доступност (Расположивост)/ Аутентичност /Интегритет/ Поверљивост</p>
<p>1. Значајан због, безбедносним инцидентом, обухваћеног географског подручја: прекогранично/државе/аутономних покрајина/округа/ градова као и подручја у којима би, услед инцидента, у потпуности било онемогућено коришћење јавних електронских комуникационих услуга.</p> <p>2. Значајан због утицаја на друштво и економију: Немогућност приступа националним бројевима за хитне службе, утицај на националне системе за упозоравање, велика материјална штета, висок ризик по јавну безбедност, губитак живота, медијска покривеност (вести), утицај на континуитет рада субјеката који су класификовани као ИКТ систем од посебног значаја у складу са законом којим се уређује област информационе безбедности, утицај на</p>	<p>Независно од трајања и броја корисника</p>

критичну инфраструктуру, утицај у току посебно значајних дана као што су дани избора, референдума и сл.	
---	--

Образложење

I. Правни основ:

Правни основ за доношење Правилника о безбедности и интегритету јавних електронских комуникационих мрежа и услуга и терминалне опреме (у даљем тексту: Правилник), садржан је у одредби члана 157. став 7. Закона о електронским комуникацијама („Службени гласник РС“, број 35/23, у даљем тексту: Закон).

Одредбом члана 157. став 7. Закона прописано је 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.

II. Разлози за доношење Правилника

Доношење Правилника иницирано је доношењем Закона, који је Народна скупштина Републике Србије донела на Другој седници Првог редовног заседања у 2023. години, 28. априла 2023. године и који је ступио на снагу 7. маја 2023. године.

III. Образложење појединих решења

У члану 1. Правилника наведен је предмет уређивања.

У члану 2. Правилника наведено је значење појединих појмова употребљених у Правилнику.

У чл. 3. и 4. Правилника наведене су техничке и организационе мере, укључујући и проверу усклађености примењених мера заштите.

У члану 5. Правилника је прописан поступак обавештавања Регулатора о безбедносним инцидентима.

У члану 6. Правилника је прописан поступак обавештавања корисника о посебним ризицима односно претњама повреде безбедности и интегритета.

Чланом 7. прописано је да овај правилник ступа на снагу осмог дана од објављивања у „Службеном гласнику Републике Србије“, а да се примењује од 1. децембра 2025. године.

IV. Предлог даљих активности

Предлаже се да Савет Регулатора размотри и усвоји Нацрт овог правилника, као и да исти, након тога, Регулатор, у складу са одредбама чл. 36. и 37. Закона, упути на јавне консултације у трајању од 30 дана.

Након спроведених јавних консултација, извршиће се обрада и анализа приспелих примедба, предлога и сугестија и Савету Регулатора ће се доставити одговарајући Предлог правилника.

По усвајању Предлога правилника, овај општи акт ће, сагласно члану 27. став 2. Закона и члану 57. став 1. Закона о државној управи („Службени гласник РС“, бр. 79/05, 101/07, 95/10, 99/14, 30/18 – др. закон и 47/18), бити упућен надлежном министарству, ради прибављања мишљења о његовој уставности и законитости. По добијеном мишљењу надлежног министарства, предметни правилник ће бити објављен у „Службеном гласнику Републике Србије“.

V. Средства за спровођење Правилника

За спровођење овог правилника, ради реализације портала, преко кога би се примала обавештења о инцидентима и њиховом току, која су привредни субјекти дужни да доставе Регулатору, потребно је обезбедити посебна средства у финансијском плану Регулатора.