РЕПУБЛИКА СРБИЈА

РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ
Савет Регулатора / Национални ЦЕРТ
Палмотићева 2
11103 Београд
Електронска пошта: **ratel@ratel.rs**

ПОДАЦИ О ПОДНОСИОЦУ

М[redacted] М[redacted]
ПТТ адреса: [redacted], 11420 Смедеревска Паланка
Е-пошта: [redacted]

Својство у коме се поднесак подноси:
заинтересован грађанин

НАЗИВ ПОСТУПКА

Јавне консултације о Нацрту правилника о садржају, начину уписа и вођења евиденције посебних центара за превенцију безбедносних ризика у информационо-комуникационим системима

ПРЕДМЕТ

ПРИМЕДБЕ, ПРЕДЛОЗИ И АМАНДМАНСКЕ ФОРМУЛАЦИЈЕ НА НАЦРТ ПРАВИЛНИКА

I. ПРОЦЕСНИ ОСНОВ

Овај поднесак се доставља у оквиру јавних консултација које Регулаторно тело за електронске комуникације и поштанске услуге спроводи на основу чл. 36. и 37. Закона о електронским комуникацијама.

Чланом 36. Закона уређена је обавеза Регулатора да спроводи јавне консултације у поступку доношења аката из своје надлежности, ради прибављања мишљења стручне и шире јавности. Чланом 37. уређује се програм јавних консултација и објављивање релевантних података о поступку. (Pravno-informacioni sistem)

РАТЕЛ је у званичном обавештењу навео:

- да су консултације започеле 25. јуна 2026. године;
- да је рок за достављање мишљења 30 дана;
- да се поднесци достављају у писаном облику;
- да поднесак треба да садржи име, односно назив и контактне податке;
- да се мишљења објављују на веб-презентацији Регулатора. (Ratel)

Правни основ за доношење самог Правилника предлагач налази у члану 35. став 5. Закона о информационој безбедности, којим је прописано да орган, односно организација у којој се обављају послови Националног ЦЕРТ-а, прописује садржај, начин уписа и вођења евиденције посебних ЦЕРТ-ова. То је наведено и у Нацрту и његовом образложењу.

II. УВОДНА РАЗМАТРАЊА

Посебни центри за превенцију безбедносних ризика у информационо-комуникационим системима имају значајну улогу у:

- превенцији и откривању сајбер-инцидената;
- пријему и обради пријава;
- подршци корисничким заједницама;
- размени информација;
- координацији одговора;
- развоју секторских и организационих капацитета;
- подизању опште отпорности информационо-комуникационих система.

Зато су оправдани циљеви да се:

- Евиденција учини тачнијом и ажурнијом;
- мандат и корисничка заједница сваког посебног ЦЕРТ-а јасније идентификују;
- јавни контактни подаци стандардизују;
- подстакне развој организационе и оперативне зрелости;
- унапреди сарадња са Националним ЦЕРТ-ом.

Овај поднесак не оспорава наведене циљеве.

Примедбе се односе на начин на који се ти циљеви нормативно спроводе, нарочито на:

1. границе законског овлашћења;
2. правну природу RFC 2350 и SIM3;
3. одсуство тачно одређене SIM3 верзије;
4. могућност фактичког динамичког упућивања на спољни стандард;
5. зависност од спољног онлајн алата;
6. обим и јавност података;
7. безбедност електронског достављања;
8. критеријуме провере самопроцене;
9. права подносиоца;
10. учесталост ажурирања;
11. рокове;

12. услове и поступак брисања;
13. трошкове и институционалне капацитете;
14. усклађеност образаца са нормативним текстом.

Циљ поднеска је конструктиван: да се задржи оправдана намера Нацрта, али да се пре усвајања обезбеде правна сигурност, сразмерност, информациона безбедност, заштита података и применљив управни поступак.

III. ОПШТА ОЦЕНА НАЦРТА

1. Позитивна решења

Позитивно је што Нацрт:

- уређује нови подзаконски режим после доношења Закона о информационој безбедности;
- прецизније набраја основне регистарске податке;
- предвиђа доношење решења у управном поступку;
- уводи обавезу пријављивања промена;
- покушава да уједначи представљање мандата и услуга кроз RFC 2350;
- подстиче организационо преиспитивање кроз SIM3;
- предвиђа да SIM3 самопроцена не буде јавно доступна;
- уводи опомену пре могућег покретања поступка брисања;
- предвиђа прелазни период за постојеће посебне ЦЕРТ-ове.

2. Општи системски недостаци

Нацрт, међутим, не обезбеђује довољно јасан одговор на следећа питања:

- која верзија SIM3 се примењује;
- који параметри и дефиниције нивоа су правно меродавни;
- ко може изменити модел;
- да ли будућа измена модела аутоматски мења домаће обавезе;
- да ли је спољни онлајн алат обавезан;
- који се подаци шаљу спољном сервису;
- где и по ком праву се подаци обрађују;
- ко проверава самопроцену;
- по којој методологији;
- да ли су оцењивачи обучени;
- који је минимални прихватљиви ниво;
- какав је статус параметара испод нивоа 2;
- да ли низак ниво може довести до одбијања или брисања;
- колико често се може захтевати нова самопроцена;
- који је рок за одлучивање;
- које је правно средство;
- који су материјални услови за брисање;
- када брисање производи дејство;
- колики су стварни трошкови примене.

3. Документа која нису представљена јавности

Уз Нацрт нису јавно представљени, односно из објављеног материјала се не може утврдити да постоје:

- потпуна правна анализа граница члана 35. став 5. Закона;
- табела усклађености са NIS2;

- анализа различитих SIM3 верзија;
- лиценцна анализа;
- анализа токова података кроз онлајн алат;
- процена утицаја на заштиту података;
- процена ризика информационе безбедности;
- процена кадровских капацитета;
- анализа административних трошкова;
- анализа утицаја на мала и средња предузећа;
- извештај о пилот-тестирању;
- анализа алтернативних модела.

У образложењу је наведено да за спровођење Правилника није потребно обезбедити посебна средства у финансијском плану Регулатора. Та констатација није праћена обрачуном радних сати, трошкова развоја система, обуке, архивирања, безбедносних мера или трошкова подносилаца.

4. Критични ризици

Најзначајнији ризици су:

- прекорачење регистарског законског овлашћења;
- динамичко упућивање на спољни модел;
- прикривена квазиакредитација;
- прекомерно прикупљање личних података;
- откривање физичких и оперативних локација;
- компромитација SIM3 слабости и планова;
- незаштићена електронска достава;
- неуједначена стручна провера;
- селективно захтевање ажурирања;
- брисање без потпуно одређеног поступка;
- несразмеран утицај на мале и новоосноване тимове;
- непроцењени буџетски и привредни трошкови.

IV. АНАЛИЗА СПОРНИХ ОДРЕДАБА И ПРЕДЛОЗИ ИЗМЕНА

ЧЛАН 1 — ПРЕДМЕТ

Одредба

Чланом 1. прописује се да се Правилником ближе уређују садржај, начин уписа и вођења Евиденције.

Примедба

Нацрт, поред регистарских питања, уводи:

- обавезну свеобухватну процену зрелости;
- планове развоја;
- периодично поновно оцењивање;
- могућу статусну последицу брисања.

Није довољно јасно да ли је упис само регистарски статус или представља и државну потврду организационе способности.

Образложење

SIM3 самопроцена није независни аудит. Упис не сме бити схваћен као акредитација, сертификација или гаранција квалитета.

Ризик

- обмањујуће тржишно представљање;
- коришћење уписа као услова јавне набавке;
- неосновано ослањање корисника;
- прикривена сертификација.

Предлог измене

После постојећег става додати:

„Евиденција има регистарску, статусну, информативну и координациону функцију.

Упис у Евиденцију не представља акредитацију, сертификацију, независну стручну процену нити гаранцију квалитета, капацитета или компетентности Посебног ЦЕРТ-а, осим потврде да је упис извршен у складу са законом и овим правилником.“

ЧЛАН 2 — RFC 2350 И SIM3

Одредба

Нацрт дефинише RFC 2350 као текстуални документ о капацитетима, услугама и безбедној комуникацији, а SIM3 као модел зрелости који развија и одржава Open CSIRT Foundation. Упућује се на спољне веб-адресе, али се не наводи верзија SIM3.

Примедба

Нису утврђени:

- тачан назив и статус RFC 2350;
- BCP ознака и датум;
- тачна SIM3 верзија;
- нормативно меродаван текст;
- услови примене будућих измена;
- домаћи превод;
- домаћи офлајн формат.

RFC 2350 је BCP 21 из јуна 1998. године и представља Internet Best Current Practice, а не пропис или сертификат. (RFC Editor)

Ризик

- променљиве обавезе;
- правна несигурност;
- зависност од спољне организације;
- различито тумачење;
- неједнак положај подносилаца.

Предлог измене

Члан 2. изменити тако да гласи:

„1) RFC 2350 је документ ‘Expectations for Computer Security Incident Response’, RFC 2350, BCP 21, објављен у јуну 1998. године, који се за потребе овог правилника примењује у обиму утврђеном Прилогом 3;

2. SIM3 самопроцена је интерна процена зрелости Посебног ЦЕРТ-а извршена применом модела Security Incident Management Maturity Model — SIM3, верзија _____, од _____, у обиму утврђеном Прилогом 4.

RFC 2350 и SIM3 представљају техничке и стручне референтне оквире и немају самостално дејство прописа Републике Србије.

Накнадна измена, допуна или замена спољног документа, модела или онлајн алата не мења права и обавезе из овог правилника без измене Правилника.

> Регулатор пре почетка примене објављује домаће упутство, терминолошки речник и електронске обрасце на српском језику и ћириличком писму.
>
> Коришћење спољног онлајн алата није обавезан услов за упис.“

ЧЛАН 3 — САДРЖАЈ ЕВИДЕНЦИЈЕ

Одредба

Члан 3. предвиђа, између осталог:

- пуну адресу Посебног ЦЕРТ-а;
- телефон и факс;
- категорију величине;
- јавни RFC линк;
- SIM3 самопроцену;
- адресу одговорног лица;
- разлог и датум брисања.

Примедба

Израз „адреса одговорног лица“ није довољно одређен и може обухватити адресу пребивалишта или боравишта.

Пуна адреса Посебног ЦЕРТ-а може представљати:

- адресу матичног правног лица;
- поштанску адресу;
- оперативну локацију;
- резервну локацију;
- локацију техничке инфраструктуре.

Категорија величине заснована на броју физичких чланова не разликује пуно и непуно радно време.

Ризик

- прекомерна обрада;
- физичко угрожавање;
- откривање оперативне локације;
- нетачна категоризација;
- већа последица повреде података.

Предлог измене

Тачку о одговорном лицу изменити тако да гласи:

> „Подаци о одговорном лицу: име и презиме, функција или радно место, службени контакт телефон, службена адреса електронске поште и датум почетка и престанка овлашћења.
>
> Адреса пребивалишта или боравишта, приватни телефон и приватна адреса електронске поште не прикупљају се.“

Податак о адреси Посебног ЦЕРТ-а заменити:

> „службеном адресом правног лица или адресом за пријем поште и местом у коме Посебан ЦЕРТ претежно обавља послове, без јавног објављивања оперативне, резервне или техничке локације“.

Категорију величине одређивати према еквиваленту пуног радног времена.

Увести и:

- верзију RFC документа;
- датум последње измене;
- контролну суму архивске копије;

- SIM3 верзију;
- датум самопроцене;
- датум последње провере тачности;
- статус уписа.

ЧЛАН 4 — УСЛОВИ ЗА УПИС

Одредба

Члан 4. предвиђа да Посебан ЦЕРТ обавља послове у оквиру одређеног правног лица, групе правних лица, области пословања „и слично“.

Примедба

Израз „и слично“ је неодређен.

Није довољно уређен положај:

- академских тимова;
- непрофитних организација;
- секторских тимова;
- виртуелних и дистрибуираних тимова;
- заједничких тимова;
- малих и новооснованих ЦЕРТ-ова.

Ризик

- различита пракса;
- дискриминација организационих модела;
- тржишна баријера;
- нејасан носилац права и обавеза.

Предлог измене

> „Посебан ЦЕРТ обавља послове за унапред одређену корисничку заједницу, једно или више правних лица, јавни или привредни сектор, академску или истраживачку заједницу, професионално удружење, непрофитну организацију или другу одредиву групу корисника.
>
> Када је Посебан ЦЕРТ организациона јединица, подносилац пријаве и носилац права и обавеза јесте правно лице у чијем је саставу.
>
> Испуњеност услова процењује се сразмерно мандату, корисничкој заједници, услугама, величини и организационој форми.“

ЧЛАН 5 — ПРИЈАВА

Одредба

Пријава се подноси на Обрасцу 1.

Примедба

Није јасно:

- ко је странка ако је ЦЕРТ организациона јединица;
- ко сме да потпише пријаву;
- како се доказује овлашћење;
- где је обавештење о обради личних података.

Ризик

- пријава неовлашћеног лица;
- спор о странци;

- непотпуна обрада;
- недовољна транспарентност.

Предлог измене

> „Пријаву подноси законски заступник правног лица или друго писано или електронски овлашћено лице.
>
> Ако је Посебан ЦЕРТ организациона јединица, пријаву подноси правно лице у чијем је саставу.
>
> Национални ЦЕРТ објављује електронски попуњив образац, упутство, обавештење о обради података, правила поверљивости и упутство за безбедну доставу.“

ЧЛАН 6 — ДОКАЗИ, RFC И SIM3

Одредба

Нацрт захтева:

- извод из систематизације;
- јавно објављен RFC 2350;
- потпуну SIM3 самопроцену;
- линк ка онлајн резултатима;
- образложење и план унапређења за сваки параметар испод нивоа 2;
- проверу конзистентности од стране Националног ЦЕРТ-а.

Примедба

Систематизација доказује формално постојање радног места, али не и стварну оперативну способност. Не узимају се довољно у обзир:

- уговорно ангажована лица;
- заједнички ресурси;
- секторски споразуми;
- дистрибуирани тимови;
- стварно обављене активности.

Није дефинисано:

- шта значи провера конзистентности;
- ко је врши;
- по којим критеријумима;
- да ли службено лице може променити оцену;
- да ли странка има право на другу проверу.

ENISA свој оквир зрелости заснива на SIM3, али пуну процену не своди само на самопроцену: препознаје и peer review као засебан елемент. (ENISA)

Ризик

- формализам;
- искључење мањих тимова;
- скривени критеријуми;
- неједнака стручна оцена;
- прекомерна јавност;
- зависност од страног алата.

Предлог измене

> „Као доказ стварног оперативног капацитета могу се доставити акт о организовању, релевантан извод из систематизације, уговори о законитом

ангажовању у редигованом облику, споразум о заједничком или секторском тиму, извештаји о активностима и други проверљиви докази.

Подносилац доставља јавни RFC профил и, ако је потребно, заштићени оперативни анекс.

SIM3 самопроцена доставља се у локалном електронском формату. Линк ка спољном сервису је добровољан и помоћан.

План унапређења тражи се само за параметре чије је унапређење неопходно с обзиром на мандат, услуге и ризике.

Национални ЦЕРТ проверава потпуност, унутрашњу логичку доследност и очигледне противречности према јавној методологији.

Ако налаз може бити основ неповољне одлуке, подносиоцу се омогућава увид, изјашњење, достављање додатних доказа и друга стручна провера.

SIM3 самопроцена не представља независни аудит или сертификацију.“

ЧЛАН 7 — НАЧИН ПОДНОШЕЊА

Одредба

Нацрт најпре предвиђа електронско подношење на веб-презентацији, а затим достављање електронских докумената на адресу електронске поште Националног ЦЕРТ-а.

Примедба

Није јасно да ли постоји портал или се документација шаље обичним имејлом.

SIM3, планови и систематизација могу садржати веома осетљиве информације.

Ризик

- пресретање;
- неовлашћени приступ;
- spoofing;
- malware;
- губитак прилога;
- спор о времену и садржају доставе.

Предлог измене

„Пријава и документација подносе се преко заштићеног електронског система, електронског сандучета органа или другог система који обезбеђује поуздану идентификацију, интегритет и доказ о достављању.

Заштићени систем обезбеђује електронски потпис или печат, шифрован пренос, временски жиг, потврду пријема, број предмета, списак прилога и проверу интегритета.

Шифрована електронска пошта може се користити као резервни канал.

SIM3, планови унапређења и оперативни анекси не достављају се незаштићеним имејлом.

Техничка сметња на систему органа не може ићи на штету благовременог подносиоца.“

ЧЛАН 8 — ОДЛУЧИВАЊЕ

Одредба

Национални ЦЕРТ одлучује решењем, у складу са законом који уређује општи управни поступак.

Примедба

Нису посебно уређени:

- рок;
- допуна;
- право на изјашњење;
- увид у стручни налаз;
- садржај образложења;
- друго стручно мишљење;
- правно средство.

Ризик

- дуготрајан поступак;
- одлука изненађења;
- неуједначена оцена;
- необразложено одбијање;
- пропуштање правне заштите.

Предлог измене

> „Решење се доноси у року од 30 дана од пријема уредне пријаве, односно у року прописаном за посебан испитни поступак.
>
> Ако је пријава неуредна, подносилац се позива на допуну, уз навођење недостатка, правног основа, рока и последица непоступања.
>
> Пре неповољног решења подносиоцу се достављају релевантне чињенице, докази и стручне оцене и оставља најмање осам дана за изјашњење.
>
> Решење садржи оцену сваког услова, списак доказа, одговор на битне наводе, разлоге одлуке и поуку о правном средству.
>
> Низак ниво појединачног SIM3 параметра не може сам по себи бити разлог за одбијање ако су испуњени законски услови.“

ЧЛАН 9 — ПРОМЕНА ПОДАТАКА

Одредба

Све промене пријављују се у року од осам дана.

Примедба

Исти рок није примерен:

- хитном контакту за инцидент;
- адреси електронске поште;
- промени одговорног лица;
- статусној промени која зависи од другог регистра.

Образац 2 не садржи SIM3, иако је SIM3 податак Евиденције.

Ризик

- неупотребљив контакт;
- неажурна Евиденција;
- немогућност пријаве свих промена;
- губитак историје измена.

Предлог измене

> „Промена хитног контакта, службеног телефона, службене електронске поште или одговорног лица пријављује се без одлагања, а најкасније у року од 24 часа.
>
> Остале промене пријављују се у року од осам дана од правног или фактичког дејства.

Национални ЦЕРТ без одлагања исправља податак који је нетачно унео или објавио.

Евиденција чува датум, правни основ и службени траг сваке измене.“

ЧЛАН 10 — АЖУРИРАЊЕ САМОПРОЦЕНЕ

Одредба

Национални ЦЕРТ може захтевати потпуну ажурирану самопроцену, са роком од 15 дана. После опомене и додатног рока од 15 дана може покренути брисање.

Примедба

Нису одређени:

- разлози за захтев;
- учесталост;
- обим;
- могућност делимичне допуне;
- продужење;
- виша сила;
- услови брисања.

Ризик

- селективна примена;
- несразмеран трошак;
- пречесто оцењивање;
- брисање због привременог кашњења;
- преусмеравање ресурса са одговора на инциденте.

Предлог измене

„Ажурирање се може захтевати ако је прошло најмање 12 месеци, после значајне организационе промене, после документованог инцидента који доводи у питање актуелност података или ако постоји документована противречност.

Потпуна редовна самопроцена не захтева се чешће од једном у 12 месеци.

Рок за потпуну процену не може бити краћи од 30 дана. Рок од 15 дана може се одредити за ограничену исправку.

Рок се продужава због више силе, већег инцидента, реорганизације, техничке сметње или другог оправданог разлога.

Пре покретања брисања обавезни су опомена, додатни рок, право на изјашњење и могућност корективног плана.“

НОВИ ЧЛАН 10а — БРИСАЊЕ

Примедба

Нацрт помиње покретање поступка, али не уређује:

- материјалне разлоге;
- надлежно лице;
- садржај акта;
- право на изјашњење;
- блаже мере;
- дејство;
- правно средство;
- поновни упис.

Предложени нормативни текст

„Члан 10а

Поступак брисања покреће се писаним обавештењем које садржи чињенице, доказе, правни основ, конкретан разлог, рок од најмање 15 дана за изјашњење и могућност отклањања недостатка.

Брисање се може извршити ако Посебан ЦЕРТ:

1. више не испуњава законом прописане услове;
2. достави битно нетачне податке који су били одлучујући за упис; или
3. ни после захтева, опомене и додатног рока неоправдано не отклони недостатак који онемогућава законито вођење Евиденције.

Пре доношења решења процењују се тежина и трајање пропуста, стварни ризик, сарадња странке, могућност отклањања и блаже мере.

Брисање се врши образложеним решењем које садржи тест сразмерности, датум дејства, услове поновног уписа и поуку о правном средству.

Низак SIM3 резултат или нереализован план унапређења не могу сами по себи бити разлог за брисање ако такав разлог није прописан Законом.

Брисање се јавно евидентира после коначности решења, осим ако је законом друкчије прописано.“

ЧЛАН 11 — ЈАВНОСТ И ПОВЕРЉИВОСТ

Одредба

Јавни део садржи пуну адресу Посебног ЦЕРТ-а, електронску пошту и јавни RFC линк. Остали подаци су нејавни и, према тексту, користе се искључиво за ангажовање у случају ризика и инцидената.

Примедба

Наведена сврха није потпуна јер се нејавни подаци користе и за:

- упис;
- проверу;
- промену;
- ажурирање;
- брисање;
- правну контролу;
- архивирање.

Бинарна подела јавни/нејавни није довољна.

Ризик

- обрада ван декларисане сврхе;
- прекомерна јавност;
- неодговарајући приступ;
- откривање слабости;
- масовно прикупљање података.

Предлог измене

Увести четири нивоа:

1. јавни;
2. професионално ограничени;
3. нејавни управни;
4. строго ограничени безбедносни.

Јавни део треба да садржи:

- број уписа;
- назив;
- место или поштанску адресу;
- статус;
- датум уписа;
- генерички контакт;
- веб-презентацију;
- јавни RFC минимум.

Строго ограничени део треба да садржи:

- SIM3;
- планове;
- оперативне анексе;
- описе слабости;
- резервне контакте и локације.

Додати:

> „Приступ нејавним деловима заснива се на службеној потреби и принципу најмањег овлашћења. Сваки приступ, измена, преузимање и извоз се евидентира.
>
> Национални ЦЕРТ обезбеђује вишефакторску аутентификацију, шифровање, резервне копије, план опоравка и периодично тестирање.
>
> Рокови чувања утврђују се посебним прилогом.“

ЧЛАН 12 — ПРЕЛАЗНИ РЕЖИМ

Одредба

Нацрт упућује на „члан 2. тачка 1) подт. (9)–(10)“, иако такве подтачке у члану 2. не постоје. Предвиђа се рок од 30 до 90 дана, без критеријума.

Примедба

Унутрашње упућивање је погрешно.

Нема критеријума за избор између 30 и 90 дана.

Ризик

- неприменљива норма;
- неједнак третман;
- прекратак рок;
- губитак статуса без јасног поступка.

Предлог измене

> „Национални ЦЕРТ упућује постојећим Посебним ЦЕРТ-овима појединачан захтев са тачним списком података и докумената, SIM3 верзијом, упутством, безбедним каналом и роком.
>
> Основни рок износи 90 дана.
>
> Краћи рок, не краћи од 30 дана, може се одредити ако тим већ поседује прописану документацију, уз образложење.
>
> На захтев странке рок се може продужити за додатних 90 дана.
>
> Постојећи статус остаје на снази до коначног окончања поступка усклађивања.
>
> Пропуштање рока не доводи до аутоматског брисања.“

Погрешно упућивање заменити тачним упућивањем на релевантне подтачке члана 3. и члана 6.

ЧЛАН 13 — ПРАВНИ КОНТИНУИТЕТ

Одредба

Престаје да важи Правилник из 2020. године.

Примедба

Није уређено шта се дешава са:

- започетим поступцима;
- предузетим процесним радњама;
- ранијим решењима.

Предлог измене

> „Поступци започети пре ступања на снагу овог правилника окончаће се по пропису по коме су започети, осим ако подносилац затражи примену новог правилника.
>
> Решења донета пре ступања на снагу остају на снази до окончања поступка усклађивања.
>
> Раније процесне радње остају важеће ако нису супротне закону.“

ЧЛАН 14 — СТУПАЊЕ НА СНАГУ И ПРИМЕНА

Одредба

Правилник ступа на снагу осмог дана од објављивања.

Примедба

Осам дана није довољно за:

- домаће обрасце;
- упутство;
- безбедан портал;
- обуку;
- процене;
- контролу приступа;
- миграцију старих података.

Предлог измене

> „Правилник ступа на снагу осмог дана од објављивања.
>
> Одредбе о SIM3, плановима унапређења, заштићеној електронској достави, нивоима приступа и прелазном усклађивању примењују се по истеку 90 дана.
>
> Примена не може почети пре објављивања техничког упутства, домаћих образаца, успостављања безбедног канала, обуке овлашћених лица и утврђивања правила чувања и приступа.“

ОБРАЗАЦ 1

Примедбе

Образац:

- нема обавештење о обради;
- нема верзију SIM3;
- нема датум процене;
- нема контролни збир;
- нема поверљивост прилога;
- нема основ овлашћења потписника;

- не предвиђа електронски потпис;
- унапред наводи „У Београду“.

Предлог

Додати:

- податке о подносиоцу и овлашћењу;
- датум и верзију RFC;
- датум и верзију SIM3;
- локалну датотеку и hash;
- степен поверљивости сваког прилога;
- изјаву о тачности;
- изјаву о обавештавању лица;
- обавештење о обради;
- електронски потпис или печат.

Формулацију „У Београду“ заменити:

„У _____, дана _____ године.“

ОБРАЗАЦ 2

Примедбе

Образац:

- не садржи SIM3 промене;
- не садржи датум настанка промене;
- не садржи разлог;
- не садржи доказ;
- не садржи поље за исправку грешке органа;
- садржи спојени текст у наслову.

Предлог

Додати:

- број уписа и решења;
- постојећи и нови податак;
- датум настанка и сазнања;
- правни или фактички основ;
- доказ;
- поверљивост;
- RFC и SIM3 верзију;
- план унапређења;
- исправку грешке органа;
- образложење кашњења;
- електронски потпис.

V. МЕЂУНАРОДНИ И ЕВРОПСКИ СТАНДАРДИ

1. NIS2

Директива (ЕУ) 2022/2555 представља релевантно приступно мерило, али није непосредно применљив домаћи пропис.

NIS2 захтева да национално одређени CSIRT тимови имају адекватне ресурсе, безбедну инфраструктуру, континуитет и безбедне алате за размену информација. Она такође наглашава поверљивост и заштиту безбедносних и пословних интереса субјеката. (Eur-Lex)

Посебни ЦЕРТ-ови из домаћег система нису нужно истоветни национално одређеним CSIRT тимовима из чл. 10–12. NIS2.

Зато NIS2 не треба користити као непосредно оправдање да сваки посебни ЦЕРТ мора:

- користити SIM3;
- достићи исти ниво;
- објавити целокупан RFC;
- бити брисан због недостављања развојне процене.

2. RFC 2350

RFC 2350 је BCP 21 и представља општи оквир за јасно представљање мандата, услуга, политика, контаката и очекивања од CSIRT тима. Није пропис, сертификат или универзални систем зрелости. (RFC Editor)

Нацрт га оправдано користи као референтни оквир, али мора:

- ограничити јавни минимум;
- заштитити интерне процедуре;
- обезбедити верзионирање и аутентичност.

3. SIM3 и ENISA

ENISA CSIRT Maturity Framework заснован је на SIM3 и користи нивое Basic, Intermediate и Advanced. ENISA наглашава самопроцену, али и peer review као други битан елемент потпуније евалуације. (ENISA)

Зато домаћа административна провера не сме бити представљена као независна процена зрелости.

4. FIRST

FIRST користи SIM3 у поступку чланства, али поступак не почива само на самопроцени. FIRST CSIRT Services Framework служи за избор и унапређење портфолија услуга и не представља самосталан стандард квалитета сваког тима. (FIRST)

5. Trusted Introducer

Trusted Introducer поступци и независне професионалне процене не могу се изједначити са домаћим регистарским поступком и административном провером самопроцене.

6. Заштита података

Европски и конвенцијски стандарди захтевају:

- закониту и одређену сврху;
- минимизацију;
- ограничење чувања;
- безбедност;
- транспарентност;
- контролу прималаца;
- права лица.

Нацрт те стандарде само делимично операционализује.

VI. МАТРИЦА АМАНДМАНА

Бр.	Одредба	Кључна измена	Приоритет

1	Члан 1	Упис није акредитација или сертификат	I
2	Члан 2	Тачно одредити RFC 2350	I
3	Члан 2	Фиксирати SIM3 верзију	I
4	Члан 2	Забранити аутоматску примену будућих верзија	I
5	Члан 2	Домаће упутство и терминологија	I
6	Чл. 2. и 6	Офлајн SIM3 алтернатива	I
7	Члан 3	Опште начело минимизације	I
8	Члан 3	Брисање приватне адресе одговорног лица	I
9	Чл. 3. и 11	Ограничити јавну физичку адресу	I
10	Члан 3	Факс учинити необавезним	III
11	Члан 3	Величина према еквиваленту пуног радног времена	II
12	Члан 3	Верзионирање RFC и SIM3	I
13	Члан 4	Одредива корисничка заједница и пропорционалност	I
14	Члан 5	Овлашћени подносилац и обавештење о обради	I
15	Члан 6	Алтернативни докази стварног капацитета	I
16	Члан 6	Јавни RFC минимум и поверљиви анекс	I
17	Члан 6	Поверљивост SIM3 и планова	I
18	Члан 6	Јавна методологија провере	I
19	Члан 6	Право на другу стручну проверу	I
20	Члан 7	Безбедан портал и доказива достава	I
21	Члан 8	Рок за одлучивање	I
22	Члан 8	Допуна и право на изјашњење	I
23	Члан 8	Структурисано образложење и правно средство	I
24	Члан 9	Хитни контакти у року од 24 часа	II
25	Члан 9	Исправка грешке органа и историја промена	I
26	Члан 10	Критеријуми ажурирања	I

27	Члан 10	Ограничење учесталости	I
28	Члан 10	Рок 30 дана и продужење	I
29	Нови члан 10a	Потпун поступак брисања	I
30	Члан 11	Четири нивоа приступа	I
31	Члан 11	Рокови чувања, логовање и опоравак	I
32	Члан 12	Исправка погрешног упућивања	I
33	Члан 12	Основни прелазни рок од 90 дана	I
34	Члан 13	Правни континуитет	I
35	Члан 14	Одложена примена	I
36	Нови члан	Обавезно техничко упутство	I
37	Нови члан	DPIA и безбедносна процена	I
38	Нови члан	Подршка малим и новооснованим тимовима	II
39	Нови члан	Годишњи извештај и двогодишња евалуација	II
40	Образац 1	Потпуна замена и усклађивање	I
41	Образац 2	Потпуна замена и усклађивање	I
42	Цео текст	Номотехничка и језичка редактура	III

Детаљне нормативне формулације дате су у **Прилогу 2 — Амандманска табела**, који чини саставни део овог поднеска.

VII. ПРЕПОРУКЕ ЗА ПРИМЕНУ

1. Техничко упутство

Пре почетка примене треба објавити техничко упутство које садржи:

- домаћи RFC образац;
- тачну SIM3 верзију;
- тумачење параметара;
- примере доказа;
- правила поверљивости;
- формате;
- начин потписивања;
- начин шифроване доставе;
- поступак у случају техничке грешке;
- help-desk контакт.

Упутством се не смеју уводити нови материјални услови.

2. Безбедан портал

Портал треба да обезбеди:

- електронску идентификацију;
- вишефакторску аутентификацију;
- електронски потпис или печат;
- временски жиг;
- потврду пријема;
- број предмета;
- hash прилога;
- контролу приступа;
- логовање;
- шифровање;
- резервне копије;
- тестирани опоравак.

3. Прелазни период

Потребно је:

- одложити примену нових обавеза најмање 90 дана;
- омогућити додатно продужење;
- не рачунати рок пре објављивања упутства и обезбеђивања канала;
- обезбедити фазно достављање.

4. Обука

Пре примене треба:

- обучити најмање два лица која врше проверу;
- организовати бесплатну обуку за подносиоце;
- објавити снимак и материјале;
- успоставити корисничку подршку.

5. Процене

Пре обраде нових категорија података и употребе спољног сервиса треба:

- спровести процену утицаја на заштиту података;
- спровести процену ризика информационе безбедности;
- идентификовати сервере и место обраде;
- утврдити руковаоца, обрађиваче и подизвођаче;
- објавити неосетљиве сажетке.

6. Периодично извештавање

После 12 месеци треба објавити извештај о:

- пријавама;
- допунама;
- уписима;
- одбијањима;
- трајању поступка;
- захтевима за ажурирање;
- опоменама;
- брисањима;
- правним средствима;

- трошковима;
- положају МСП;
- регионалној структури;
- повредама података.

После 24 месеца треба спровести пуну процену ефеката.

VIII. ПРОЦЕСНИ ЗАХТЕВИ ПОДНОСИОЦА

Молим Регулаторно тело за електронске комуникације и поштанске услуге да:

1. Потврда пријема

Достави потврду да је овај поднесак примљен, са:

- датумом;
- временом;
- списком прилога;
- називом примљених датотека.

2. Заводни број

Достави број под којим је поднесак заведен у службеној евиденцији.

3. Објављивање поднеска

Објави овај поднесак у оквиру материјала јавних консултација, у складу са објављеним програмом, уз редиговање само оних личних података чије објављивање није неопходно.

4. Унос сваке примедбе у извештај

Сваку материјалну примедбу, предлог и амандманску формулацију унесе у извештај о јавним консултацијама, појединачно или у јасно идентификованим тематским групама.

5. Образложен одговор

За сваки прихваћени или неприхваћени предлог наведе:

- став Регулатора;
- правни основ;
- стручни разлог;
- чињенични или аналитички основ;
- измену која је извршена, ако је предлог прихваћен;
- разлог због ког измена није извршена, ако је предлог одбијен.

РАТЕЛ у својој објављеној пракси извештавања о јавним консултацијама користи структуру у којој се наводе мишљења учесника и став Регулатора, што је пример који треба применити и у овом поступку. (Ratel)

6. Извештај о консултацијама

Објави извештај о спроведеним јавним консултацијама у разумном року после њиховог окончања.

7. Коначни текст

Објави коначни текст Правилника пре, односно најкасније истовремено са његовим упућивањем у даљу процедуру, у мери у којој процес доношења то дозвољава.

8. Упоредни приказ

Објави упоредни приказ који садржи:

- текст Нацрта;
- текст после консултација;
- означене измене;

- извор или разлог сваке материјалне измене.

9. Технички проблеми

Без одлагања обавести подносиоца ако:

- неки прилог није примљен;
- датотека не може да се отвори;
- формат није прихватљив;
- прилог је оштећен;
- величина није дозвољена;
- постоји други технички недостатак.

Подносиоцу треба омогућити да технички недостатак отклони без губитка благовремености, ако је основни поднесак достављен у року.

10. Нови круг консултација

Ако после овог поступка буду битно измењени:

- SIM3 режим;
- верзија модела;
- обим података;
- јавност;
- начин провере;
- услови брисања;
- обрасци;
- електронски канал;
- прелазни режим,

објави нови или циљани круг јавних консултација о измењеном тексту и свим прилозима.

11. Документација

Објави или учини доступним, у неосетљивом делу:

- правну анализу;
- табелу NIS2 усклађености;
- анализу SIM3 верзије;
- процену утицаја на податке;
- процену информационе безбедности;
- анализу трошкова;
- резултате пилота;
- техничко упутство;
- правила чувања;
- политику поверљивости.

IX. ЗАКЉУЧНИ ПРЕДЛОГ

На основу изложеног, предлаже се да Савет Регулатора:

1. Не усвоји Нацрт у објављеном облику

Потребне измене нису само редакцијске, већ се односе на правни основ, права странака, безбедност, обраду података, трошкове и поступак брисања.

2. Усвоји Нацрт само уз битне измене

Као минимални услов треба прихватити:

- фиксирање SIM3 верзије;

- забрану аутоматских измена;
- домаће упутство;
- офлајн алтернативу;
- минимизацију података;
- брисање приватне адресе;
- ограничење јавне физичке адресе;
- јавни RFC минимум и поверљиви анекс;
- поверљивост SIM3;
- безбедан канал;
- рок за одлучивање;
- допуну и изјашњење;
- образложено решење;
- правно средство;
- критеријуме ажурирања;
- потпун поступак брисања;
- рокове чувања;
- логовање;
- исправку грешака;
- процене;
- исправку члана 12;
- нове обрасце;
- одложену примену.

3. Допуни образложење

Образложење треба да садржи:

- конкретан проблем;
- податке о примени важећег режима;
- разматране алтернативе;
- разлоге избора SIM3;
- анализу FIRST и Trusted Introducer правила;
- трошкове;
- утицај на МСП;
- кадровске и техничке капацитете;
- безбедносне и приватносне ризике.

4. Спроведе додатне процене

Пре почетка примене треба спровести:

- правну проверу;
- NIS2 табелу;
- процену ефеката;
- DPIA;
- процену информационе безбедности;
- анализу спољног алата;
- пилот-тестирање.

5. Спроведе нову јавну консултацију

Ако се прихвате битне измене, потребно је омогућити јавности да се изјасни о:

- пречишћеном тексту;

- обрасцима;
- RFC прилогу;
- SIM3 прилогу;
- техничком упутству;
- правилима приступа;
- роковима чувања;
- допуњеној процени ефеката.

Коначна оцена

Нацрт је прихватљив само уз битне измене.

Ако се не обезбеде наведене измене и предуслови, предлаже се одлагање усвајања и поновна израда спорних делова.

X. ПРИЛОЗИ

Уз овај поднесак достављају се или се могу доставити:

Прилог 1 — Матрица ризика

Табеларни приказ:

- одредбе;
- ризика;
- вероватноће;
- последице;
- мера ублажавања;
- приоритета.

Прилог 2 — Амандманска табела

За сваки амандман:

- одредба;
- постојећи текст;
- предложени текст;
- образложење;
- ризик;
- правни основ;
- очекивани ефекат;
- приоритет.

Прилог 3 — Списак извора

Обухвата:

- домаће прописе;
- званични Нацрт;
- RFC 2350;
- SIM3;
- NIS2;
- ENISA;
- FIRST;
- Trusted Introducer;
- релевантне стандарде заштите података и електронске идентификације.

Прилог 4 — Упоредноправни и међународни преглед

Обухвата:

- правну снагу сваког извора;
- значај за приступање ЕУ;
- однос Нацрта према стандарду;
- границе применљивости.

XI. ЗАВРШНА ПРОЦЕСНА ФОРМУЛА

Молим да се овај поднесак размотри у целини, укључујући све прилоге, и да се не третира само као општи коментар, већ као:

- образложена примедба на конкретне одредбе;
- предлог нормативних измена;
- захтев за допуну образложења;
- захтев за додатну процену ефеката;
- предлог за обезбеђивање процесних и безбедносних гаранција.

Поднесак је формулисан процесно неутрално и не прејудицира:

- незаконитост коначног акта;
- намеру предлагача;
- стручност службених лица;
- исход јавних консултација.

Његов циљ је да се пре усвајања отклоне ризици који могу утицати на:

- законитост;
- једнаку примену;
- информациону безбедност;
- заштиту података;
- права подносилаца;
- конкуренцију;
- положај малих тимова;
- делотворност Националног ЦЕРТ-а;
- поверење јавности у Евиденцију.

МЕСТО, ДАТУМ И ПОТПИС

Смедеревска Паланка, 24.07.2026. године

Милан Милошевић

Електронски потписано
Милан Милошевић
1516700581613001
25.07.2026 17:35:17

Прилог 1 — Матрица ризика

АНАЛИЗА РИЗИКА ПО ЈАВНИ ИНТЕРЕС

1. Методологија

Користи се следећа скала:

Вероватноћа

- **Н** — ниска;
- **С** — средња;
- **В** — висока.

Тежина

- **О** — ограничена;
- **З** — значајна;
- **К** — критична.

Приоритет

- **I** — отклонити пре усвајања;
- **II** — отклонити пре почетка примене;
- **III** — пратити и унапређивати у примени.

---

2. Правни ризици

Најважнији правни ризици произлазе из ограниченог законског овлашћења за садржај, упис и вођење Евиденције, док Нацрт уводи планове зрелости, континуирано ажурирање и статусно брисање. Додатни ризик ствара неодређено упућивање на SIM3 који се тренутно развија ка новој верзији. (Pravno Informacioni Sistem)

Ознака	Ризик и узрок	Изложени субјекти и последица	В / Т	Постојећа мера и недостатак	Предложена мера	Носилац / рок / индикатор
ПР-1	Прекорачење подзаконског овлашћења кроз обавезну зрелост, планове и брисање	Сви ЦЕРТ-ови; оспоравање акта и правна несигурност	С /К	Законски основ постоји за Евиденцију, али граница није образложена	Раздвојити регистарске доказе од материјалних услова; затражити мишљење министарства	Савет РАТЕЛ-а; пре усвајања; јавно правно образложење
ПР-2	Динамичко упућивање на SIM3	Субјекти могу добити нове обавезе без измене Правилника	В /К	Наведен је само назив и веб-страница	Фиксирати верзију и параметре у прилогу	Савет; пре усвајања; верзија у тексту

ПР-3	Неодређен поступак брисања	Губитак статуса без пуних гаранција	С/К	Опомена постоји, али нема решења и правног лека	Посебан члан о брисању	Савет; пре усвајања; прописана изрека, жалба и изјашњење
ПР-4	Неодређени критеријуми конзистентности	Неуједначено одлучивање	В/З	Провера је наведена без методологије	Објављени критеријуми и записник о оцени	Национални ЦЕРТ; пре примене; 100% предмета са контролном листом
ПР-5	Погрешно упућивање у члану 12	Неизводљивост прелазне норме	В/З	Нема корективне мере	Исправити на члан 3. тачка 1) подт. 9)–10)	Савет; пре усвајања; исправљен текст
ПР-6	Непознат правни лек	Ограничена управна и судска заштита	С/К	Опште упућивање на ЗУП	Изричита поука о жалби/управном спору	Савет; пре усвајања; сва решења са поуком

---

3. Безбедносни и сајбер ризици

Нацрт предвиђа јавну пуну адресу и RFC линк, нејавне SIM3 резултате и доставу осетљиве документације електронском поштом. Сам RFC 2350 наглашава поверљивост, интегритет и аутентичност комуникације и признаје да не морају све интерне процедуре бити јавне.

Ознака	**Ризик и узрок**	**Изложени субјекти и последица**	**В/Т**	**Постојећа мера и недостатак**	**Предложена мера**	**Носилац / рок / индикатор**
БР-1	Откривање оперативне локације	Тимови и инфраструктура; физичко извиђање и циљани напад	С/К	Пуна адреса је јавна	Јавно само место/адреса за доставу	Савет; пре усвајања; оперативне адресе нису јавне
БР-2	Прекомерна RFC објава	Чланови тима и процедуре; phishing и социјални инжењеринг	В/З	Нема јавног минимума	Јавни профил + поверљиви анекс	РАТЕЛ; пре примене; шаблон са класификацијом

БР-3	Слање SIM3 имејлом	Компромитација слабости, кадровских и организационих података	В/К	Електронски документ је прописан, али не и шифровање	Заштићени портал, енкрипција и временски жиг	РАТЕЛ; пре примене; 100% електронских пријава преко заштићеног канала
БР-4	Неовлашћен приступ SIM3 линку	Откривање слабости	С/К	Линк је обавезан, права приступа нису уређена	Архивска датотека као доказ; линк само помоћан и ограничен	Национални ЦЕРТ; пре примене; нема јавних SIM3 URL-ова
БР-5	Компромитација Евиденције	Сви субјекти; лажни или измењени регистарски подаци	С/К	Електронска Евиденција је предвиђена без техничких мера	MFA, RBAC, audit trail, интегритет, резервне копије	РАТЕЛ; пре примене; периодични тестови и нула неевидентираних измена
БР-6	Зависност од страног алата	Недоступност, измена или губитак доказа	В/З	Нема офлајн алтернативе	Домаћи формат, локална копија и план изласка	РАТЕЛ; пре примене; свака процена доступна независно од спољног сервиса
БР-7	Ризик ланца снабдевања	РАТЕЛ и ЦЕРТ-ови; зависност од хостинга и добављача	С/З	Добављачи нису идентификовани	Попис обрађивача и техничких зависности	РАТЕЛ; 60 дана; регистар добављача и процена ризика

4. Ризици за заштиту података о личности

Нацрт прикупља име, функцију, адресу и службене контакте одговорног лица, али не одређује рок чувања, руковаоца, обрађиваче, права лица и поступак повреде. Постоји и противречност између ограничене сврхе из члана 11. и шире стварне употребе података у поступцима уписа и брисања.

Ознака	**Ризик**	**Субјекти и последица**	**В/Т**	**Недостатак**	**Мера**	**Носилац / рок / индикатор**

ЗП-1	Прикупљање приватне адресе одговорног лица	Физичка лица; прекомерна обрада и безбедносно излагање	В/З	„Адреса“ није дефинисана	Избрисати; дозволити само службену адресу	Савет; пре усвајања; нула приватних адреса
ЗП-2	Нејасна сврха	Сви чији се подаци обрађују; секундарна употреба	В/З	Члан 11 не обухвата упис, проверу и брисање	Таксативно утврдити сврхе	Савет; пре усвајања; политика обраде објављена
ЗП-3	Нема рокова чувања	Одговорна лица и запослени; неограничено чување	В/З	Нема правила	Матрица рокова по категоријама	РАТЕЛ; пре примене; аутоматизовано преиспитивање рокова
ЗП-4	Спољни алат и могући пренос	Подносилац и чланови тима	С/К	Нису утврђени токови података и метаподаци	DPIA, техничка анализа и офлајн опција	РАТЕЛ/Повереник; пре примене; објављена процена
ЗП-5	Нема обавештења лицима	Одговорна лица не знају права и сврху	В/З	Обрасци немају privacy notice	Обавештење уз оба обрасца	РАТЕЛ; пре примене; обавештење доступно
ЗП-6	Нема поступка повреде	Сви субјекти; закаснела реакција	С/К	Нема протокола	План повреде и обавештавања	РАТЕЛ; пре примене; годишња вежба
ЗП-7	Нејасан руковалац/обрађивач	Правна несигурност	В/З	Улоге нису наведене	Идентификовати РАТЕЛ, организационе јединице и добављаче	РАТЕЛ; 30 дана; регистар радњи обраде

5. Институционални и управљачки ризици

Национални ЦЕРТ истовремено прима пријаву, проверава доказе, оцењује конзистентност, доноси решење, води Евиденцију, захтева ажурирање, шаље опомену и може покренути брисање. Нацрт не прописује независну проверу или објављене критеријуме.

Ознака	**Ризик**	**Последица**	**В/Т**	**Недостатак**	**Мера**	**Носилац / рок / индикатор**

ИР-1	Концентрација функција	Пристрасност или привид пристрасности	С/К	Нема раздвајања	Раздвојити пријем, стручну оцену и одлучивање	РАТЕЛ; пре примене; најмање два нивоа контроле
ИР-2	Необучена лица за SIM3	Неуједначене оцене	С/З	Нема услова стручности	Обука, овлашћење и периодична провера	РАТЕЛ; пре примене; 100% оцењивача обучено
ИР-3	Недостатак критеријума	Селективна примена	В/К	Нема методологије	Јавна контролна листа и анонимизована пракса	Национални ЦЕРТ; пре првог решења; објављени критеријуми
ИР-4	Нема рокова одлучивања	Административна неизвесност	С/З	Само опште упућивање на ЗУП	Посебан рок и праћење	Савет; пре усвајања; просечно време поступка
ИР-5	Недовољни ресурси	Кашњење и формална контрола	С/З	Тврди се да нема посебних средстава без анализе рада	Кадровска и техничка процена	РАТЕЛ; пре примене; план капацитета
ИР-6	Нема спољне контроле оцене	Технички спор без ефективне ревизије	С/К	Само органска контрола	Друга стручна оцена или независни експерт	Савет; пре примене; поступак ревизије

6. Економски и тржишни ризици

Образложење наводи само да за спровођење нису потребна посебна средства у финансијском плану Регулатора. Та тврдња не обухвата трошкове Националног ЦЕРТ-а у радним сатима, нити трошкове постојећих и будућих посебних ЦЕРТ-ова.

Раздвајање трошкова

Носилац	**Врсте трошкова**
РАТЕЛ	портал, безбедност, архивирање, обука, правна подршка, одржавање

Национални ЦЕРТ	прегледи, комуникација, решења, опомене, ажурирање, контрола
Постојећи ЦЕРТ-ови	RFC, SIM3, планови, документација, усклађивање
Нови подносиоци	успостављање процеса, систематизација, алати, превод, консултанти
Друштво	мањи број тимова, концентрација тржишта, одложено успостављање регионалних капацитета
Опортунитетни трошак	време стручњака преусмерено са оперативног одговора на документацију

Ознака	**Ризик**	**Последица**	**В/Т**	**Мера**	**Носилац / рок / индикатор**
ЕР-1	Неевидентирани директни трошкови	Нереална процена ефеката	В/З	Анализа административног трошка по типу тима	РАТЕЛ; пре усвајања; објављена процена
ЕР-2	Баријера за мале и нове тимове	Смањена конкуренција и број ЦЕРТ-ова	В/З	Фазни и пропорционални режим	Савет; пре усвајања; број пријава МСП
ЕР-3	Лиценцни ризик SIM3	Комерцијални субјекти не знају услове употребе	С/З	Правно мишљење и домаћи офлајн формат	РАТЕЛ; пре примене; јасни услови без појединачне неизвесности
ЕР-4	Фаворизовање великих организација	Концентрација тржишта	С/К	Процена утицаја на конкуренцију	Савет/надлежни орган; пре усвајања; структура уписаних по величини
ЕР-5	Трошак континуираног ажурирања	Непредвидиви годишњи расходи	В/З	Утврдити редован циклус и максималну учесталост	Савет; пре усвајања; просечан број захтева по тиму
ЕР-6	Регулаторни захват без cost-benefit анализе	Мере скупље од користи	С/К	Сценарији и алтернативе	Савет; пре усвајања; објављено поређење варијанти

7. Политички ризици и јавна одговорност

Ознака	Ризик	Узрок и последица	В/Т	Мера	Носилац / рок / индикатор
ПО-1	Селективно захтевање ажурирања	Нема критеријума; могућ различит третман	С/К	Образложени ризично засновани критеријуми	Национални ЦЕРТ; пре примене; јавна статистика захтева
ПО-2	Селективно брисање	„Може покренути“ без мерила	С/К	Матрица сразмерности и обавезно образложење	Савет; пре усвајања; сва решења са тестом сразмерности
ПО-3	Непримерен утицај на оцену	Концентрација техничке и управне моћи	Н/К	Изузеће, двострука контрола, лог одлучивања	РАТЕЛ; пре примене; регистар сукоба интереса
ПО-4	Недовољна јавна контрола	Нема извештаја о примени и критеријума	В/З	Годишњи агрегирани извештај	РАТЕЛ; годишње; објављен извештај
ПО-5	Формалне консултације	Примедбе без образложеног одговора	С/З	Табела прихваћених и неприхваћених предлога	Савет; пре усвајања; извештај о консултацијама
ПО-6	Регулаторно заробљавање	Доминација великих комерцијалних тимова у стручним консултацијама	Н/З	Транспарентност састанака и интереса	РАТЕЛ; трајно; регистар консултованих субјеката

Социјални и радноправни ризици

Ознака	Ризик	Последица	В/Т	Постојећа мера/недостатак	Мера	Носилац / рок / индикатор
СР-1	Недостатак стручног кадра	Немогућност достизања планиране зрелости	В/З	SIM3 мери кадрове, али нема подршке	Програм обуке и заједнички ресурси	РАТЕЛ/струковна тела; 12 месеци; број обучених

СР-2	Прекомерно оптерећење	Burnout и пад оперативне способности	С/З	Нема анализе радног времена и дежурстава	Процена оптерећења и минимална резилијентност	Матична лица; 6 месеци; прековремени рад и одсуства
СР-3	Искључивање малих/академских тимова	Мања разноврсност система	В/З	Јединствен модел доказа	Пропорционални докази и фазни рокови	Савет; пре усвајања; број академских и непрофитних уписа
СР-4	Територијална неравномерност	Недоступност стручне подршке ван великих центара	С/З	Нема регионалног индикатора	Подршка регионалним и виртуелним тимовима	Надлежно министарство; 24 месеца; регионална покривеност
СР-5	Неприступачан алат/упутства	Искључење лица са инвалидитетом	С/З	Доступност није доказана	WCAG провера и приступачан офлајн образац	РАТЕЛ; пре примене; извештај о приступачности
СР-6	Неосновано индивидуално профилисање	SIM3 слабост приписује се појединим запосленима	С/З	Самопроцена је организациона, али нема забране индивидуалне злоупотребе	Правило да оцена није индивидуална радна оцена	Савет/послодавци; пре примене; политика употребе резултата

Родни и други специфични ризици нису непосредно документовани Нацртом. Могу се пратити кроз агрегиране податке о доступности стручног усавршавања, али не треба конструисати нормативни проблем без података.

---

9. Просторни ризици

Просторна компонента је посредна, али стварна у погледу јавне адресе, физичке безбедности, регионалне покривености и отпорности инфраструктуре.

Ознака	**Ризик**	**Последица**	**В/Т**	**Мера**	**Носилац / рок / индикатор**
ПСР-1	Јавна прецизна локација	Физички и комбиновани напад	С/К	Јавно само место/адреса за пошту	Савет; пре усвајања; нула јавних оперативних локација

ПСР-2	Концентрација у Београду и великим центрима	Регионална зависност	С/З	Агрегирано праћење и подршка удаљеним тимовима	РАТЕЛ/министарство; годишње; број региона са активним тимом
ПСР-3	Недостатак резервне локације	Прекид рада после пожара, поплаве или другог догађаја	С/К	Нејавни план континуитета и удаљени рад	Матична лица; 12 месеци; тест опоравка
ПСР-4	Зависност од једне телекомуникационе /енергетске тачке	Недоступност у кризи	С/К	Редундантни приступ и резервно напајање	ЦЕРТ-ови; 12 месеци; резултат годишњег теста
ПСР-5	Јавна повезаност адресе и капацитета	Нападач комбинује јавне податке	С/К	Минимизација и процена ризика пре објаве	Национални ЦЕРТ; пре објаве; документован преглед

10. Еколошки и климатски ризици

Еколошки ефекти Правилника су углавном **индиректни**. Нацрт не уређује изградњу дата-центара или набавку опреме, па не треба приписивати непосредне значајне еколошке последице самом упису у Евиденцију.

Ознака	**Ризик**	**Карактер**	**В/Т**	**Мера**	**Индикатор**
ЕК-1	Додатна потрошња енергије за алате, архиве и резервне копије	Индиректан	С/О	Енергетски ефикасна инфраструктура и рационални рокови чувања	Потрошња по услузи/систему
ЕК-2	Резервно напајање и батерије	Индиректан	С/З	План одржавања и законито збрињавање	Евиденција замене и отпада
ЕК-3	Електронски отпад	Индиректан	Н/З	Продужени животни циклус и овлашћено збрињавање	Количина предате опреме
ЕК-4	Екстремни временски догађај	Индиректан, али безбедносно значајан	С/К	Географска редундантност и DR план	Резултат теста опоравка

ЕК-5	Прекомерно чување података	Индиректан	С/О	Ограничење чувања и дедупликација	Обим архиве и стопа брисања

Непосредни утицај на животну средину може се оценити као **ограничен**, док је климатска отпорност значајна за континуитет рада.

---

11. Културолошки, језички и приступачносни ризици

RFC 2350 и SIM3 су доступни првенствено на енглеском језику. Нацрт не одређује службени превод, домаћу терминологију или поступак решавања разлика у тумачењу. (rfc-editor.org)

Ознака	**Ризик**	**Последица**	**В/Т**	**Мера**	**Носилац / рок / индикатор**
КР-1	Нема званичног превода	Различито тумачење обавеза	В/З	Одобрени српски превод и речник	РАТЕЛ; пре примене; објављен превод
КР-2	Неодређени енглески појмови	Неуједначена пракса	В/З	Дефинисати mandate, constituency, audit, assessment, maturity	Савет; пре усвајања; нормативни речник
КР-3	Мешање CERT/CSIRT и домаће терминологије	Правна и стручна конфузија	С/З	Уједначити термине и навести еквиваленте	РАТЕЛ; пре примене; терминолошко упутство
КР-4	Недоступност ћириличке и двојезичне документације	Смањена употребљивост	С/З	Обрасци и упутства на ћирилици; енглеска верзија јавног RFC-а као допуна	РАТЕЛ; пре примене; обе верзије доступне
КР-5	Различита техничка култура организација	Неједнак квалитет самопроцене	В/З	Обуке, примери и контролна питања	Национални ЦЕРТ; пре првог циклуса; број обука и исправних пријава
КР-6	Неприступачни електронски документи	Искључење појединих корисника	С/З	Приступачни HTML/PDF и офлајн образац	РАТЕЛ; пре примене; тест приступачности

---

12. Консолидована оцена највиших ризика

Критични ризици — приоритет I

1. неодређена и променљива SIM3 верзија;
2. непотпун правни основ за развојне и статусне обавезе;
3. непотпун поступак брисања;
4. нема јасног правног средства;
5. слање осетљиве документације обичном електронском поштом;
6. пуна јавна адреса и могућа прекомерна RFC објава;
7. неуређене сврхе, рокови и приступ SIM3 и личним подацима;
8. концентрација функција без контролних механизама;
9. погрешно упућивање у члану 12;
10. неусклађеност Обрасца 2 са садржајем Евиденције.

Значајни ризици — приоритет II

1. несразмерни трошкови за мале тимове;
2. непостојање офлајн алтернативе;
3. нејасни критеријуми ажурирања;
4. рок од 15 дана;
5. недостатак превода;
6. недостатак техничког упутства;
7. неизвршена DPIA и безбедносна процена;
8. недостатак архивског и лог режима;
9. неуређен статус започетих поступака;
10. недостатак одложене примене.

---

13. Завршни тест јавног интереса

Нацрт се може сматрати прихватљивим са становишта јавног интереса тек ако су испуњени следећи минимални услови:

1. **законски тест** — свака обавеза има јасно упориште у Закону;
2. **верзиони тест** — RFC и SIM3 су прецизно идентификовани;
3. **процесни тест** — постоје допуна, изјашњење, образложење и правни лек;
4. **безбедносни тест** — осетљиви подаци не шаљу се незаштићеним каналом;
5. **тест приватности** — прикупљају се само нужни службени подаци;
6. **тест сразмерности** — брисање је крајња, а не прва мера;
7. **тест једнакости** — постоје објављени критеријуми и контрола дискреције;
8. **тест трошкова** — обухваћени су и трошкови регулисаних субјеката;
9. **тест континуитета** — постоје архиве, резервне копије и план опоравка;
10. **језички тест** — домаћи субјекти имају приступ разумљивом и меродавном тексту стандарда.

Синтетичка оцена

Предложена решења имају легитиман циљ: побољшање проверљивости, зрелости и сарадње посебних ЦЕРТ-ова. Међутим, садашњи текст није довољно прецизан у погледу

правног основа, SIM3 верзије, управне заштите, безбедности доставе, обраде података и брисања.

Прелиминарна оцена:

Нацрт је прихватљив само уз битне измене пре усвајања.

Није довољна само редакцијска корекција. Потребне су системске измене чл. 2, 3, 6, 7, 8, 10, 11. и 12, као и оба обрасца.

Прилог 2 — Амандманска табела

ПРЕДЛОЗИ ИЗМЕНА И АМАНДМАНСКЕ ФОРМУЛАЦИЈЕ

1. Уводна нормативна напомена

Амандмански текст је припремљен према Нацрту који је РАТЕЛ објавио 25. јуна 2026. године у поступку јавних консултација. Дословни делови постојећих одредаба проверени су према званичном PDF документу и обрасцима. (Ratel)

Предложена нумерација нових ставова, чланова и прилога мора се технички ускладити после прихватања амандмана. Где се предлаже замена целог члана, текст је формулисан као непосредно уносив текст.

Основни правни ослонци су:

- члан 35. став 5. Закона о информационој безбедности, који овлашћује надлежни орган да пропише садржај, начин уписа и вођења Евиденције; (Pravno-informacioni sistem)
- Закон о општем управном поступку, за уредност поднеска, изјашњење странке, образложење, достављање и правну заштиту; (Pravno Informacioni Sistem)
- Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању; (Pravno Informacioni Sistem)
- Закон о заштити података о личности и стандарди процене утицаја обраде на заштиту података; (Data Protection Advocate)
- NIS2, посебно стандарди безбедних комуникационих канала, поверљивости, отпорности и сарадње CSIRT тимова; (EUR-Lex)
- RFC 2350/BCP 21, као необавезујућа најбоља пракса, а не пропис или сертификат; (RFC Editor)
- SIM3 и ENISA оквир зрелости, при чему ENISA пуну оцену не своди само на самопроцену, већ препознаје и peer review; (Open CSIRT Foundation)
- FIRST CSIRT Services Framework, који не захтева да сваки тим пружа све услуге и не прописује сам по себи квалитет или зрелост; (FIRST)
- Trusted Introducer поступак сертификације, који укључује проверу од стране квалификованих SIM3 аудитора и није истоветан самопроцени. (Trusted Introducer)

АМАНДМАН/ПРЕДЛОГ БРОЈ 1

Правна природа уписа у Евиденцију

Одредба на коју се односи:
Члан 1, после постојећег става 1.

Постојећи текст:

> „Овим правилником ближе се прописују садржај, начин уписа и вођења евиденције...“ (Ratel)

Предложени текст:

После става 1. додају се ст. 2. и 3, који гласе:

> „Евиденција има регистарску, статусну, информативну и координациону функцију.
>
> Упис у Евиденцију не представља акредитацију, сертификацију, независну стручну процену нити гаранцију квалитета, капацитета или компетентности Посебног ЦЕРТ-а, осим потврде да је упис извршен у складу са законом и овим правилником.“

Образложење:

Нацрт захтева RFC 2350 и SIM3 самопроцену, али не предвиђа независни аудит који би оправдао представљање уписа као сертификације. RFC 2350 је најбоља пракса, а SIM3 самопроцена није истоветна професионалној сертификацији. FIRST Services Framework такође не прописује капацитет, зрелост или квалитет појединачног тима. (RFC Editor)

Ризик који се отклања:

- прикривена акредитација;
- обмањујуће тржишно представљање;
- неосновано коришћење уписа као доказа стручне способности;
- фаворизовање уписаних субјеката у јавним набавкама.

Правни и међународни основ:

Закон о информационој безбедности; принцип правне сигурности; RFC 2350; FIRST CSIRT Services Framework.

Очекивани ефекат:

- 100% јавних приказа уписа садржи напомену о правној природи;
- смањење спорова о томе шта упис доказује;
- спречавање употребе уписа као неформалне лиценце.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 2

Прецизно одређивање RFC 2350

Одредба на коју се односи:
Члан 2, тачка 1).

Постојећи текст:

> „RFC 2350... је текстуални документ којим подносилац пријаве описује своје капацитете и каталог услуга...“ (Ratel)

Предложени текст:

Тачка 1) мења се и гласи:

> „1) RFC 2350 је документ ‘Expectations for Computer Security Incident Response’, RFC 2350, BCP 21, објављен у јуну 1998. године, којим су дате препоруке за представљање мандата, корисничке заједнице, услуга, политика, контактних података и начина безбедне комуникације CSIRT/ЦЕРТ тима.
>
> За примену овог правилника користи се домаћи RFC 2350 профил утврђен Прилогом 3, који чини његов саставни део.“

Образложење:

Постојећи текст нетачно развија скраћеницу RFC као „Request for Comments“ у контексту назива конкретног документа и не наводи:

- назив;
- BCP ознаку;
- годину;
- ауторе;
- нормативно релевантан обим;
- домаћи минимални садржај.

RFC 2350 сам наводи да није могуће утврдити један сет захтева који одговара свим тимовима. Зато није довољно само упутити на цео Анекс D без домаћег профила. (RFC Editor)

Ризик који се отклања:

- различито тумачење обавезних поља;

- прекомерно објављивање;
- претварање препоруке у неодређен услов;
- спор о верзији и садржају документа.

Правни и међународни основ:

Члан 35. став 5. Закона; RFC 2350/BCP 21; принцип одређености подзаконског акта.

Очекивани ефекат:

- један домаћи образац за 100% подносилаца;
- упоредиви профили;
- смањење допуна због различитог тумачења;
- јасно раздвајање обавезних и необавезних поља.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 3

Одређивање верзије SIM3

Одредба на коју се односи:
Члан 2, тачка 2).

Постојећи текст:

> „SIM3... је модел зрелости... Модел развија и одржава Open CSIRT Foundation.“ (Ratel)

Предложени текст:

Тачка 2) мења се и гласи:

> „2) SIM3 самопроцена је интерна процена зрелости Посебног ЦЕРТ-а извршена применом модела Security Incident Management Maturity Model — SIM3, верзија 2 interim, од 1. јануара 2023. године, у обиму, структури и према дефиницијама параметара утврђеним Прилогом 4, који чини саставни део овог правилника.“

Образложење:

Нацрт не идентификује верзију модела. Званична страница Open CSIRT Foundation и даље означава SIM3 v2 interim као референтну верзију, уз најаву пуне верзије 2 током 2026. године. Неодређено упућивање може довести до промене обавеза без измене Правилника. (Open CSIRT Foundation)

Уколико до усвајања буде коначно објављена друга верзија, она се може преузети само после:

1. објављивања тачног текста;
2. анализе разлика;
3. процене ефеката;
4. омогућавања јавности да се о њој изјасни.

Ризик који се отклања:

- динамичко и непрозирно мењање обавеза;
- неупоредивост процена;
- спор о параметрима;
- ретроактивно преиспитивање ранијих пријава.

Правни и међународни основ:

Принцип правне сигурности; члан 35. Закона; SIM3 документација; ENISA оквир зрелости.

Очекивани ефекат:

- 100% самопроцена користи исту верзију;
- нула измена правних обавеза без измене Правилника;
- могућност архивског поређења резултата.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 4

Забрана аутоматске примене будућих измена спољних стандарда

Одредба на коју се односи:
Члан 2, нови ст. 2–4.

Постојећи текст:

Не постоји одредба која уређује последице накнадне измене RFC 2350, SIM3 или спољног алата.

Предложени текст:

После тачке 2) додају се ст. 2–4:

> „RFC 2350 и SIM3 представљају техничке и стручне референтне оквире и немају самостално дејство прописа Републике Србије.
>
> Накнадна измена, допуна, замена, повлачење или промена услова коришћења RFC 2350 документа, SIM3 модела или спољног онлајн алата не мења права и обавезе утврђене овим правилником.
>
> Нова верзија спољног документа може се примењивати тек после измене одговарајућег прилога овог правилника, спроведене процене ефеката и јавних консултација.“

Образложење:

Обавезе домаћих субјеката не смеју зависити од једностраних одлука стране приватне организације. RFC 2350 је BCP, док SIM3 одржава Open CSIRT Foundation; ниједан од тих субјеката нема домаће регулаторно овлашћење. (RFC Editor)

Ризик који се отклања:

- преношење нормативне функције;
- непредвидиви нови трошкови;
- нарушавање законитости;
- промена услова уписа без јавне процедуре.

Правни и међународни основ:

Уставни принцип законитости; члан 35. Закона; правна природа RFC и SIM3.

Очекивани ефекат:

- свака промена обавеза пролази јавну процедуру;
- мерљив број аутоматских промена обавеза: **0**;
- стабилност регистарског режима.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 5

Званично домаће упутство, превод и приступачност

Одредба на коју се односи:
Члан 2, нови ст. 5–7.

Постојећи текст:

Нацрт упућује на веб-странице на енглеском језику, без домаћег меродавног упутства. (Ratel)

Предложени текст:

„Регулатор пре почетка примене објављује на српском језику и ћириличком писму:

1. домаће упутство за примену RFC 2350;
2. домаће упутство за примену SIM3;
3. терминолошки речник;
4. примере правилно попуњених докумената;
5. објашњење критеријума провере.

Када услови лиценце то допуштају, Регулатор обезбеђује и објављује превод релевантних делова референтних докумената. У случају несагласности, за домаћи управни поступак меродаван је садржај утврђен прилозима овог правилника.

Документи, упутства и електронски обрасци морају бити доступни особама са инвалидитетом и у формату погодном за употребу помоћних технологија.“

Образложење:

Нормативна обавеза не треба да зависи од способности подносиоца да сам преведе стране стручне термине. ENISA модел користи специфичну терминологију и више нивоа процене, што захтева уједначено домаће тумачење. (ENISA)

Ризик који се отклања:

- различита тумачења;
- језичка дискриминација;
- неприступачност;
- повећани трошкови превода;
- неуједначено одлучивање.

Правни и међународни основ:

Принцип приступачности јавних услуга; равноправност странака; ENISA и SIM3 као стручни, а не домаћи нормативни текстови.

Очекивани ефекат:

- објављена најмање четири домаћа документа пре примене;
- мањи број допуна због погрешног тумачења;
- приступачни обрасци у HTML и означеном PDF формату.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 6

Локална и офлајн алтернатива SIM3 алату

Одредба на коју се односи:
Члан 2, нови став 8; члан 6, став 1, тачка 3).

Постојећи текст:

„Модел и онлајн алат за самопроцену доступни су на адреси...“ (Ratel)

и:

„...са електронском везом ка резултатима самопроцене на онлајн алату...“ (Ratel)

Предложени текст:

У члану 2. додаје се став:

„Коришћење спољног онлајн алата није обавезан услов за упис или останак у Евиденцији.“

У члану 6. став 1. тачка 3) мења се и гласи:

„3) SIM3 самопроцену достављену у прописаном табеларном, машински читљивом и архивски одрживом електронском формату. Електронска веза ка

спољном алату може се доставити добровољно и има искључиво помоћни карактер.“

Образложење:

Службени предмет мора садржати стабилан доказ који остаје доступан независно од рада трећег лица. Онлајн сервис може променити URL, формат, услове, власника или престати да ради.

Ризик који се отклања:

- vendor lock-in;
- губитак доказа;
- прекогранична обрада;
- прекид поступка услед недоступности алата;
- обавезно прихватање приватних услова коришћења.

Правни и међународни основ:

Закон о електронском документу; принцип технолошке неутралности; стандарди интегритета и доступности; NIS2 захтеви отпорности. (Pravno-informacioni sistem)

Очекивани ефекат:

- 100% предмета садржи локалну архивску копију;
- поступак је могућ и када је спољни сервис недоступан;
- нула обавезних прекограничних преноса само ради уписа.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 7

Минимизација података у Евиденцији

Одредба на коју се односи:
Члан 3, уводна реченица и тачка 1).

Постојећи текст:

„У Евиденцију се уписују следећи подаци...“ (Ratel)

Предложени текст:

После уводне реченице додаје се став:

„У Евиденцију се уписују само подаци који су примерени, битни и ограничени на оно што је неопходно за идентификацију, вођење управног поступка, ажурирање Евиденције и координацију у случају ризика и инцидената.

Пре увођења нове категорије података Национални ЦЕРТ документује њену сврху, правни основ, јавност, круг корисника и рок чувања.“

Образложење:

Постојећи списак не садржи образложење нужности сваког податка. Минимизација је посебно важна јер се део података јавно објављује, а други део може открити кадровске и оперативне слабости.

Ризик који се отклања:

- прекомерна обрада;
- повећана последица повреде података;
- прикупљање података без јасне сврхе;
- неограничено ширење регистра.

Правни и међународни основ:

Закон о заштити података о личности; Конвенција 108; члан 8. ЕКЉП; приступни стандарди GDPR-а. Србија је страна Конвенције 108 од 2006. године. (Portal)

Очекивани ефекат:

- за свако поље постоји документована сврха;
- мањи број личних и осетљивих података;
- смањена површина напада на Евиденцију.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 8

Брисање приватне адресе одговорног лица

Одредба на коју се односи:
Члан 3, тачка 2).

Постојећи текст:

> „...контакт подаци... (адреса, службени контакт телефон и службена адреса електронске поште)“ (Ratel)

Предложени текст:

Тачка 2) мења се и гласи:

> „2) подаци о одговорном лицу у Посебном ЦЕРТ-у: име и презиме, функција или радно место, службени контакт телефон, службена адреса електронске поште и датум почетка и престанка овлашћења.
>
> Адреса пребивалишта или боравишта, приватни број телефона и приватна адреса електронске поште одговорног лица не прикупљају се.“

Образложење:

Израз „адреса“ може обухватити адресу пребивалишта, иако Образац 1 такво поље не садржи. Приватна адреса није неопходна ако постоје службена адреса ЦЕРТ-а, службени телефон и службени имејл.

Ризик који се отклања:

- прекомерна обрада;
- физичко угрожавање лица;
- крађа идентитета;
- неусклађеност текста и обрасца.

Правни и међународни основ:

Начела минимизације и ограничења сврхе; Конвенција 108; члан 8. ЕКЉП; Закон о заштити података.

Очекивани ефекат:

- број прикупљених приватних адреса: **0**;
- усклађеност члана 3. и Обрасца 1;
- смањење ризика по физичка лица.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 9

Ограничење јавне објаве физичке адресе

Одредба на коју се односи:
Члан 3, тачка 1), подтачка 3); члан 11, став 2.

Постојећи текст:

> „адреса Посебног ЦЕРТ-а (општина, улица и број, поштански број и место, ПАК)“ (Ratel)

Предложени текст:

Подтачка 3) мења се и гласи:

„3) службена адреса правног лица или адреса за пријем поште, као и место у коме Посебан ЦЕРТ претежно обавља послове.“

У члану 11. додаје се:

„Прецизна оперативна локација, резервна локација, локација техничке инфраструктуре и адреса рада дистрибуираног тима не објављују се у јавном делу Евиденције.“

Образложење:

Пуна адреса није увек неопходна за јавни контакт и може открити оперативну или резервну локацију тима. Нови Закон захтева да информациони системи Националног ЦЕРТ-а буду на сигурним локацијама и да се обезбеде поверљивост и резервни капацитети, што потврђује значај просторне безбедности. (Paragraf)

Ризик који се отклања:

- физичко извиђање;
- комбиновани физички и сајбер напад;
- откривање резервне инфраструктуре;
- социјални инжењеринг.

Правни и међународни основ:

Закон о информационој безбедности; NIS2 захтеви безбедне инфраструктуре и континуитета; принцип минимизације.

Очекивани ефекат:

- јавни регистар не садржи оперативне и резервне локације;
- 100% адреса пре објављивања пролази безбедносну проверу;
- очувана могућност службене доставе.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 10

Телефон, факс и категорија величине тима

Одредба на коју се односи:
Члан 3, тачка 1), подт. 6) и 9).

Постојећи текст:

„број телефона и факса субјекта који подноси пријаву“ (Ratel)

и:

„мали... средњи... велики...“ (Ratel)

Предложени текст:

Подтачка 6) мења се и гласи:

„6) службени контакт телефон; број факса уписује се само ако га подносилац користи.“

Подтачка 9) мења се и гласи:

„9) категорија величине Посебног ЦЕРТ-а, утврђена према броју еквивалената пуног радног времена ангажованих на његовим пословима:

(1) мали — до три;

(2) средњи — више од три, а до десет;

(3) велики — више од десет.

Начин израчунавања еквивалената пуног радног времена утврђује се Прилогом 5.“

Образложење:

Факс не треба наметати субјекту који га не користи. Број физичких лица није довољан показатељ ако лица раде непуно време, деле улоге или су спољно ангажована.

Ризик који се отклања:

- нетачна категоризација;
- дискриминација флексибилних тимова;
- непотребно прикупљање података;
- формално, а не функционално мерење капацитета.

Правни и међународни основ:

Пропорционалност; FIRST Framework, који избор услуга везује за мандат и корисничку заједницу, а не за униформан модел тима. (FIRST)

Очекивани ефекат:

- упоредивији показатељ величине;
- мање спорова о томе ко се сматра чланом;
- факс постаје необавезан.

Приоритет: II

АМАНДМАН/ПРЕДЛОГ БРОЈ 11

Верзионирање RFC и SIM3 докумената

Одредба на коју се односи:
Члан 3, тачка 1), подт. 10) и 11).

Постојећи текст:

„електронска веза ка јавно доступном RFC 2350 документу“ (Ratel)

и:

„самопроцена нивоа зрелости... према SIM3“ (Ratel)

Предложени текст:

Подтачке 10) и 11) мењају се и гласе:

„10) електронска веза ка јавном RFC 2350 профилу, број верзије, датум усвајања, датум последње измене и контролни збир архивске копије;

11. назив и верзија SIM3 модела, датум самопроцене, датум достављања и идентификатор архивске копије, без уписивања појединачних резултата у јавни део Евиденције.“

Образложење:

Сам URL не доказује који је садржај важио у тренутку уписа. Садржај веб-странице може бити накнадно промењен.

Ризик који се отклања:

- губитак доказног трага;
- неприметна промена документа;
- спор о верзији;
- немогућност реконструкције управног предмета.

Правни и међународни основ:

Закон о електронском документу; принцип интегритета и непорецивости; RFC 2350 препознаје значај аутентичности профила. (Pravno-informacioni sistem)

Очекивани ефекат:

- 100% RFC и SIM3 докумената има верзију и датум;
- свака измена је реконструисива;
- смањење спорова о садржају достављеног документа.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 12

Услови за упис и пропорционалност различитим типовима тимова

Одредба на коју се односи:
Члан 4, тач. 2) и 3), и нови став 2.

Постојећи текст:

> „...у оквиру одређеног правног лица, групе правних лица, области пословања и слично.“ (Ratel)

Предложени текст:

Тачка 3) мења се и гласи:

> „3) да у тренутку подношења пријаве стварно обавља послове превенције и заштите од безбедносних ризика за унапред одређену корисничку заједницу, једно или више правних лица, јавни или привредни сектор, академску или истраживачку заједницу, професионално удружење, непрофитну организацију или другу одредиву групу корисника.“

После става 1. додаје се став 2:

> „Када је Посебан ЦЕРТ организациона јединица, подносилац пријаве и носилац права и обавеза из решења јесте правно лице у чијем је саставу.
>
> Испуњеност услова процењује се сразмерно мандату, корисничкој заједници, врсти услуга, величини и организационој форми тима.“

Образложење:

Израз „и слично“ је неодређен. Јединствен модел не сме искључити академске, секторске, непрофитне, комерцијалне, виртуелне или новоосноване тимове.

Ризик који се отклања:

- неједнак третман;
- административна и тржишна баријера;
- нејасан носилац решења;
- произвољно тумачење корисничке заједнице.

Правни и међународни основ:

Принцип једнакости и сразмерности; FIRST Framework; RFC 2350, који не прописује један модел за све тимове. (RFC Editor)

Очекивани ефекат:

- повећан број прихватљивих организационих модела;
- смањен број одбијања због форме организације;
- веће учешће академских, непрофитних и малих тимова.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 13

Овлашћени подносилац, обавештење о обради и техничка упутства

Одредба на коју се односи:
Члан 5, после постојећег става 1.

Постојећи текст:

„Пријава за упис у Евиденцију подноси се на Обрасцу 1...“ (Ratel)

Предложени текст:

Додају се ст. 2–5:

„Пријаву подноси законски заступник правног лица или друго лице овлашћено у писаном или електронском облику.

Ако је Посебан ЦЕРТ организациона јединица, пријаву подноси правно лице у чијем је саставу.

Уз пријаву се доставља доказ о овлашћењу, осим ако се овлашћење може проверити у службеној евиденцији.

Национални ЦЕРТ на веб-презентацији објављује електронски попуњив образац, упутство за попуњавање, обавештење о обради података, дозвољене формате, правила означавања поверљивих прилога и упутство за безбедну електронску доставу.“

Образложење:

Постојећи члан не одређује странку, потписника и доказ овлашћења. Образац не садржи обавештење о обради података.

Ризик који се отклања:

- пријаве неовлашћених лица;
- спор о статусу странке;
- нетранспарентна обрада личних података;
- технички неуредни поднесци.

Правни и међународни основ:

ЗУП; Закон о заштити података; Закон о електронском документу.

Очекивани ефекат:

- 100% пријава има проверљивог потписника;
- смањен број захтева за допуну;
- свако одговорно лице добија обавештење о обради.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 14

Алтернативни докази стварног оперативног капацитета

Одредба на коју се односи:
Члан 6, став 1, тачка 1), и став 2.

Постојећи текст:

„извод из акта о унутрашњој организацији и систематизацији послова...“ (Ratel)

Предложени текст:

Тачка 1) мења се и гласи:

„1) акт о оснивању или организовању Посебног ЦЕРТ-а и један или више доказа о стварном оперативном капацитету, као што су:

(1) релевантан извод из акта о унутрашњој организацији и систематизацији;

(2) уговори о раду или другом законитом ангажовању стручних лица, у редигованом облику;

(3) споразум о заједничком или секторском тиму;

(4) извештај о обављеним активностима;

(5) каталог стварно доступних услуга;

(6) други проверљиви доказ.“

Постојећи став 2. брише се као сувишан или се усклађује са овом листом.

Образложење:

Систематизовано радно место доказује формалну структуру, али не и да је место попуњено и да тим функционише. Истовремено може искључити тимове са законито ангажованим спољним стручњацима.

Ризик који се отклања:

- формализам;
- искључење малих и виртуелних тимова;
- непоуздан доказ капацитета;
- фаворизовање великих организација.

Правни и међународни основ:

Принцип материјалне истине у управном поступку; пропорционалност; FIRST Framework.

Очекивани ефекат:

- више врста прихватљивих доказа;
- смањење одбијања због организационе форме;
- боља веза између доказа и стварног рада.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 15

Јавни RFC 2350 минимум и заштићени оперативни анекс

Одредба на коју се односи:
Члан 6, став 1, тачка 2).

Постојећи текст:

„попуњен документ RFC 2350... на којој је тај документ јавно објављен“ (Ratel)

Предложени текст:

Тачка 2) мења се и гласи:

„2) јавни RFC 2350 профил израђен према Прилогу 3, који садржи:

(1) назив и мандат;

(2) корисничку заједницу;

(3) основни каталог услуга;

(4) генеричке јавне контакте;

(5) радно време;

(6) јавни кључ или други јавни начин безбедне комуникације;

(7) општа правила пријављивања и поверљивости;

(8) број верзије и датум.

Оперативно осетљиви контакти, резервни канали, интерне ескалационе процедуре, резервне локације и други поверљиви подаци достављају се у заштићеном оперативном анексу, који није јавно доступан.“

Образложење:

RFC 2350 подстиче транспарентност према корисничкој заједници, али не захтева објаву свих интерних процедура. (RFC Editor)

Ризик који се отклања:

- phishing;
- социјални инжењеринг;
- откривање ескалационих процедура;
- откривање интерних ограничења и резервних контаката.

Правни и међународни основ:

RFC 2350; NIS2 поверљивост и безбедна сарадња; Закон о информационој безбедности.

Очекивани ефекат:

- сваки ЦЕРТ има употребљив јавни профил;
- нула јавних резервних и интерних контаката;
- 100% осетљивих анекса има ограничен приступ.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 16

Поверљивост SIM3 самопроцене и планова унапређења

Одредба на коју се односи:

Члан 6, после става 3.

Постојећи текст:

„Самопроцена... мора бити потпуна и обухватати све параметре SIM3.“ (Ratel)

Предложени текст:

После става 3. додаје се нови став:

„SIM3 самопроцена, образложења параметара, приложени докази и планови унапређења сматрају се безбедносно осетљивом службеном документацијом.

Документа из става 4. нису јавно доступна. Приступ се одобрава само овлашћеним лицима чији је приступ неопходан за поступак, контролу законитости или координацију у случају ризика и инцидента.

Свако приступање, преузимање, измена, извоз или достављање трећем лицу евидентира се у системском логу.“

Образложење:

Резултати могу открити непостојеће или недокументоване процесе, кадровске празнине, ограничења алата и друге слабости. ENISA користи SIM3 за развој зрелости, али то не значи да резултати треба да буду јавни. (ENISA)

Ризик који се отклања:

- циљани напад;
- злоупотреба кадровских празнина;
- репутациона штета;
- неовлашћено профилисање тимова.

Правни и међународни основ:

NIS2; Закон о информационој безбедности; начела интегритета и поверљивости; Конвенција 108.

Очекивани ефекат:

- 100% приступа SIM3 документима је логован;
- нула јавних појединачних резултата;
- документована контрола овлашћења.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 17

Критеријуми провере, стручност оцењивача и право на другу проверу

Одредба на коју се односи:
Члан 6, последњи став.

Постојећи текст:

„Национални ЦЕРТ проверава њену конзистентност са осталим доказима...“ (Ratel)

Предложени текст:

Последњи став мења се и гласи:

„Подносилац одговара за тачност и потпуност самопроцене.

Национални ЦЕРТ проверава:

1. потпуност;
2. унутрашњу логичку доследност;
3. очигледне противречности са другим доказима;
4. примену верзије модела прописане овим правилником.

Провера се спроводи према јавно објављеној методологији и контролној листи.

Проверу врши лице које је прошло документовану обуку за примену SIM3 и које није учествовало у изради самопроцене подносиоца.

Ако налаз може бити основ неповољног решења, подносилац има право на увид, изјашњење, достављање додатних доказа и другу стручну проверу коју врши лице које није учествовало у првој провери.

Провера конзистентности не представља независни аудит или сертификацију.“

Образложење:

Trusted Introducer сертификација укључује процену обучених аудитора; ENISA препознаје peer review као засебан елемент. Не сме се административна провера неформално претворити у аудит без критеријума и права странке. (ENISA)

Ризик који се отклања:

- скривени критеријуми;
- нестручна процена;
- сукоб интереса;
- неједнака пракса;
- одлука без изјашњења странке.

Правни и међународни основ:

ЗУП; принцип непристрасности; ENISA; Trusted Introducer.

Очекивани ефекат:

- 100% провера има контролну листу;
- 100% негативних налаза доставља се странци;
- најмање два нивоа контроле у спорним случајевима.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 18

Безбедан и доказив канал за подношење

Одредба на коју се односи:
Члан 7.

Постојећи текст:

„...може се поднети у писаном облику или електронским путем на веб презентацији...“ (Ratel)

и:

„...на адресу електронске поште Националног ЦЕРТ-а.“ (Ratel)

Предложени текст:

Члан 7. мења се и гласи:

„Пријава и пратећа документација подносе се:

1. преко заштићеног електронског система Националног ЦЕРТ-а;
2. преко електронског сандучета органа или другог система електронске управе који обезбеђује поуздану идентификацију и доказ о достављању;
3. шифрованом електронском поштом, као резервним каналом;
4. непосредно или поштом, у писаном облику.

Електронски систем обезбеђује:

1. идентификацију подносиоца;
2. електронски потпис или печат;
3. шифрован пренос;
4. временски жиг;
5. потврду пријема;
6. број предмета;
7. списак и контролне збирове прилога;
8. заштиту од злонамерног садржаја.

SIM3 документација, планови унапређења и оперативни анекси не достављају се незаштићеном електронском поштом.

Техничка сметња на систему органа не може ићи на штету подносиоца који учини вероватним да је покушао достављање у року.“

Образложење:

Нацрт истовремено помиње веб-презентацију и имејл, без објашњења односа та два канала. Закон о информационој безбедности захтева поуздане, доступне и поверљиве комуникационе канале Националног ЦЕРТ-а. (Paragraf)

Ризик који се отклања:

- пресретање;
- спор о пријему;
- malware;
- губитак прилога;
- компромитација имејл налога;
- неблаговременост због техничке грешке.

Правни и међународни основ:

Закон о електронском документу; Закон о информационој безбедности; NIS2.

Очекивани ефекат:

- 100% електронских поднесака има потврду и временски жиг;
- нула незаштићених SIM3 пошиљака;
- сваки прилог има доказ интегритета.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 19

Рок за одлучивање

Одредба на коју се односи:

Члан 8, после става 1.

Постојећи текст:

„О поднетој пријави... одлучује Национални ЦЕРТ, решењем...“ (Ratel)

Предложени текст:

После става 1. додаје се став:

„Решење се доноси у року од 30 дана од дана пријема уредне пријаве. Ако је због сложености предмета потребно спровести посебан испитни поступак, примењује се рок утврђен законом којим се уређује општи управни поступак.“

Образложење:

Постојећи члан не одређује посебан рок и не објашњава када се пријава сматра уредном. Због техничке сложености и могуће провере SIM3, странка мора имати предвидив временски оквир.

Ризик који се отклања:

- дуготрајно ћутање;
- неуједначена брзина поступања;
- тржишна неизвесност;
- административно одлагање.

Правни и међународни основ:

ЗУП; право на делотворно и благовремено поступање.

Очекивани ефекат:

- најмање 90% уредних пријава решено у року;
- јавно објављено просечно време поступка;
- мањи број правних средстава због ћутања.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 20

Допуна неуредне пријаве и право на изјашњење

Одредба на коју се односи:
Члан 8, нови ст. 3. и 4.

Постојећи текст:

Не постоји посебна одредба о допуни и изјашњењу.

Предложени текст:

„Ако је пријава неуредна или непотпуна, Национални ЦЕРТ позива подносиоца да је допуни у примереном року и наводи:

1. који податак или документ недостаје;
2. зашто је неопходан;
3. правни основ;
4. рок;
5. последице непоступања.

Пре доношења решења неповољног за подносиоца, Национални ЦЕРТ доставља подносиоцу чињенице, доказе и стручне оцене које могу бити основ одлуке и оставља рок од најмање осам дана за изјашњење.“

Образложење:

Техничка процена не сме бити скривени основ одбијања. Странка мора имати прилику да исправи грешку, објасни параметар или достави доказ.

Ризик који се отклања:

- одбијање због отклоњивог недостатка;
- одлука изненађења;
- једнострано техничко оцењивање;
- повећан број спорова.

Правни и међународни основ:

ЗУП; право на саслушање и делотворно учешће странке.

Очекивани ефекат:

- 100% отклоњивих недостатака претходно предмет допуне;
- 100% негативних стручних налаза доступно странци;
- смањење поништених решења.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 21

Садржај образложења и правно средство

Одредба на коју се односи:
Члан 8, нови ст. 5–7.

Постојећи текст:

Нацрт само наводи да се одлучује решењем по правилима општег управног поступка. (Ratel)

Предложени текст:

„Решење садржи:

1. оцену испуњености сваког услова из члана 4;
2. списак и оцену доказа;
3. налаз о потпуности и конзистентности документације;
4. одговор на битне наводе подносиоца;
5. датум уписа или јасне разлоге одбијања;
6. поуку о правном средству.

Низак ниво појединачног SIM3 параметра не може сам по себи бити разлог за одбијање ако су испуњени услови утврђени Законом.

Поука о правном средству садржи, у складу са законом, податке о допуштености жалбе, надлежном органу, року и начину подношења, односно могућности покретања управног спора.“

Образложење:

Подзаконски акт не треба сам да ствара нову надлежност другостепеног органа, али мора обезбедити да странка буде тачно поучена о доступној заштити. У новом Закону се код других управних аката изричито наводи када жалба није допуштена, а управни спор јесте, што показује значај јасне поуке. (Paragraf)

Ризик који се отклања:

- необразложена одлука;
- мешање SIM3 са законским условом;
- пропуштање правног лека;
- нетранспарентна пракса.

Правни и међународни основ:

ЗУП; право на делотворно правно средство; члан 6. и 13. ЕКЉП у релевантном процесном контексту.

Очекивани ефекат:

- 100% решења има структурисано образложење;
- 100% решења има потпуну поуку;
- смањење процесних грешака.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 22

Промена, хитна исправка и историја података

Одредба на коју се односи:
Члан 9.

Постојећи текст:

„...о свим променама... у року од осам дана од дана настанка промене.“ (Ratel)

Предложени текст:

Члан 9. став 1. мења се и додају се нови ставови:

„Промена службеног контакта за пријаву инцидента, службеног телефона, службене адресе електронске поште или одговорног лица пријављује се без одлагања, а најкасније у року од 24 часа од настанка промене или сазнања за њу.

Остале промене пријављују се у року од осам дана од дана када су произвеле правно или фактичко дејство.

Ако промена зависи од акта или поступања трећег лица, рок тече од дана пријема тог акта или сазнања за коначан исход.

Национални ЦЕРТ без одлагања исправља нетачан податак који је сам унео или објавио и о исправци обавештава Посебан ЦЕРТ.

Евиденција чува историју сваке промене, датум, правни основ и идентификатор лица које је измену извршило.“

Образложење:

Јединствени рок није примерен свим врстама промена. Неактуелан контакт за инцидент захтева хитну исправку, док статусна промена може зависити од регистра или другог органа.

Ризик који се отклања:

- недоступност у инциденту;
- погрешни јавни подаци;
- немогућност реконструкције измена;
- санкционисање због промене која зависи од трећег лица.

Правни и међународни основ:

Начело тачности; ЗУП; NIS2 захтеви доступности комуникације.

Очекивани ефекат:

- хитни контакти ажурирани у року од 24 часа;
- 100% промена има audit trail;
- краће трајање нетачног јавног податка.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 23

Критеријуми и ограничење учесталости захтева за ажурирање

Одредба на коју се односи:
Члан 10, став 1.

Постојећи текст:

„Посебан ЦЕРТ је у обавези да на захтев Националног ЦЕРТ-а достави ажурирану самопроцену...“ (Ratel)

Предложени текст:

Став 1. мења се и гласи:

„Национални ЦЕРТ може образложеним захтевом затражити ажурирану SIM3 самопроцену:

1. ако је од претходне потпуне самопроцене прошло најмање 12 месеци;
2. после значајне промене мандата, организације, корисничке заједнице, услуга или капацитета;
3. ако документовани инцидент указује да подаци више нису актуелни;
4. ако постоји документована противречност између Евиденције и других службених података;
5. на захтев самог Посебног ЦЕРТ-а.

Потпуна самопроцена не захтева се чешће од једном у 12 месеци, осим ако постоји непосредан и образложен безбедносни разлог.“

Образложење:

Неограничено дискрециono право може довести до селективног или пречестог захтева и несразмерног трошка.

Ризик који се отклања:

- селективна примена;
- административно узнемиравање;
- непредвидив трошак;
- преусмеравање ресурса са одговора на инциденте.

Правни и међународни основ:

Сразмерност; једнакост; правна предвидивост; ENISA континуирано унапређење као развојни, а не произвољни процес.

Очекивани ефекат:

- максимално једна редовна потпуна процена годишње;
- 100% ванредних захтева садржи образложење;
- јавна агрегирана статистика захтева.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 24

Рок, продужење, опомена и право на отклањање недостатка

Одредба на коју се односи:
Члан 10, ст. 1–3.

Постојећи текст:

„...у року од 15 дана од дана пријема захтева.“ (Ratel)

Предложени текст:

Рок од 15 дана замењује се роком од 30 дана, а ст. 2. и 3. мењају се и гласе:

„За ограничену исправку или допуну појединачног параметра може се одредити рок од 15 дана.

На образложен захтев Посебног ЦЕРТ-а рок се продужава ако постоје виша сила, већи безбедносни инцидент, значајна реорганизација, техничка сметња или други оправдан разлог.

Ако Посебан ЦЕРТ не поступи у року, Национални ЦЕРТ доставља писану опомену и оставља додатни рок који не може бити краћи од 15 дана.

Опомена садржи опис пропуста, правни основ, доказ претходног захтева, нови рок, право на изјашњење, могућност продужења и упозорење на могуће покретање поступка брисања.

Посебном ЦЕРТ-у мора се омогућити да недостатак отклони или предложи корективни план пре покретања поступка брисања.“

Образложење:

Потпуна самопроцена свих параметара може захтевати учешће више организационих јединица. Рок од 15 дана није заснован на објављеном пилот-тесту или процени административног оптерећења.

Ризик који се отклања:

- несразмеран рок;
- брисање због привременог кашњења;
- игнорисање више силе;
- недовољно упозорење.

Правни и међународни основ:

ЗУП; сразмерност; право странке на изјашњење; принцип корективног поступања пре статусне санкције.

Очекивани ефекат:

- више благовремено завршених процена;
- мањи број поступака брисања;
- свака опомена садржи прописане елементе.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 25

Нови члан 10а — поступак брисања

Одредба на коју се односи:
После члана 10.

Постојећи текст:

„Национални ЦЕРТ може покренути поступак брисања...“ (Ratel)

Нацрт не уређује даљи ток поступка.

Предложени текст:

„Поступак брисања
Члан 10а

Поступак брисања покреће се по службеној дужности писаним обавештењем које се доставља Посебном ЦЕРТ-у.

Обавештење садржи:

1. чињенице и доказе;
2. правни основ;
3. конкретан разлог;
4. рок од најмање 15 дана за изјашњење;
5. могућност отклањања недостатка;
6. могућност предлагања корективне мере.

Брисање се може извршити само ако је утврђено да:

1. Посебан ЦЕРТ више не испуњава законом прописане услове; или
2. је доставио битно нетачне податке који су били одлучујући за упис; или
3. ни после захтева, опомене и додатног рока неоправдано није отклонио недостатак који онемогућава законито вођење Евиденције.

Пре доношења решења Национални ЦЕРТ процењује тежину и трајање пропуста, стварни безбедносни ризик, сарадњу странке, могућност отклањања и примену блаже мере.

Брисање се врши образложеним решењем које садржи тест сразмерности, датум дејства, начин јавног приказа статуса, услове за поновни упис и поуку о правном средству.

Низак SIM3 резултат или нереализован план унапређења не могу сами по себи бити разлог за брисање, ако такав разлог није утврђен Законом.

Брисање се у јавном делу евидентира после коначности решења, осим ако је законом друкчије прописано.“

Образложење:

Брисање је статусна мера са репутационим и тржишним последицама. Не може се спровести као техничка измена базе података.

Ризик који се отклања:

- произвољно брисање;
- аутоматска статусна санкција;
- повреда права на изјашњење;
- репутациона штета пре коначне одлуке;
- непостојање теста сразмерности.

Правни и међународни основ:

ЗУП; право на делотворно правно средство; принцип сразмерности; инспекцијски модел Закона који најпре препознаје отклањање неправилности у разумном року. (Paragraf)

Очекивани ефекат:

- 100% брисања засновано на формалном решењу;
- 100% предмета садржи тест сразмерности;
- смањење незаконитих или преурањених брисања.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 26

Нивои приступа Евиденцији

Одредба на коју се односи:
Члан 11.

Постојећи текст:

„Национални ЦЕРТ води и ажурира Евиденцију, која је... јавно доступна...“ (Ratel)

Предложени текст:

Члан 11. мења се тако да се Евиденција дели на:

„1) јавни део;

2. део ограничено доступан овлашћеним ЦЕРТ-овима;
3. нејавни службени део;
4. строго ограничени безбедносни део.“

У јавном делу објављују се:

„јединствени број уписа, назив правног лица, назив Посебног ЦЕРТ-а, место или службена адреса за пријем поште, статус, датум уписа, датум последњег ажурирања, веб-презентација, генеричка адреса електронске поште и јавни RFC профил.“

Ограничено доступан део садржи:

„хитне и резервне контакте и податке неопходне за професионалну координацију.“

Нејавни службени део садржи:

„матични број, ПИБ, податке одговорног лица, управне акте, доказе и историју промена.“

Строго ограничени део садржи:

„SIM3 самопроцене, планове унапређења, оперативне анексе и описе слабости.“

Образложење:

Бинарна подела јавни/нејавни није довољна. Хитни контакти могу бити потребни другим овлашћеним тимовима, али не и целој јавности.

Ризик који се отклања:

- прекомерна јавност;
- недоступност неопходних контаката партнерским тимовима;
- исти режим за податке различите осетљивости;
- масовно прикупљање осетљивих података.

Правни и међународни основ:

NIS2 сарадња и поверљивост; Закон о информационој безбедности; начело најмањег овлашћења.

Очекивани ефекат:

- сваки податак има утврђен ниво приступа;
- нула јавних SIM3 резултата;
- контролисан приступ хитним контактима.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 27

Сврхе, рокови чувања, логови, резервне копије и исправка

Одредба на коју се односи:
Члан 11, став 3. и нови ставови.

Постојећи текст:

„Остали подаци... користе се искључиво у сврху ангажовања Посебних ЦЕРТ-ова...“ (Ratel)

Предложени текст:

Постојећи став 3. мења се и гласи:

„Нејавни подаци користе се искључиво ради:

1. вођења поступка уписа, промене и брисања;
2. вођења и ажурирања Евиденције;
3. координације и ангажовања;
4. поступања у случају ризика и инцидента;
5. контроле законитости и правне заштите;
6. архивирања и доказивања службеног поступања.“

Додају се ставови:

„Рокови чувања по категоријама утврђују се Прилогом 6.

Национални ЦЕРТ обезбеђује приступ по улогама, вишефакторску аутентификацију, логовање, шифровање, резервне копије, географски одвојену копију, план континуитета и периодично тестирање опоравка.

Свако лице има право да захтева исправку нетачног личног податка, а Посебан ЦЕРТ исправку сваког нетачног регистарског податка.

О свакој повреди података поступа се у складу са законом и унапред утврђеним планом реаговања.“

Образложење:

Постојећа „искључива“ сврха није тачна јер се подаци користе и за упис, проверу, промену и брисање. Закон о информационој безбедности за Национални ЦЕРТ захтева поверљивост, поузданост, доступност и резервне капацитете. (Paragraf)

Ризик који се отклања:

- обрада ван декларисане сврхе;
- неограничено чување;
- неовлашћени приступ;
- губитак података;
- немогућност исправке;
- непостојање плана за повреду података.

Правни и међународни основ:

Закон о заштити података; Закон о информационој безбедности; Конвенција 108; NIS2.

Очекивани ефекат:

- 100% приступа нејавним подацима логовано;
- годишња провера овлашћења;
- најмање један тест опоравка годишње;
- документовани рок за сваку категорију.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 28

Исправка погрешног унутрашњег упућивања и прелазни рок

Одредба на коју се односи:
Члан 12, став 1.

Постојећи текст:

„...података из члана 2. тачка 1) подт. (9)–(10)...“ (Ratel)

Предложени текст:

Речи:

„из члана 2. тачка 1) подт. (9)–(10)“

замењују се речима:

„из члана 3. тачка 1) подт. 9)–11)“.

Преостали део става мења се и гласи:

„...са роком за поступање од 90 дана од дана пријема захтева.

Изузетно, краћи рок, који не може бити краћи од 30 дана, може се одредити ако Посебан ЦЕРТ већ поседује документе у верзији и формату прописаним овим правилником. Одлука о краћем року мора бити образложена.“

Образложење:

Члан 2. нема тачку 1) са подтачкама 9) и 10); намеравано упућивање је на садржај Евиденције у члану 3. Ово је очигледна номотехничка грешка.

Распон 30–90 дана без критеријума омогућава неједнак третман.

Ризик који се отклања:

- неприменљива прелазна норма;
- различити рокови без образложења;
- кратак рок за сложене тимове;
- спор о предмету захтева.

Правни и међународни основ:

Правна сигурност; једнакост; номотехничка правила; ЗУП.

Очекивани ефекат:

- исправно упућивање;
- основни рок од 90 дана;
- 100% краћих рокова писано образложено.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 29

Заштита постојећег статуса и продужење прелазног рока

Одредба на коју се односи:

Члан 12, нови ст. 2–5; постојећи став 2. постаје став 6.

Постојећи текст:

> „Уколико Посебни ЦЕРТ не поступи... Национални ЦЕРТ доставља писану опомену...“ (Ratel)

Предложени текст:

> „Посебни ЦЕРТ уписан пре ступања на снагу овог правилника задржава статус до коначног окончања поступка усклађивања.
>
> Захтев за усклађивање садржи тачан списак докумената, верзију SIM3, техничко упутство, начин заштићене доставе, рок и могућност продужења.
>
> На образложен захтев Посебног ЦЕРТ-а рок се може продужити за додатних 90 дана због организационе сложености, измене интерних аката, недостатка кадрова, већег инцидента, техничке сметње или другог оправданог разлога.
>
> Пропуштање рока не доводи до аутоматског брисања.
>
> На поступак опомене и брисања сходно се примењују чл. 10. и 10а.“

Образложење:

Постојећи тимови могу морати да израде нови RFC профил, процене више десетина параметара и измене интерне акте. Правна сигурност захтева да раније решење остане на снази док нови поступак не буде коначно решен.

Ризик који се отклања:

- губитак статуса без коначне одлуке;
- ретроактивни ефекат;
- несразмеран прелазни трошак;
- аутоматско брисање.

Правни и међународни основ:

Правна сигурност; ЗУП; принцип легитимних очекивања и сразмерности.

Очекивани ефекат:

- нула аутоматских брисања у прелазном периоду;
- већи проценат усклађених постојећих тимова;
- мање правних спорова.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 30

Правни континуитет започетих поступака

Одредба на коју се односи:
Члан 13.

Постојећи текст:

„Даном ступања на снагу... престаје да важи Правилник... број 37/20.“ (Ratel)

Предложени текст:

После постојећег става додају се ст. 2–4:

„Поступци започети пре ступања на снагу овог правилника окончаће се по пропису по коме су започети, осим ако подносилац затражи примену новог правилника и допуни пријаву.

Решења о упису донета пре ступања на снагу овог правилника остају на снази до окончања поступка усклађивања из члана 12.

Процесне радње предузете по ранијем правилнику остају важеће ако нису у супротности са законом.“

Образложење:

Сам престанак важења старог правилника не решава статус текућих предмета и раније донетих решења.

Ризик који се отклања:

- правна празнина;
- понављање процесних радњи;
- неједнак третман предмета;
- спор о важењу решења.

Правни и међународни основ:

Правна сигурност; ЗУП; принцип економичности поступка.

Очекивани ефекат:

- сваки започети предмет има јасан процесни режим;
- нула предмета без применљивог прописа;
- очување важећих радњи.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 31

Одложена примена нових обавеза

Одредба на коју се односи:
Члан 14.

Постојећи текст:

„...ступа на снагу осмог дана од дана објављивања.“ (Ratel)

Предложени текст:

Члан 14. мења се и гласи:

„Овај правилник ступа на снагу осмог дана од дана објављивања у ‘Службеном гласнику Републике Србије’.

Одредбе које се односе на SIM3 самопроцену, планове унапређења, заштићену електронску доставу, нивое приступа и прелазно усклађивање примењују се по истеку 90 дана од дана ступања на снагу.

Примена одредаба из става 2. не може почети пре него што Регулатор:

1. објави техничко упутство;
2. обезбеди заштићени канал;
3. објави домаће обрасце и терминолошко упутство;
4. обучи овлашћена лица;
5. утврди рокове чувања и правила приступа;
6. објави обавештење о обради података.“

Образложење:

Осам дана није довољно за израду упутстава, развој безбедног система, обуку и припрему тимова.

Ризик који се отклања:

- фактички непримењљив пропис;
- импровизована достава;
- скривени критеријуми;
- неједнака почетна пракса.

Правни и међународни основ:

Правна сигурност; сразмерност; стандарди квалитетне регулативе и процене ефеката.

Очекивани ефекат:

- сви предуслови доступни пре почетка рокова;
- мање техничких грешака;
- већи проценат уредних првих пријава.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 32

Нови члан 14а — обавезно техничко упутство

Одредба на коју се односи:
После члана 14, уз одговарајуће пренумерисање завршних одредаба.

Постојећи текст:

Не постоји.

Предложени текст:

„Техничко упутство
Члан 14а

Национални ЦЕРТ доноси и јавно објављује техничко упутство за примену овог правилника најкасније 30 дана од дана његовог ступања на снагу.

Упутство садржи:

1. правила попуњавања образаца;
2. SIM3 верзију и тумачење параметара;
3. RFC 2350 јавни профил и оперативни анекс;
4. примере доказа;
5. критеријуме провере;
6. формате и величину прилога;
7. правила електронског потписивања;
8. поступак шифроване доставе;
9. правила означавања поверљивости;
10. поступак у случају техничке грешке;
11. контакт за корисничку подршку.

Техничким упутством не могу се уводити нови услови, обавезе, разлози одбијања или брисања који нису прописани законом и овим правилником.“

Образложење:

Техничко упутство је потребно, али не сме постати „скривени пропис“.

Ризик који се отклања:

- скривени критеријуми;
- различито поступање службеника;
- техничка неуредност пријава;
- проширење обавеза без консултација.

Правни и међународни основ:

Правна сигурност; хијерархија прописа; приступачност управног поступка.

Очекивани ефекат:

- једно јавно упутство пре примене;
- мањи број техничких допуна;
- нула нових материјалних услова уведених упутством.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 33

Нови члан 14б — процена утицаја на заштиту података и безбедносна процена

Одредба на коју се односи:
После новог члана 14а.

Постојећи текст:

Не постоји.

Предложени текст:

„Претходне процене
Члан 14б

Пре почетка обраде података у новом или битно измењеном информационом систему Регулатор:

1. утврђује да ли су испуњени услови за обавезну процену утицаја обраде на заштиту података о личности и, ако јесу, спроводи је пре почетка обраде;
2. спроводи процену ризика информационе безбедности Евиденције;
3. спроводи процену ризика употребе сваког спољног алата или сервиса;
4. утврђује токове података, место обраде, руковаоце, обрађиваче и подизвођаче;
5. прибавља мишљење лица за заштиту података;
6. објављује неосетљиви сажетак процена.

Ако процена покаже неприхватљив ризик који није могуће умањити одговарајућим мерама, спољни алат или планирана радња обраде не користе се.“

Образложење:

Повереник наводи да се процена утицаја спроводи пре почетка обраде ако је вероватно да ће нова технологија и природа, обим, околности или сврха обраде створити висок ризик. (Data Protection Advocate)

Ризик који се отклања:

- непознати токови података;
- прекогранични пренос без основа;

- употреба небезбедног сервиса;
- неидентификован обрађивач;
- неприпремљено реаговање на повреду.

Правни и међународни основ:

Закон о заштити података; смернице Повереника; Конвенција 108; NIS2.

Очекивани ефекат:

- документована процена пре примене;
- јавни сажетак;
- нула спољних алата без анализе података и безбедности.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 34

Нови члан 14в — подршка малим и новоосниваним ЦЕРТ-овима

Одредба на коју се односи:
После новог члана 14б.

Постојећи текст:

Не постоји.

Предложени текст:

> **„Пропорционалност и стручна подршка**
> **Члан 14в**
>
> Национални ЦЕРТ обезбеђује малим, новоосниваним, академским и непрофитним Посебним ЦЕРТ-овима:
>
> 1. бесплатне обрасце;
> 2. најмање једну бесплатну обуку годишње;
> 3. приступачно онлајн упутство;
> 4. корисничку подршку;
> 5. могућност фазног достављања плана унапређења;
> 6. примере доказа примерене различитим организационим моделима.
>
> Обим плана унапређења и документације одређује се сразмерно мандату, корисничкој заједници, услугама, величини и ризику тима.
>
> Немогућност ангажовања спољног консултанта не може сама по себи бити разлог за одбијање уписа.“

Образложење:

Униформни трошкови несразмерно оптерећују мале тимове и могу створити тржишну баријеру. FIRST Framework изричито полази од тога да тимови бирају услуге према мандату и корисничкој заједници. (FIRST)

Ризик који се отклања:

- фаворизовање великих организација;
- одустајање малих тимова;
- регионална концентрација;
- смањена иновација и конкуренција.

Правни и међународни основ:

Сразмерност; једнакост; заштита конкуренције; приступни стандарди добре регулативе.

Очекивани ефекат:

- најмање једна бесплатна обука годишње;

- праћење удела малих и новооснованих тимова;
- мања стопа одустајања од пријаве.

Приоритет: II

АМАНДМАН/ПРЕДЛОГ БРОЈ 35

Нови члан 14г — периодично преиспитивање ефеката

Одредба на коју се односи:
После новог члана 14в.

Постојећи текст:

Не постоји.

Предложени текст:

„Праћење и процена ефеката
Члан 14г

Регулатор после 12 месеци од почетка примене објављује први извештај о примени, а после 24 месеца спроводи потпуну накнадну процену ефеката.

Извештај садржи најмање:

1. број примљених, допуњених, одобрених, одбијених и одбачених пријава;
2. просечно трајање поступка;
3. број захтева за ажурирање;
4. број опомена и поступака брисања;
5. број правних средстава и исхода;
6. административне и буџетске трошкове;
7. утицај на мала и средња предузећа;
8. регионалну и секторску структуру;
9. број повреда података и безбедносних инцидената у вези са Евиденцијом;
10. оцену користи за координацију и сајбер-безбедност.

Подаци се објављују агрегирано и без откривања појединачних SIM3 резултата или других осетљивих података.

Регулатор у процену укључује представнике Посебних ЦЕРТ-ова, привреде, академске заједнице, стручних удружења и организација цивилног друштва.“

Образложење:

Нацрт уводи нове обавезе без потпуне квантитативне процене трошкова. Потребно је проверити стварне, а не само очекиване ефекте.

Ризик који се отклања:

- трајно задржавање неефикасних решења;
- непримећена тржишна баријера;
- непрозирни трошкови;
- недостатак јавне одговорности.

Правни и међународни основ:

Закон о планском систему и методологија анализе ефеката; принцип одговорне регулације. (Pravno-informacioni sistem)

Очекивани ефекат:

- први извештај после 12 месеци;
- пуна процена после 24 месеца;
- јавни индикатори примене;
- благовремене измене ако се утврде негативни ефекти.

Приоритет: II

АМАНДМАН/ПРЕДЛОГ БРОЈ 36

Потпуна замена Обрасца 1

Одредба на коју се односи:
Образац 1.

Постојећи текст:

Образац садржи, између осталог:

> „Адреса Посебног ЦЕРТ-а...“, „Број факса...“, „Самопроцена нивоа зрелости према SIM3“ и „У Београду...“ (Ratel)

Предложени текст:

Образац 1 замењује се новим обрасцем са следећим блоковима:

I. Идентификација подносиоца

1. пословно име или назив;
2. матични број;
3. ПИБ;
4. службена адреса за доставу;
5. законски заступник;
6. овлашћени подносилац;
7. основ овлашћења;
8. службени контакт за поступак;
9. адреса за електронско достављање.

II. Подаци о Посебном ЦЕРТ-у

1. назив;
2. организациона форма;
3. матично правно лице;
4. корисничка заједница;
5. мандат;
6. место рада;
7. службена адреса за пошту;
8. веб-презентација;
9. генерички имејл;
10. контакт за пријаву инцидента;
11. категорија величине и датум пресека.

III. Одговорно лице

1. име и презиме;
2. функција;
3. службени телефон;
4. службени имејл;
5. датум почетка овлашћења.

Образац садржи напомену:

> „Не уносе се адреса пребивалишта или боравишта, приватни телефон и приватни имејл.“

IV. RFC 2350

1. број верзије;
2. датум;
3. URL јавног профила;
4. контролни збир архивске копије;
5. постојање оперативног анекса;
6. ознака поверљивости анекса.

V. SIM3

1. назив и верзија;
2. датум самопроцене;
3. локална датотека;
4. контролни збир;
5. добровољни спољни линк;
6. изјава да ли су подаци пренети спољном сервису;
7. списак приложених планова.

VI. Прилози

За сваки прилог:

- назив;
- формат;
- величина;
- контролни збир;
- ниво поверљивости;
- основ ограничења приступа.

VII. Изјаве

„Потврђујем да су достављени подаци тачни, потпуни и актуелни.“

„Потврђујем да су физичка лица обавештена о обради њихових података.“

„Означени су прилози који садрже пословну тајну, личне или безбедносно осетљиве податке.“

VIII. Обавештење о обради

Образац садржи:

- идентитет руковаоца;
- контакт;
- контакт лица за заштиту података;
- сврху;
- правни основ;
- примаоце;
- рокове;
- права лица;
- право на притужбу Поверенику;
- податке о спољним обрађивачима и преносу.

IX. Потпис

„У _____, дана _____ године.“

Предвидети:

- својеручни потпис;
- квалификовани електронски потпис;

- електронски печат правног лица.

Образложење:

Постојећи образац није усклађен са свим подацима из члана 3, не садржи SIM3 верзију, поверљивост, доказ интегритета, обавештење о обради ни електронски потпис. Формула „У Београду“ није примерена подносиоцима из целе Србије.

Ризик који се отклања:

- неуредне пријаве;
- прекомерна обрада;
- неозначени осетљиви прилози;
- спор о верзији;
- недоказив потпис;
- неједнак положај подносилаца ван Београда.

Правни и међународни основ:

Чл. 3, 5–7. Правилника после измена; Закон о заштити података; Закон о електронском документу.

Очекивани ефекат:

- 100% пријава садржи верзије и датуме;
- сваки осетљиви прилог има ознаку;
- сва лица добијају обавештење о обради;
- електронске пријаве су проверљиво потписане.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 37

Потпуна замена Обрасца 2

Одредба на коју се односи:
Образац 2.

Постојећи текст:

Наслов садржи спојени текст:

„ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМСИСТЕМИМА“ (Ratel)

Образац не садржи SIM3 промену, датум настанка, основ промене или доказ.

Предложени текст:

Образац 2 замењује се новим обрасцем који садржи:

I. Идентификација уписа

1. јединствени број уписа;
2. број решења;
3. назив правног лица;
4. назив Посебног ЦЕРТ-а.

II. Подаци о промени

За сваку промену:

1. назив поља;
2. постојећи податак;
3. нови податак;
4. датум настанка;
5. датум сазнања;
6. правни или фактички основ;

7. приложени доказ;
8. степен поверљивости.

III. Врста промене

Означава се једно или више:

- хитан контакт;
- одговорно лице;
- адреса;
- назив;
- организациона форма;
- величина тима;
- RFC верзија;
- RFC линк;
- SIM3 верзија;
- датум самопроцене;
- план унапређења;
- престанак рада;
- друга промена.

IV. Посебни захтеви

- захтев за исправку грешке органа;
- образложење кашњења;
- захтев за продужење;
- захтев за хитну објаву исправног контакта.

V. Изјаве, обавештење о обради и потпис

Примењују се одговарајући блокови из Обрасца 1.

Наслов се исправља тако да гласи:

> „ПРИЈАВА ЗА УПИС ПРОМЕНЕ ПОДАТАКА САДРЖАНИХ У ЕВИДЕНЦИЈИ ПОСЕБНИХ ЦЕНТАРА ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМИМА“.

Образложење:

SIM3 је по члану 3. податак Евиденције, али га Образац 2 не садржи. То онемогућава потпуну примену члана 9.

Ризик који се отклања:

- немогућност пријаве свих промена;
- непотпун службени траг;
- неажурна самопроцена;
- спор о благовремености;
- техничке и језичке грешке.

Правни и међународни основ:

Начело усклађености прилога са нормативним текстом; тачност података; ЗУП.

Очекивани ефекат:

- свака категорија из члана 3. може бити промењена кроз образац;
- смањење слободних и неструктурисаних поднесака;
- потпуна историја промена.

Приоритет: I

АМАНДМАН/ПРЕДЛОГ БРОЈ 38

Редакцијске и номотехничке исправке

Одредба на коју се односи:
Чл. 2, 3, 6, 9. и 12. и обрасци.

Постојећи текст:

Уочени су, између осталог:

- различито означавање подтачака „9)“, „(10)“, „(11)“;
- „ка е веб презентацији“;
- „пријава уписа промене“ уместо „пријава за упис промене“;
- погрешно упућивање у члану 12;
- спојени текст у Обрасцу 2;
- непотпуна интерпункција у пољу адресе.

Предложени текст:

Пре утврђивања коначног текста извршити:

1. уједначавање нумерације;
2. исправку свих унутрашњих упућивања;
3. уједначавање термина „веб-презентација“;
4. уједначавање „Посебан ЦЕРТ“/„посебни ЦЕРТ“;
5. исправку „пријава за упис промене“;
6. исправку спојених речи;
7. уједначавање употребе цртице и црте;
8. уједначавање назива Закона и органа;
9. језичку и правописну редактуру образаца;
10. проверу да сва поља образаца имају основ у нормативном тексту.

Образложење:

Номотехничке грешке могу имати материјалну последицу, посебно када погрешно упућивање одређује предмет прелазне обавезе.

Ризик који се отклања:

- погрешна примена;
- различито тумачење;
- непотпуна пријава;
- неизводљива прелазна одредба.

Правни и међународни основ:

Принцип јасности и одређености прописа.

Очекивани ефекат:

- нула погрешних унутрашњих упућивања;
- потпуна усклађеност образаца и чланова;
- језички и технички исправан коначни текст.

Приоритет: III, осим исправке члана 12, која је **I**.

---

2. Предлог нових прилога

Прилог 3 — Домаћи RFC 2350 профил

Треба да садржи:

1. обавезни јавни минимум;

2. необавезна јавна поља;
3. поља која се не објављују;
4. заштићени оперативни анекс;
5. правила верзионирања;
6. правила електронског потписивања;
7. српско-енглески речник;
8. правила приступачности.

Прилог 4 — SIM3 самопроцена

Треба да садржи:

1. пун назив и верзију;
2. датум верзије;
3. све параметре;
4. дефиниције нивоа;
5. категорију „није применљиво“, уз образложење;
6. поље за доказ;
7. поље за план;
8. поље за степен поверљивости;
9. правила архивирања;
10. машински читљив офлајн формат.

Прилог 5 — Методологија величине тима

Треба да уреди:

- еквивалент пуног радног времена;
- непуно радно време;
- спољна ангажовања;
- заједничке ресурсе;
- лица ангажована у више тимова;
- датум пресека.

Прилог 6 — Матрица рокова чувања

Категорија	**Предложени режим**
Решења и основни регистарски траг	Према прописима о архивској грађи
Актуелни јавни контакти	Док су актуелни
Застарели јавни контакти	Уклонити без одлагања
Подаци бившег одговорног лица	До истека рокова правне заштите, затим преиспитати
SIM3 самопроцена	До замене новом и истека рокова правне заштите
Планови унапређења	До окончања и истека контролног периода
Неуспеле пријаве	До окончања поступка и истека правне заштите

Логови приступа	Рок заснован на процени ризика, не краћи од периода потребног за истрагу инцидента
Резервне копије	Према документованом циклусу и плану опоравка

---

3. Минимални пакет измена без ког Нацрт не треба усвојити

Као апсолутни минимум треба прихватити амандмане који обезбеђују:

1. фиксну SIM3 верзију;
2. забрану аутоматске примене будућих измена;
3. домаће упутство;
4. офлајн алтернативу;
5. брисање приватне адресе одговорног лица;
6. ограничење јавне физичке адресе;
7. јавни RFC минимум и заштићени анекс;
8. поверљивост SIM3 резултата;
9. безбедан канал;
10. рок за одлучивање;
11. допуну и изјашњење;
12. образложено решење и поуку;
13. критеријуме и максималну учесталост ажурирања;
14. продужење рокова;
15. потпуно уређен поступак брисања;
16. нивое приступа;
17. рокове чувања и логовање;
18. процену утицаја и безбедности;
19. исправку члана 12;
20. усклађивање образаца;
21. одложену примену;
22. техничко упутство пре почетка примене.

---

4. Коначна амандманска оцена

Предложени пакет не негира потребу да Евиденција буде тачна, ажурна и оперативно употребљива. Он спречава да се тај циљ остварује:

- неодређеним спољним стандардом;
- незаштићеном доставом;
- прекомерном обрадом;
- скривеним критеријумима;
- несразмерним трошковима;
- статусним брисањем без пуног поступка;
- техничким упутством које би фактички постало нови пропис.

Закључна формула:

> **Нацрт захтева системске, а не само редакцијске измене. Пре уписа морају бити јасни услови. Пре самопроцене — верзија и критеријуми. Пре доставе**

— безбедан канал. Пре јавности — минимизација. Пре брисања — чињенице, право на изјашњење, сразмерност и делотворна правна заштита.

Прилог 3 — Списак извора

ИЗВОРИ И ХИЈЕРАРХИЈА ИЗВОРА

1. Основно методолошко правило

Анализа Нацрта правилника мора се заснивати првенствено на **званичним, важећим, аутентичним и непосредно проверљивим изворима**.

Ниједан налаз о законитости, уставности, правима и обавезама субјеката, надлежности РАТЕЛ-а, положају Националног ЦЕРТ-а, обради података, управном поступку или међународним обавезама не сме се заснивати искључиво на:

- медијском тексту;
- незваничном пречишћеном тексту прописа;
- презентацији;
- стручном блогу;
- комерцијалној правној бази;
- незваничном преводу;
- саопштењу које не садржи текст правне норме;
- интерној или приватној методологији;
- условима чланства у струковној организацији.

Такви извори могу имати помоћну, објашњавајућу или упоредну вредност, али не могу заменити пропис, потврђени међународни уговор, званични акт органа или изворни текст техничког стандарда.

За свако спорно питање потребно је утврдити:

1. који извор садржи правно правило;
2. ко је извор донео или објавио;
3. да ли је извор правно обавезујући;
4. на које субјекте и ситуације се примењује;
5. да ли је важио у тренутку израде и објављивања Нацрта;
6. да ли је и даље на снази у тренутку анализе;
7. да ли је доступан званичан пречишћен текст;
8. да ли су ступање на снагу и почетак примене временски раздвојени;
9. да ли постоје прелазне одредбе;
10. да ли је извор касније измењен, допуњен, замењен или стављен ван снаге.

---

2. Примарни извори поступка

Као непосредне изворе за утврђивање садржаја предложеног регулаторног решења користити:

1. Текст Нацрта правилника

Текст Нацрта је основни предмет нормативне анализе.

Анализирати:

- назив акта;
- правни основ наведен у уводној формули;
- доносиоца;
- предмет уређивања;
- дефиниције;
- права, обавезе и овлашћења;
- услове за упис;

- садржај евиденције;
- начин достављања података;
- поступак одлучивања;
- ажурирање података;
- услове брисања;
- јавност и заштиту података;
- прелазне и завршне одредбе;
- ступање на снагу и почетак примене.

За сваки налаз обавезно означити:

Нацрт правилника, члан __, став __, тачка __.

Када се анализира формулација која није нумерисана, навести назив одељка и дословни део текста.

2. Образложење Нацрта

Образложење користити ради утврђивања:

- разлога за доношење;
- проблема који се наводно решава;
- циљева прописа;
- објашњења појединих решења;
- процењених финансијских и административних последица;
- разлога за избор RFC 2350 и SIM3;
- односа са важећим правилником;
- очекиваних ефеката;
- процене потребних кадровских, техничких и буџетских капацитета.

Образложење **није нормативни текст** и не може допунити, изменити или исправити правну норму која није довољно јасно формулисана у самом Правилнику.

Ако је неко ограничење, услов, гаранција или право наведено само у образложењу, а не и у нормативном тексту, то означити као посебан ризик правне несигурности.

3. Обрасци који су саставни део Нацрта

Обрасце анализирати као нормативне прилоге ако је самим Правилником предвиђено да чине његов саставни део.

Проверити:

- да ли су обрасци усклађени са члановима Правилника;
- да ли се њима траже подаци који нису предвиђени нормативним текстом;
- да ли недостају подаци које Правилник изричито захтева;
- да ли обрасци уводе додатне обавезе;
- да ли су поља јасна и недвосмислена;
- да ли се раздвајају службени и приватни контакт подаци;
- да ли се омогућава означавање пословне тајне и безбедносно осетљивих података;
- да ли постоји обавештење о обради података о личности;
- да ли су предвиђени електронски потпис, електронски печат и потврда пријема;
- да ли су верзије RFC 2350 и SIM3 прецизно означене.

У случају несагласности између нормативног текста и обрасца, предност има нормативни текст, али несагласност мора бити означена као недостатак који треба отклонити пре усвајања.

4. Обавештење РАТЕЛ-а о јавним консултацијама

Обавештење користити за утврђивање:

- назива поступка;

- органа који спроводи консултације;
- почетка и завршетка консултација;
- начина достављања примедаба;
- адресе за достављање;
- електронске адресе;
- обавезних података подносиоца;
- пратеће документације;
- начина објављивања резултата;
- евентуалних посебних процесних упутстава.

Подаци из обавештења морају се упоредити са подацима објављеним на Порталу еКонсултације. У случају разлике, потребно је:

1. забележити оба податка;
2. утврдити који је касније објављен;
3. проверити да ли је објављена исправка;
4. затражити појашњење од РАТЕЛ-а;
5. применити процесно сигурније решење, нарочито у погледу рока и начина достављања.

5. Страница поступка на Порталу еКонсултације

Страница поступка користи се за утврђивање службеног јавног трага поступка, укључујући:

- идентификациони број поступка;
- назив органа;
- фазу поступка;
- рок;
- објављене документе;
- накнадне измене и допуне;
- обавештења;
- примљене коментаре, ако су јавни;
- извештај о спроведеним консултацијама;
- коначни исход поступка.

За сваки документ преузет са Портала еКонсултације забележити:

- назив датотеке;
- датум преузимања;
- формат;
- број страна;
- величину датотеке;
- евентуалну ознаку верзије;
- контролни збир датотеке, ако се успоставља строжи протокол архивирања.

---

3. Правно обавезујући извори Републике Србије

1. Устав Републике Србије

Устав користити као највише унутрашње правно мерило.

Посебно размотрити одредбе о:

- владавини права;
- јединству правног поретка;
- законитости рада органа и ималаца јавних овлашћења;
- заштити података о личности;

- тајности комуникација;
- праву на обавештеност;
- праву на правно средство;
- једнакој заштити права;
- ограничењу људских права;
- надлежностима Републике Србије;
- хијерархији домаћих и међународних извора;
- сагласности подзаконских аката са законом.

Према уставној хијерархији, закони и други општи акти морају бити у сагласности са Уставом и не смеју бити у супротности са потврђеним међународним уговорима и општеприхваћеним правилима међународног права. (Pravno-informacioni sistem)

За свако уставноправно питање навести конкретан члан Устава, а не само општу формулацију „супротно Уставу“.

2. Закон о информационој безбедности

Користити актуелни Закон о информационој безбедности, објављен у „Службеном гласнику РС“, број 91/2025. Закон уређује мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности субјеката и институционални систем информационе безбедности. (Pravno-informacioni sistem)

Посебно анализирати:

- појмове Националног и посебних ЦЕРТ-ова;
- положај и послове Националног ЦЕРТ-а;
- услове и сврху евидентирања посебних ЦЕРТ-ова;
- законско овлашћење за доношење Правилника;
- тачан предмет који закон допушта да се уреди подзаконским актом;
- обим података предвиђен законом;
- сарадњу и размену података;
- поверљивост;
- надзор;
- прелазне рокове;
- однос новог закона према ранијим прописима.

Кључни тест је:

> Да ли свака материјална обавеза прописана Нацртом има довољно јасно упориште у Закону о информационој безбедности?

Посебно проверити да ли законско овлашћење за уређивање садржаја и начина вођења евиденције обухвата и овлашћење за:

- увођење обавезне процене зрелости;
- прописивање минималних нивоа зрелости;
- обавезну употребу спољног онлајн алата;
- периодично поновно оцењивање;
- обавезне планове унапређења;
- брисање због неиспуњавања накнадно постављених захтева.

3. Закон о електронским комуникацијама

Користити актуелни Закон о електронским комуникацијама, објављен у „Службеном гласнику РС“, број 35/2023. Закон уређује област електронских комуникација и надлежности Регулаторног тела за електронске комуникације и поштанске услуге. (Pravno-informacioni sistem)

Анализирати:

- правни положај РАТЕЛ-а;

- надлежности Савета и стручне службе;
- јавна овлашћења;
- доношење општих аката;
- јавне консултације;
- транспарентност;
- објављивање аката;
- решавање у управним стварима;
- правна средства и судску контролу;
- заштиту поверљивих података.

4. Закон о општем управном поступку

Користити Закон о општем управном поступку, „Службени гласник РС“, бр. 18/2016, 95/2018 — аутентично тумачење и 2/2023 — одлука Уставног суда. (Pravni Informacioni Sistem)

Закон је релевантан ако се о:

- упису;
- одбијању уписа;
- промени података;
- брисању из евиденције;
- другим правима, обавезама или правним интересима

одлучује управним актом.

Посебно анализирати начела:

- законитости и предвидивости;
- сразмерности;
- заштите права странака;
- помоћи странци;
- делотворности и економичности;
- истине и слободне оцене доказа;
- права странке на изјашњење;
- приступа списима;
- образложења решења;
- права на жалбу или друго делотворно правно средство.

5. Закон о заштити података о личности

Закон користити за анализу сваког податка који се односи на идентификовано или одредиво физичко лице.

За сваки податак утврдити:

- ко је руковалац;
- ко је обрађивач;
- правни основ;
- конкретну сврху;
- нужност;
- сразмерност;
- рок чувања;
- круг прималаца;
- јавност податка;
- безбедносне мере;
- права лица;
- могућност прекограничног преноса;

- потребу за проценом утицаја на заштиту података.

Посебно испитати:

- име и презиме одговорног лица;
- адресу одговорног лица;
- број телефона;
- адресу електронске поште;
- податке о члановима тима;
- податке који се уносе у спољни SIM3 алат;
- јавно објављивање контактних података.

6. Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању

Користити закон објављен у „Службеном гласнику РС“, број 94/2017. Њиме је успостављен правни оквир за електронски документ, електронску идентификацију и услуге од поверења. (Pravno-informacioni sistem)

Анализирати:

- правно дејство електронског документа;
- електронски потпис;
- електронски печат;
- временски жиг;
- електронску доставу;
- пријем електронског поднеска;
- потврду пријема;
- аутентичност и интегритет документа;
- доказивање времена предаје;
- поузданост коришћене шеме електронске идентификације.

Посебно проверити да ли је достављање осетљиве документације обичном електронском поштом довољно са становишта:

- поверљивости;
- интегритета;
- аутентичности;
- доказивости пријема;
- заштите од неовлашћеног приступа.

7. Закон о слободном приступу информацијама од јавног значаја

Овај закон користити за анализу:

- јавности евиденције;
- приступа актима РАТЕЛ-а;
- приступа критеријумима за упис и брисање;
- приступа извештајима о консултацијама;
- приступа уговорима и документима који се односе на спољне алате;
- односа јавности и заштите података;
- односа јавности и пословне тајне;
- ограничења приступа због информационе безбедности.

Приликом анализе не полазити од претпоставке да је документ у целини јаван или у целини поверљив. Применити тест:

1. да ли документ садржи информацију од јавног значаја;
2. да ли постоји законски основ за ограничење;
3. да ли би приступ озбиљно повредио претежнији интерес;

4. да ли је могућ делимичан приступ;
5. да ли се осетљиви делови могу издвојити, прекрити или анонимизовати.

8. Прописи о електронској управи

Анализирати прописе који уређују:

- електронско општење органа и странака;
- електронске услуге;
- електронске евиденције;
- размену података по службеној дужности;
- јединствено електронско сандуче;
- електронску идентификацију;
- доступност електронских услуга;
- заштиту и интероперабилност информационих система.

9. Прописи о архивској грађи и канцеларијском пословању

Користити за анализу:

- евидентирања примљених пријава;
- доделе заводног броја;
- формирања предмета;
- чувања поднесака и прилога;
- рокова чувања;
- електронског архивирања;
- миграције формата;
- аутентичности архивиране документације;
- издвајања и уништавања;
- евиденције приступа;
- трајне доступности службеног трага.

Посебно утврдити да ли Нацрт довољно уређује однос између оперативне евиденције посебних ЦЕРТ-ова и службеног управног предмета у коме се одлучује о упису, промени или брисању.

---

4. Потврђени међународни уговори

Као правно обавезујуће међународне изворе користити само уговоре:

1. које је Република Србија потврдила;
2. који су ступили на снагу у односу на Републику Србију;
3. који су објављени у службеном гласилу;
4. чије су одредбе материјално релевантне за анализирано питање.

За сваки уговор навести:

- пун назив;
- међународну организацију у чијем оквиру је усвојен;
- датум усвајања;
- закон о потврђивању;
- број „Службеног гласника РС — Међународни уговори“;
- датум ступања на снагу за Републику Србију;
- конкретну одредбу;
- питање за које је одредба релевантна.

Посебно размотрити релевантне уговоре у областима:

- приватности;

- заштите података;
- људских права;
- сајбер-криминала;
- међународне сарадње;
- приступа информацијама;
- заштите критичне инфраструктуре, ако су применљиви.

Не представљати као правно обавезујуће:

- декларације;
- смернице;
- препоруке;
- приручнике;
- закључке конференција;
- политичке изјаве;
- непотврђене конвенције;
- документе међународних организација без уговорне снаге.

---

5. Право Европске уније

Изворе права Европске уније разврстати на:

1. Примарно право ЕУ

- Уговор о Европској унији;
- Уговор о функционисању Европске уније;
- Повељу ЕУ о основним правима.

2. Секундарно право ЕУ

- уредбе;
- директиве;
- одлуке;
- делегиране акте;
- спроведбене акте.

3. Необавезујуће изворе

- препоруке;
- мишљења;
- смернице;
- комуникације Европске комисије;
- документи ENISA;
- техничке смернице;
- извештаји и приручници.

За сваки акт ЕУ утврдити:

1. да ли је акт на снази;
2. да ли је непосредно применљив у државама чланицама;
3. да ли захтева транспоновање;
4. да ли је Република Србија преузела обавезу усклађивања;
5. да ли је релевантан у оквиру Споразума о стабилизацији и придруживању;
6. да ли је обухваћен преговарачким поглављем или кластером;
7. да ли је већ делимично или потпуно пренет у домаће право;
8. да ли се користи као обавезујуће или упоредно мерило.

Директиву (ЕУ) 2022/2555 — NIS2 не представљати као пропис који се непосредно примењује у Републици Србији. Користити је као:

- релевантан акт права ЕУ;
- приступно и упоредно мерило;
- извор за оцену правца усклађивања;
- мерило институционалне и техничке добре праксе,

осим у делу у ком је конкретно решење већ преузето домаћим законом или обавезујућим међународним инструментом.

---

6. Технички стандарди и најбоље праксе

1. RFC 2350

Користити изворни документ:

RFC 2350 — BCP 21, Expectations for Computer Security Incident Response, који су објавили RFC Editor/IETF механизми у јуну 1998. године.

RFC 2350 има статус „Best Current Practice“ и представља оквир за објављивање информација о политикама, услугама, надлежности, контактима и начину рада CSIRT тимова. Сам документ наглашава да није могуће утврдити јединствен скуп захтева примерен свим тимовима, већ нуди оквир и образац за представљање релевантних информација. (rfc-editor.org)

У анализи RFC 2350 означити као:

> међународно признату техничку најбољу праксу, која сама по себи није закон, потврђени међународни уговор нити непосредно обавезујући пропис Републике Србије.

Ако домаћи Правилник упути на RFC 2350 и учини његову примену обавезном, правна обавезност за домаће субјекте не произлази непосредно из RFC документа, већ из домаћег прописа који на њега упућује.

Проверити:

- да ли је означена тачна верзија;
- да ли се упућује на стабилан извор;
- да ли постоји исправка или errata;
- да ли је обезбеђен званичан или одобрени превод;
- да ли су сви делови обавезни;
- да ли су поједини делови прилагођени националном правном систему;
- да ли би објављивање свих података могло угрозити безбедност или поверљивост.

2. SIM3

SIM3 анализирати као модел процене зрелости тимова за управљање безбедносним инцидентима.

Open CSIRT Foundation одржава и развија SIM3 модел и повезане алате, док се модел користи и у поступцима самопроцене, процене и сертификације у различитим професионалним оквирима. (opencsirt.org)

У анализи обавезно утврдити:

- пуни назив модела;
- организацију која га одржава;
- верзију;
- датум верзије;
- број и структуру параметара;
- начин оцењивања;
- значење нивоа зрелости;

- правила лиценцирања;
- услове коришћења онлајн алата;
- место и начин обраде података;
- могућност офлајн процене;
- поступак измене модела;
- улогу сертификованих SIM3 аудитора;
- разлику између самопроцене и независне процене.

SIM3 не представљати као:

- закон;
- пропис Европске уније;
- потврђени међународни уговор;
- ISO стандард;
- обавезујуће правило за све ЦЕРТ-ове.

Ако Нацрт SIM3 самопроцену учини обавезном, правни основ обавезе мора бити тражен у домаћем закону и Правилнику, а не у самом моделу.

3. FIRST CSIRT Services Framework

FIRST CSIRT Services Framework користити као стручни и технички оквир за опис и развој услуга CSIRT тимова.

FIRST наводи да је сврха оквира да помогне успостављању и унапређењу рада CSIRT тимова и развоју њиховог портфолија услуга. Оквир не прописује једну обавезну комбинацију услуга за сваки тим. (FIRST)

Разликовати:

- FIRST стандарде и оквире;
- услове за чланство у FIRST-у;
- поступак пријема у чланство;
- стручне препоруке;
- правне обавезе по домаћем праву.

Услов за чланство у FIRST-у не може се аутоматски представити као општи законски услов за упис посебног ЦЕРТ-а у домаћу евиденцију.

4. Trusted Introducer

Правила Trusted Introducer користити само за:

- упоредну анализу;
- анализу професионалне акредитације и сертификације;
- проверу начина употребе SIM3;
- проверу тврдњи из образложења Нацрта.

Trusted Introducer користи SIM3 профиле у поступцима сертификације и одређује нивое које тим мора достићи у оквиру тог конкретног професионалног система. (Trusted Introducer)

Та правила:

- нису пропис Републике Србије;
- нису право Европске уније;
- нису потврђени међународни уговор;
- не обавезују организације које нису добровољно приступиле том систему, осим ако домаћи пропис на њих изричито и законито упути.

5. ISO/IEC и други стандарди

Када се користе ISO/IEC, ETSI, ENISA или други стручни стандарди и смернице, за сваки извор навести:

- пун назив и ознаку;

- верзију и годину;
- издавача;
- статус;
- област примене;
- да ли је стандард добровољан;
- да ли је преузет као српски стандард;
- да ли је прописом учињен обавезним;
- да ли је текст бесплатно и јавно доступан.

Не закључивати да је стандард правно обавезан само зато што је:

- широко прихваћен;
- наведен у смерницама;
- коришћен у поступку сертификације;
- означен као „industry standard“;
- препоручен од стране ENISA, FIRST или друге организације.

---

7. Хијерархија извора

Изворе користити у следећем редоследу правне и доказне снаге:

Ниво	**Категорија извора**	**Правна улога**
I	Устав Републике Србије	Највише унутрашње правно мерило
II	Општеприхваћена правила међународног права и потврђени међународни уговори	Део правног поретка, у складу са Уставом
III	Закони Републике Србије	Примарни законски основ права, обавеза и надлежности
IV	Уредбе и други подзаконски акти Владе	Разрада закона у границама законског овлашћења
V	Правилници и други општи акти регулаторних и управних органа	Техничка и поступовна разрада закона
VI	Појединачни управни и судски акти	Примена права у конкретном случају
VII	Званична образложења, извештаји и мишљења органа	Помоћ при тумачењу; немају снагу норме
VIII	Право ЕУ које није непосредно применљиво у Србији	Приступно, упоредно и хармонизационо мерило
IX	Технички стандарди и најбоље праксе	Стручно и техничко мерило
X	Правила чланства и сертификације професионалних организација	Уговорно или добровољно правило у оквиру организације

XI	Научни, стручни и комерцијални извори	Допунско тумачење и критичка анализа
XII	Медијски и други секундарни извори	Контекст и идентификација питања, не доказ правне норме

Ниже рангирани извор не сме се користити за измену значења извора више правне снаге.

---

8. Решавање несагласности извора

Ако су извори међусобно несагласни, применити следећи редослед провере:

1. **lex superior** — извор више правне снаге има предност;
2. **lex specialis** — посебна норма има предност у односу на општу норму, ако су исте правне снаге;
3. **lex posterior** — каснија норма може имати предност у односу на ранију норму исте правне снаге;
4. проверити прелазне и завршне одредбе;
5. проверити одлуке Уставног суда;
6. проверити аутентична тумачења;
7. проверити да ли је новим прописом ранији пропис изричито или прећутно стављен ван снаге;
8. проверити предмет, циљ и границе законског овлашћења.

Не примењивати правила lex specialis и lex posterior механички. У сваком случају образложити:

- који су извори у сукобу;
- да ли уређују исто питање;
- да ли се односе на исте субјекте;
- да ли имају исту правну снагу;
- зашто се једном извору даје предност.

---

9. Провера актуелности

За сваки пропис извршити најмање следеће провере:

- да ли је објављен у службеном гласилу;
- да ли је ступио на снагу;
- да ли је почео да се примењује;
- да ли је мењан или допуњаван;
- да ли постоји одлука Уставног суда;
- да ли постоји аутентично тумачење;
- да ли је престао да важи;
- да ли постоји нови пропис који га замењује;
- да ли је доступан важећи пречишћен текст;
- који је текст важио на дан објављивања Нацрта;
- који текст важи на дан анализе.

Као примарни електронски извор за домаће прописе користити Правно-информациони систем Републике Србије, који садржи службена гласила, регистар и текстове важећих прописа. (Pravno-informacioni sistem)

Пропис не означавати као „важећи“ само зато што је доступан на интернету.

---

10. Обавезни библиографски запис

За сваки коришћени извор формирати запис који садржи:

За домаћи пропис

- пун назив;
- доносиоца;
- службено гласило;
- број и годину;
- бројеве измена и допуна;
- конкретан члан, став, тачку или алинеју;
- статус важења;
- електронски извор;
- датум приступа.

Модел:

> Закон о _____, Народна скупштина Републике Србије, „Службени гласник РС“, бр. ***/***, ***/*** и ***/***, члан __. Електронски извор: Правно-информациони систем Републике Србије. Датум приступа: 25. јул 2026. године.

За подзаконски акт

> Правилник о _____, доносилац _____, „Службени гласник РС“, број ***/***, члан __. Електронски извор: _____. Датум приступа: 25. јул 2026. године.

За међународни уговор

> Пун назив уговора, закон о потврђивању, „Службени гласник РС — Међународни уговори“, број ***/***, члан __, датум ступања на снагу за Републику Србију _____. Датум приступа: 25. јул 2026. године.

За акт Европске уније

> Пун назив акта, институција ЕУ, број акта, CELEX број, датум усвајања, релевантни члан, статус и рок за транспоновање, ако постоји. Електронски извор: EUR-Lex. Датум приступа: 25. јул 2026. године.

За RFC

> Brownlee, N.; Guttman, E., RFC 2350 — BCP 21, Expectations for Computer Security Incident Response, RFC Editor, јун 1998, одељак __. Статус: Best Current Practice. Датум приступа: 25. јул 2026. године.

За SIM3

> Open CSIRT Foundation, Security Incident Management Maturity Model — SIM3, верзија __, година __, параметар __. Статус: модел зрелости/стручна методологија. Датум приступа: 25. јул 2026. године.

За FIRST или Trusted Introducer

> Назив организације, назив документа или поступка, верзија/датум, конкретан одељак. Статус: професионални оквир, правило чланства или сертификације — није пропис Републике Србије. Датум приступа: 25. јул 2026. године.

---

11. Ознаке правне снаге у анализи

У регистру извора сваком документу доделити једну од следећих ознака:

- **ПО — правно обавезујући извор;**
- **ПМ — приступно или хармонизационо мерило;**
- **ТС — технички стандард или најбоља пракса;**
- **ПЧ — правило чланства или сертификације;**
- **ПР — препорука или смерница;**

- **ИМ — интерна методологија;**
- **ПОИ — помоћни или интерпретативни извор;**
- **СИ — секундарни извор.**

Пример:

Извор	**Ознака**	**Правна снага**	**Начин употребе**
Закон о информационој безбедности	ПО	Закон	Основ надлежности и обавеза
NIS2 директива	ПМ	Право ЕУ; није непосредно применљива у Србији	Мерило усклађивања
RFC 2350	ТС	Best Current Practice	Технички оквир
SIM3	ТС/ИМ	Модел зрелости	Самопроцена и упоредна анализа
FIRST услови чланства	ПЧ	Правило професионалне организације	Само за чланство и упоредну анализу
Trusted Introducer профил	ПЧ	Правило сертификације	Упоредно мерило
Образложење Нацрта	ПОИ	Нема нормативну снагу	Тумачење циља предлагача

---

12. Посебан тест за упућивање на спољни стандард

Када Нацрт упућује на RFC 2350, SIM3 или други спољни документ, обавезно применити следећи тест:

1. Да ли је документ прецизно идентификован?
2. Да ли је наведена верзија?
3. Да ли је наведен датум?
4. Да ли је садржај бесплатно доступан?
5. Да ли је доступан на српском језику?
6. Да ли домаћи субјект може трајно да сачува примењену верзију?
7. Ко може изменити документ?
8. Да ли се будуће измене примењују аутоматски?
9. Да ли би аутоматска измена фактички мењала домаће обавезе без измене Правилника?
10. Да ли документ садржи опциона и обавезна правила?
11. Ко тумачи нејасне параметре?
12. Да ли постоји поступак оспоравања оцене?
13. Да ли употреба документа захтева слање података трећем лицу?
14. Да ли постоје лиценцна ограничења?
15. Да ли је обезбеђена офлајн алтернатива?
16. Да ли постоји план поступања ако документ или алат постану недоступни?
17. Да ли је стандард прилагођен домаћем правном и институционалном систему?

18. Да ли је упућивање статичко или динамичко?

Ако верзија није наведена, означити ризик да приватни или страни субјект изменом документа фактички мења обавезе домаћих субјеката без новог домаћег нормативног поступка.

---

13. Забрана погрешног представљања извора

У анализи се не смеју користити формулације:

- „међународни пропис захтева SIM3“;
- „RFC 2350 је обавезујући међународни стандард“;
- „FIRST прописује обавезе Републици Србији“;
- „Trusted Introducer захтева да сви ЦЕРТ-ови…“;
- „ENISA налаже Републици Србији…“;
- „NIS2 се непосредно примењује у Србији“,

осим ако је таква тврдња поткрепљена конкретним правно обавезујућим основом.

Користити прецизније формулације:

- „RFC 2350 препоручује…“;
- „SIM3 модел предвиђа…“;
- „у оквиру FIRST поступка чланства захтева се…“;
- „Trusted Introducer користи SIM3 у поступку сертификације…“;
- „NIS2 представља релевантно приступно и упоредно мерило…“;
- „домаћи Нацрт предлаже да се примена овог модела учини обавезном…“.

---

14. Поступање са незваничним преводима

Када званичан превод није доступан:

1. користити изворни текст;
2. навести језик изворника;
3. означити превод као радни;
4. задржати изворни термин у загради;
5. не заснивати правни закључак само на радном преводу;
6. проверити терминологију у домаћим прописима;
7. означити могуће разлике у значењу;
8. препоручити објављивање званичног или одобреног превода.

Посебну пажњу посветити појмовима:

- CERT;
- CSIRT;
- constituency;
- authority;
- mandate;
- maturity;
- assessment;
- self-assessment;
- audit;
- accreditation;
- certification;
- incident handling;
- vulnerability management;

- disclosure policy.

---

15. Документовање датума и верзије

Сваки електронски извор архивирати са:

- датумом приступа;
- називом датотеке;
- верзијом;
- датумом документа;
- веб-адресом;
- PDF копијом или другим стабилним форматом;
- снимком релевантне странице, ако је садржај динамичан;
- напоменом о каснијим изменама;
- контролним збиром, када је то практично оправдано.

Код динамичних страница, онлајн алата и методологија обавезно забележити стање на дан анализе, јер каснија измена садржаја може отежати проверу налаза.

---

16. Регистар извора

На крају анализе израдити јединствени регистар:

Бр.	Извор	Доносилац/издавач	Број и година/верзија	Релевантна одредба	Ознака снаге	Електронски извор	Датум приступа	Напомена

Регистар мора омогућити да се за сваки значајан аналитички налаз утврди:

- на ком извору је заснован;
- какав је правни статус извора;
- која је верзија коришћена;
- да ли је извор био важећи и доступан;
- да ли налаз представља правни закључак, техничку оцену или препоруку.

---

17. Завршно правило доказне дисциплине

Сваки значајан налаз означити једном од следећих категорија:

- **Нормативно утврђено** — непосредно произлази из важећег прописа;
- **Документовано у Нацрту** — произлази из текста Нацрта или прилога;
- **Наведено у образложењу** — став или тврдња предлагача;
- **Технички стандард** — произлази из признатог стручног извора;
- **Упоредно решење** — постоји у другој јурисдикцији;
- **Стручно тумачење** — аналитички закључак изведен из више извора;
- **Ризик или пројекција** — могућа последица која још није наступила;
- **Није могуће потврдити** — недостају документ, податак или званичан извор.

Одсуство јавно доступног доказа не значи аутоматски да документ или правни основ не постоји. У том случају користити формулацију:

> „Постојање и садржина документа нису могли бити потврђени на основу јавно доступне документације, због чега је потребно затражити његово достављање или објављивање.“

Овај приступ обезбеђује да се јасно раздвоје:

- право од стручне праксе;
- обавеза од препоруке;
- домаћи пропис од страног модела;
- доказана чињеница од процене;
- недостатак јавног документа од тврдње да документ не постоји.

Прилог 4 — Упоредноправни и међународни преглед

МЕЂУНАРОДНЕ ОБАВЕЗЕ И ЕВРОПСКЕ ИНТЕГРАЦИЈЕ

1. Метод анализе и категорије извора

Усклађеност Нацрта не може се оцењивати тако што се сви европски и међународни документи третирају као извори исте правне снаге.

Потребно је разликовати:

1. Правно обавезујуће изворе за Републику Србију

У ову групу спадају:

- Споразум о стабилизацији и придруживању;
- Европска конвенција о људским правима;
- Конвенција Савета Европе број 108 о заштити лица у односу на аутоматску обраду података о личности;
- други потврђени међународни уговори који су ступили на снагу у односу на Републику Србију.

Ови извори представљају део правног поретка Републике Србије у складу са Уставом.

2. Правне тековине Европске уније као приступно и хармонизационо мерило

У ову групу спадају:

- Директива (ЕУ) 2022/2555 — NIS2;
- Општа уредба о заштити података — GDPR;
- Уредба (ЕУ) број 910/2014 — eIDAS, са изменама из 2024. године;
- други релевантни акти ЕУ у области сајбер-безбедности, електронске идентификације, услуга од поверења и дигиталног тржишта.

Ови акти нису, само на основу свог постојања, непосредно применљиви као домаћи прописи у Републици Србији. Они, међутим, представљају релевантно мерило постепеног усклађивања домаћег права у оквиру Споразума о стабилизацији и придруживању и процеса приступања ЕУ.

3. Необавезујуће европске смернице и оквири

Овде спадају:

- ENISA оквири и смернице;
- европски модели зрелости;
- приручници за CSIRT тимове;
- препоруке за координисано откривање рањивости;
- смернице о размени информација и управљању инцидентима.

Ови документи имају стручну и хармонизациону вредност, али сами не стварају правне обавезе домаћим субјектима.

4. Технички стандарди и најбоље праксе

У ову групу спадају:

- RFC 2350;
- SIM3;
- FIRST CSIRT Services Framework;
- ISO/IEC стандарди;
- други признати оквири управљања инцидентима.

Они постају обавезујући за домаће субјекте само ако их домаћи пропис, уговор или други правни акт учини обавезним на довољно одређен и законит начин.

5. Правила добровољних професионалних система

Овде спадају:

- услови за чланство у FIRST-у;
- правила Trusted Introducer листирања;
- поступци Trusted Introducer акредитације и сертификације;
- правила професионалних аудитора.

Та правила обавезују само учеснике који добровољно приступе конкретном професионалном систему. Она нису општи међународни прописи.

---

2. Синтетичка матрица извора и оцене Нацрта

Извор	**Правни статус за Србију**	**Значај за приступање ЕУ**	**Однос Нацрта према извору**	**Начин примене у Нацрту**
Споразум о стабилизацији и придруживању	Правно обавезујући међународни уговор	Непосредан основ постепеног усклађивања	Делимично у складу	Селективно и без потпуне анализе усклађености
NIS2	Није непосредно применљив домаћи пропис	Кључно приступно мерило за сајбер-безбедност	Делом у складу, делом испод, у појединим аспектима изнад	Селективно
GDPR	Није опште непосредно применљив као домаћи пропис; може обухватити поједине српске субјекте у условима свог територијалног домета	Кључно приступно мерило	Испод стандарда у више процесних тачака	Делимично
eIDAS / Европски оквир дигиталног идентитета	Није непосредно применљив као домаћи пропис	Значајно приступно и интероперабилно мерило	Испод стандарда доказиве електронске доставе	Недовољно примењен
Конвенција 108	Правно обавезујућа	Истовремено европски стандард	Постоји ризик непотпуне усклађености	Делимично

Протокол 108+	Србија га је ратификовала, али модернизована Конвенција још није ступила на снагу	Снажно будуће и приступно мерило	Испод очекиваног модернизованог стандарда	Није системски примењен
Европска конвенција о људским правима	Правно обавезујућа	Основно европско мерило људских права	Ризик у погледу законитости и сразмерности обраде	Делимично
ENISA оквири	Необавезујуће стручне смернице	Значајно техничко приступно мерило	Селективно усклађен	Самопроцена преузета, peer review и шири оквир нису
RFC 2350	Best Current Practice, не пропис	Индиректан стручни значај	У основној намери у складу; обавезност и јавност могу бити шире од стандарда	Селективно
SIM3	Добровољни модел зрелости	Стручно мерило, не acquis сам по себи	Уведен строже него у многим добровољним режимима	Непотпуно и нормативно неодређено
FIRST Services Framework	Добровољни професионални оквир	Индиректан стручни значај	Делимично у складу у погледу каталога услуга	Селективно
FIRST услови чланства	Добровољна правила организације	Немају самосталну приступну снагу	Образложење их поједностављује	Делимично нетачно представљено
Trusted Introducer	Добровољни професионални систем	Нема самосталну приступну снагу	Образложење меша различите TI статусе	Непрецизно представљено
ISO/IEC стандарди	Добровољни стандарди, осим ако су правно преузети	Релевантно стручно мерило	Само посредно усклађен	Није системски примењен

3. Споразум о стабилизацији и придруживању

3.1. Правна снага

Споразум о стабилизацији и придруживању између Европских заједница, њихових држава чланица и Републике Србије јесте правно обавезујући међународни уговор. Ступио је на снагу 1. септембра 2013. године, док Србија има статус кандидата од 2012. године и води приступне преговоре од 2014. године. (Consilium)

3.2. Члан 72 — постепено усклађивање права

Члан 72. предвиђа постепено усклађивање постојећих и будућих прописа Србије са правним тековинама ЕУ и њихово правилно спровођење и примену. Обавеза није ограничена на формално преписивање правних норми, већ обухвата и изградњу административних и институционалних капацитета за њихову примену. (Eur-Lex)

Оцена Нацрта

Нацрт је **правцем усклађен** са овом обавезом зато што:

- настоји да институционализује сарадњу ЦЕРТ-ова;
- уводи проверљивији опис мандата и услуга;
- покушава да подстакне развој организационе зрелости;
- успоставља структурисанију евиденцију.

Међутим, поступак усклађивања није довољно документован јер није објављено:

- са којим конкретним одредбама NIS2 је Нацрт упоређен;
- које обавезе се преузимају;
- које нису релевантне за овај правилник;
- у чему Нацрт уводи аутономна домаћа решења;
- зашто је изабран SIM3;
- зашто су одређени баш предложени рокови и последице.

Оцена: делимична и недокументована усклађеност.

3.3. Члан 81 — заштита података

Споразум обавезује Србију да усклади законодавство о заштити података са правом ЕУ и другим европским и међународним прописима о приватности и да обезбеди делотворно функционисање независних надзорних органа. (Eur-Lex)

Оцена Нацрта

Нацрт делимично препознаје потребу за поверљивошћу јер:

- податак о величини тима није јаван;
- SIM3 резултати нису јавно доступни;
- подаци одговорног лица нису предвиђени за јавну објаву.

Ипак, испод очекиваног стандарда остају:

- нејасна „адреса одговорног лица“;
- неидентификован руковалац;
- непостојање обавештења о обради;
- непостојање рокова чувања;
- непотпуно одређене сврхе;
- неуређен однос са спољним SIM3 сервисом;
- непостојање процене утицаја на заштиту података;
- непостојање правила о повреди података.

Оцена: Нацрт је само делимично усклађен са правцем обавеза из члана 81. ССП-а.

3.4. Чл. 105. и 106 — информационо друштво и електронске комуникације

ССП предвиђа сарадњу у развоју информационог друштва, постепено усклађивање политика и прописа и подстицање интероперабилности мрежа и услуга. У области електронских комуникација сарадња је усмерена ка постепеном усклађивању са правним тековинама ЕУ. (Eur-Lex)

Оцена

Нацрт доприноси овим циљевима кроз:

- формализацију домаће ЦЕРТ заједнице;
- лакшу идентификацију тимова;
- уједначенији опис услуга;
- потенцијално лакшу прекограничну сарадњу.

Недостају, међутим:

- правила техничке интероперабилности;
- заштићени механизми размене;
- доказива електронска достава;
- правила аутентификације;
- јасна подршка европским механизмима сарадње;
- план усклађивања са NIS2 и ENISA оквирима.

---

4. NIS2 директива

4.1. Правна природа

Директива (ЕУ) 2022/2555 обавезује државе чланице ЕУ да остваре њене циљеве кроз националне прописе. Она није непосредно применљив домаћи пропис у Републици Србији.

За Србију NIS2 представља:

- релевантан део правних тековина ЕУ;
- приступно мерило;
- смер правног и институционалног усклађивања;
- упоредни стандард за процену домаћег система.

4.2. Разлика између NIS2 CSIRT-а и посебних ЦЕРТ-ова

Чл. 10. и 11. NIS2 односе се пре свега на CSIRT тимове које држава чланица формално одреди за обављање законом утврђених националних функција. Они морају имати:

- адекватне ресурсе;
- безбедну и отпорну комуникациону инфраструктуру;
- високу доступност;
- одговарајуће просторије;
- континуитет пословања;
- обучено особље;
- резервне системе и радни простор;
- способности за обраду инцидената и сарадњу. (Eur-Lex)

Посебни ЦЕРТ-ови из Нацрта могу бити:

- интерни корпоративни тимови;
- секторски тимови;
- академски тимови;
- комерцијални пружаоци услуга;

- организационе јединице приватних или јавних правних лица.

Зато се сви захтеви NIS2 за национално одређене CSIRT тимове не могу аутоматски пренети на сваки посебан ЦЕРТ.

Кључна последица

NIS2 сам по себи не захтева да сваки приватни или секторски тим:

- буде уписан у јавну националну евиденцију;
- објави целокупан RFC 2350;
- достави SIM3 самопроцену;
- изради план за сваки параметар испод нивоа 2;
- буде избрисан из евиденције ако не достави нову самопроцену.

У том делу Нацрт уводи **аутономно домаће решење које иде изнад минималних захтева NIS2**, али без објављене анализе нужности и сразмерности.

4.3. Захтеви за безбедност, поверљивост и сарадњу

NIS2 захтева да CSIRT тимови обезбеде безбедне комуникационе канале и да у сарадњи са другим тимовима поштују правила заштите података и поверљивости. Размена информација мора бити нужна, релевантна и сразмерна, уз заштиту пословних интереса и безбедности података. (Eur-Lex)

Поређење са Нацртом

NIS2 стандард	Решење Нацрта	Оцена
Безбедни комуникациони канали	Документи се могу слати електронском поштом без прописаног шифровања	Испод стандарда
Висока доступност CSIRT-а	Нацрт не уређује доступност	Ван ужег предмета, али није могуће закључити усклађеност
Континуитет и резервни системи	Није уређено	Ван ужег предмета; потребно у ширем систему
Адекватно обучено особље	Тражи се број чланова, не и компетенције	Делимично
Безбедна размена информација	RFC помиње методе, али Правилник не прописује минимум	Испод стандарда
Поверљивост	Постоји јавни/нејавни режим	Делимично
Сразмерност размене	Није изричито уређена	Испод стандарда
Сарадња са другим CSIRT-овима	Посредно кроз RFC и Евиденцију	Делимично
Координација са трећим државама	Није уређена	Није непосредни предмет

Нацрт не треба оптеретити свим оперативним захтевима NIS2 ако је његов предмет само Евиденција. Међутим, не сме се тврдити да је Нацрт потпуно усклађен са NIS2 само зато што уводи SIM3.

4.4. Координисано откривање рањивости

Члан 12. NIS2 предвиђа да један од национално одређених CSIRT тимова има улогу координатора за координисано откривање рањивости. Тај координатор делује као поуздани посредник, омогућава и анонимно пријављивање када се то захтева и сарађује са другим националним координаторима и ENISA-ом. (Eur-Lex)

Нацрт не уређује:

- који посебни ЦЕРТ може примати пријаве рањивости;
- како се рањивости прослеђују Националном ЦЕРТ-у;
- правила анонимног пријављивања;
- заштиту истраживача;
- координацију са произвођачима;
- рокове објављивања;
- приступ европској бази рањивости.

Ово није нужно недостатак самог правилника о Евиденцији. Међутим, RFC 2350 профил треба да садржи јасну информацију:

- да ли тим прима пријаве рањивости;
- по којој процедури;
- којим безбедним каналом;
- да ли и коме их прослеђује.

4.5. Укупна оцена према NIS2

Нацрт је:

- **у складу са правцем NIS2** у погледу институционализације сарадње, идентификације тимова и подстицања зрелости;
- **изнад NIS2** у делу у ком свим посебним ЦЕРТ-овима намеће свеобухватну SIM3 самопроцену и развојне планове;
- **испод NIS2 стандарда** у погледу безбедне електронске комуникације, поверљивости, доказивости размене и контроле приступа;
- **непотпун** у погледу координисаног откривања рањивости;
- **селективно усклађен**, али не представља потпуно преношење NIS2.

---

5. Право ЕУ о заштити података

5.1. Правна природа GDPR-а

GDPR је уредба која се непосредно примењује у државама чланицама ЕУ. Република Србија није држава чланица, па GDPR није општи домаћи пропис. Ипак:

- представља кључно приступно мерило;
- релевантан је преко члана 81. ССП-а;
- може се, под условима свог територијалног домета, применити на поједине субјекте из Србије;
- домаћи Закон о заштити података о личности већ преузима бројна решења европског модела.

5.2. Начела обраде

GDPR захтева:

- законитост, правичност и транспарентност;
- ограничење сврхе;
- минимизацију;
- тачност;
- ограничење чувања;
- интегритет и поверљивост;
- одговорност руковаоца. (Eur-Lex)

Поређење

Начело	Стање у Нацрту	Оцена
Законитост	Постоји законски основ за Евиденцију, али је спорна ширина SIM3 режима	Делимично
Транспарентност	Обрасци немају обавештење о обради	Испод стандарда
Ограничење сврхе	Члан 11 наводи ужу сврху од стварне употребе	Неусклађено
Минимизација	„Адреса одговорног лица“ је прекомерна и неодређена	Испод стандарда
Тачност	Постоји рок за промену	Делимично усклађено
Ограничење чувања	Рокови не постоје	Испод стандарда
Интегритет и поверљивост	SIM3 је нејаван, али канал и приступ нису уређени	Делимично
Одговорност	Руковалац и обрађивачи нису идентификовани	Испод стандарда

5.3. Обавештење лицу

Европски стандард захтева да се лицу чији се подаци прикупљају саопште:

- идентитет и контакт руковаоца;
- контакт лица за заштиту података;
- сврха;
- правни основ;
- примаоци;
- рок чувања;
- права лица;
- могући преноси. (Eur-Lex)

Обрасци 1 и 2 не садрже ниједан од ових блокова.

5.4. Обрађивачи и спољни SIM3 сервис

Када спољни пружалац услуге обрађује податке за рачун руковаоца, европски стандард захтева правно уређен однос, документована упутства, поверљивост, безбедносне мере и контролу подизвођача. (Eur-Lex)

Пре прописивања обавезног SIM3 онлајн алата треба утврдити:

1. да ли се подаци заиста шаљу серверу;
2. који се метаподаци прикупљају;
3. да ли се резултат чува;
4. где су сервери;
5. ко има приступ;
6. да ли је спољни субјект обрађивач или самостални руковалац;
7. да ли постоји пренос у другу државу;
8. који правни механизам преноса постоји.

Правила о преносу података у треће државе захтевају посебан правни основ и одговарајуће гаранције. (Eur-Lex)

5.5. Безбедност обраде

Европски стандард обухвата:

- псеудонимизацију и шифровање;
- трајну поверљивост, интегритет, доступност и отпорност;
- благовремени опоравак;
- редовно тестирање мера. (Eur-Lex)

Нацрт не прописује ове мере за Евиденцију нити за електронску доставу.

5.6. Процена утицаја

За обраду која може створити висок ризик, посебно када се систематски обрађују безбедносно осетљиви организациони подаци, европски стандард предвиђа процену утицаја. GDPR такође предвиђа консултовање надзорног органа током припреме законодавних или регулаторних мера које се односе на обраду. (Eur-Lex)

Зато је пре усвајања оправдано:

- спровести процену утицаја;
- затражити мишљење Повереника;
- објавити бар неосетљиви сажетак процене.

Укупна оцена

Нацрт је **испод европског стандарда заштите података** док се не уреде:

- минимизација;
- сврхе;
- рокови;
- улоге;
- права лица;
- безбедност;
- спољни сервис;
- повреда података;
- процена утицаја.

---

6. Европски оквир електронске идентификације и услуга од поверења

6.1. Правни статус

Уредба eIDAS број 910/2014, измењена Уредбом (ЕУ) 2024/1183 о успостављању Европског оквира дигиталног идентитета, непосредно се примењује у ЕУ, али не представља непосредно применљив домаћи пропис у Србији. За Србију има значај:

- приступног мерила;
- стандарда интероперабилности;
- модела за електронски потпис, печат, временски жиг и регистровану електронску доставу. (Eur-Lex)

6.2. Релевантна правила

Европски оквир признаје:

- правно дејство електронског потписа;
- изједначавање квалификованог електронског потписа са својеручним потписом;
- претпоставку интегритета и порекла код квалификованог електронског печата;
- доказну вредност квалификованог временског жига;
- доказе слања и пријема код квалификоване електронске регистроване доставе;
- правно дејство електронског документа. (Eur-Lex)

6.3. Оцена Нацрта

Нацрт допушта електронске документе и оверене дигитализоване акте, што је у складу са европским правцем.

Ипак, не уређује:

- ниво електронског потписа;
- електронски печат правног лица;
- временски жиг;
- поуздану потврду пријема;
- доказ времена достављања;
- регистровану електронску доставу;
- проверу сертификата;
- дугорочно очување валидности потписа;
- доказни режим у случају спора.

Слање обичном електронском поштом не обезбеђује аутоматски доказ:

- идентитета пошиљаоца;
- интегритета прилога;
- тачног времена предаје;
- пријема од стране органа.

Оцена

Нацрт је **делимично усклађен у признавању електронског документа**, али је **испод стандарда поуздане и доказиве електронске трансакције**.

Препорука

Увести:

- заштићени портал;
- електронску идентификацију;
- електронски потпис или печат;
- временски жиг;
- аутоматску потврду;
- доказиви број предмета;
- електронско достављање решења.

7. Конвенција 108 и модернизовани стандарди 108+

7.1. Конвенција 108

Конвенција Савета Европе број 108 први је правно обавезујући међународни инструмент посебно посвећен заштити лица у односу на аутоматску обраду података. Република Србија је њена страна уговорница. (Portal)

Она захтева да обрада буде:

- правична и законита;
- заснована на одређеној и легитимној сврси;
- сразмерна;
- тачна;
- временски ограничена;
- безбедна.

Оцена Нацрта

Постојећи недостаци у погледу:

- адресе одговорног лица;
- сврхе;
- рокова чувања;
- спољног алата;
- права лица;
- безбедности комуникације

стварају ризик непотпуне усклађености са обавезујућим конвенцијским стандардом.

7.2. Протокол 108+

Србија је 26. маја 2020. године ратификовала Протокол CETS 223 којим се модернизује Конвенција 108. Међутим, према стању у јулу 2026. године, Протокол још није достигао потребан број ратификација за опште ступање на снагу; у мају 2026. забележена је 34. ратификација, док је потребно 38. (Portal)

Зато 108+ не треба представљати као већ оперативни измењени текст Конвенције за све стране. Ипак, ратификација Србије чини га снажним мерилом проактивног усклађивања.

Модернизовани стандард наглашава:

- одговорност руковаоца;
- транспарентност;
- процену ризика;
- privacy by design;
- безбедност;
- делотворна овлашћења надзорног органа;
- правила прекограничног преноса. (Portal)

Оцена

Нацрт је **испод модернизованог стандарда 108+** јер не садржи:

- процену ризика обраде;
- уграђену заштиту података;
- јасан ланац одговорности;
- потпуна правила преноса;
- документовану контролу спољног сервиса.

8. Европска конвенција о људским правима

8.1. Правни статус

Европска конвенција о људским правима правно обавезује Србију од 3. марта 2004. године. Члан 8. штити приватни и породични живот, дом и преписку. Мешање јавне власти мора бити:

1. засновано на закону;
2. усмерено ка легитимном циљу;
3. неопходно у демократском друштву;
4. сразмерно. (ECHR)

8.2. Примена на Нацрт

Прикупљање службених података одговорног лица може имати легитимну сврху. Међутим, формулација „адреса одговорног лица“ не задовољава у потпуности тест предвидивости јер није јасно да ли обухвата приватну адресу.

Јавна објава пуне физичке адресе ЦЕРТ-а може бити оправдана само ако је:

- стварно потребна за идентификацију и контакт;
- безбедносно процењена;
- ограничена на службену адресу;
- мање рестриктивна алтернатива недовољна.

Неограничено чување личних података такође би створило проблем сразмерности.

Оцена

Нацрт може остварити легитиман циљ сајбер-безбедности, али поједине мере нису довољно прецизне и сразмерне.

Потребне измене

- изричито искључити адресу пребивалишта;
- одредити рокове чувања;
- ограничити јавни део;
- обезбедити исправку и правну заштиту;
- документовати тест нужности за сваки јавни податак.

---

9. ENISA оквири

9.1. Правна природа

ENISA је агенција ЕУ за сајбер-безбедност. Њени приручници, модели и оквири нису сами по себи правно обавезујући прописи. Они представљају:

- стручно мерило;
- инструмент хармонизације;
- техничку подршку спровођењу NIS2;
- релевантну најбољу праксу.

9.2. ENISA CSIRT Maturity Framework

ENISA-ов оквир зрелости заснован је на SIM3, али разликује три нивоа:

- Basic;
- Intermediate;
- Advanced.

Оквир не своди потпуну процену само на самопроцену. ENISA наглашава значај самопроцене, али и peer review-а као суштинског елемента потпуније процене зрелости. (ENISA)

Поређење са Нацртом

Нацрт:

- преузима SIM3 самопроцену;
- не преузима ENISA нивое;
- не предвиђа peer review;
- не предвиђа независну проверу;
- не одређује минимални профил;
- не објашњава однос нивоа 2 према ENISA категоријама.

Оцена

SIM3 је примењен **селективно и непотпуно**. Самопроцена се фактички користи у статусном поступку, иако недостаје други ниво стручне провере који ENISA сматра значајним за пуну оцену.

9.3. ENISA и координисано откривање рањивости

ENISA развија смернице за националне политике координисаног откривања рањивости и подржава европску базу рањивости у оквиру NIS2. (ENISA)

Нацрт не уређује ову функцију, али би RFC профил требало да садржи:

- да ли ЦЕРТ прима пријаве рањивости;
- контакт;
- политику откривања;
- поступак координације;
- режим поверљивости.

---

10. Међународни CSIRT оквири

10.1. RFC 2350

Правна природа

RFC 2350, односно BCP 21, објављен је у јуну 1998. године као Internet Best Current Practice. Он није закон, међународни уговор или обавезујући технички пропис. Његова сврха је да одреди теме о којима CSIRT треба јасно да обавести своју корисничку заједницу. Сам документ изричито наводи да није могуће дефинисати један сет захтева погодан за све тимове. (RFC Editor)

Усклађеност Нацрта

Нацрт је у складу са основном сврхом RFC 2350 када захтева:

- јасан мандат;
- каталог услуга;
- контакт;
- методе безбедне комуникације;
- јавно доступан профил.

Међутим, RFC 2350:

- не прописује обавезан државни регистар;
- не прописује брисање;
- не захтева јавност свих интерних процедура;
- не представља сертификат;
- не утврђује минималну зрелост.

RFC посебно наглашава потребу за сигурним комуникационим каналима и заштитом информација које тимови размењују. (RFC Editor)

Оцена

Нацрт примењује RFC 2350 **селективно**:

- правилно преузима јавни опис тима;
- недовољно преузима захтев за безбедну комуникацију;
- ризикује прекомерну јавност;
- даје документу јаче правно дејство него што га он сам има.

10.2. SIM3

Правна природа

SIM3 је модел зрелости који одржава Open CSIRT Foundation. Користи се за:

- самопроцену;
- peer review;
- независне процене;
- професионалне поступке сертификације;
- развој тимова.

Он није:

- ISO стандард;
- пропис ЕУ;
- међународни уговор;
- универзално обавезујући услов рада ЦЕРТ-а.

ENISA користи SIM3 као основу свог оквира зрелости, што потврђује његову стручну релевантност, али му не даје правну снагу прописа. (ENISA)

Оцена Нацрта

Нацрт SIM3 примењује:

- обавезно;
- на све параметре;
- у поступку уписа;
- уз обавезне планове за параметре испод нивоа 2;
- уз накнадно ажурирање;
- уз могућу статусну последицу брисања.

То је строжи режим од обичне добровољне самопроцене.

Нацрт не одређује:

- верзију;
- датум;
- лиценцу;
- домаћи меродавни текст;
- параметре;
- критеријуме провере;
- право на стручну ревизију;
- однос према новом издању модела.

Оцена

SIM3 је примењен **стручно оправдано у принципу**, али **нормативно непотпуно и потенцијално динамички**.

10.3. FIRST CSIRT Services Framework

FIRST CSIRT Services Framework представља каталог могућих функција и услуга CSIRT тима. Сам оквир наглашава:

- да се не очекује да сваки тим пружа све наведене услуге;
- да избор услуга зависи од мандата и корисничке заједнице;
- да оквир сам не прописује ниво способности, капацитета, зрелости или квалитета. (FIRST)

Оцена Нацрта

Нацрт је у складу са FIRST Services Framework-ом када захтева каталог услуга.

Не би, међутим, било правилно из тога извести да:

- сваки посебан ЦЕРТ мора пружати исте услуге;
- постоји универзални минимални портфолио;
- упис доказује квалитет услуга;
- број услуга одређује зрелост.

Предлог

У RFC профилу треба омогућити да тим јасно наведе:

- услуге које пружа;
- услуге које не пружа;
- корисничку заједницу;
- ограничења;
- начин упућивања другом тиму.

---

11. FIRST услови за чланство

11.1. Стварни поступак

Актуелни поступак FIRST чланства не заснива се само на SIM3 самопроцени. Он укључује:

- формалну пријаву;
- SIM3 самопроцену;
- подршку два постојећа FIRST тима;
- проверу од стране спонзора;
- посету или одговарајућу непосредну проверу примарног спонзора;
- проверу организације, мандата, контаката и оперативног рада;
- одлучивање у оквиру FIRST поступка.

FIRST користи одређени основни скуп SIM3 параметара као део чланског поступка, а не прописује да сваки кандидат мора имати исти високи ниво у сваком параметру. (FIRST)

11.2. Поређење са Нацртом

FIRST	**Нацрт**
Добровољно чланство	Обавезни домаћи услов за упис
SIM3 као део шире провере	SIM3 као обавезни доказ
Спонзори и непосредна провера	Нема спонзора ни независне теренске провере
Основни профил параметара	План за сваки параметар испод нивоа 2

Професионална одлука организације	Управно решење државног регулаторног система

Оцена образложења

Тврдња да је SIM3 релевантан за FIRST чланство **у основи је тачна**.

Била би, међутим, непотпуна или обмањујућа ако се из ње закључи:

- да FIRST чланство зависи само од самопроцене;
- да FIRST захтева ниво 2 за сваки параметар;
- да домаћи упис представља еквивалент FIRST чланству;
- да FIRST правила стварају обавезу Србији.

---

12. Trusted Introducer

12.1. Структура система

Trusted Introducer не представља једноставан систем „чланства“. Он разликује више професионалних статуса и поступака, нарочито:

- листирање;
- акредитацију;
- сертификацију.

Поступак сертификације користи SIM3 и утврђује конкретне минималне нивое по параметрима, уз стручну проверу. Trusted Introducer сертификација није исто што и самопроцена. (Trusted Introducer)

Акредитација је посебан поступак стандардизоване провере тима и не треба је аутоматски изједначити са SIM3 сертификацијом. (Trusted Introducer)

12.2. Поређење

Trusted Introducer	**Нацрт**
Добровољни професионални режим	Домаћи регистарски услов
Различити статуси	Јединствени статус уписаног ЦЕРТ-а
Сертификација са профилом и провером	Самопроцена и административна провера конзистентности
Професионална оцена	Управно одлучивање
Посебни минимални профили	Општа обавеза плана испод нивоа 2
Периодична професионална провера	Ажурирање на неодређени захтев Националног ЦЕРТ-а

12.3. Оцена образложења

Ако образложење наводи да се SIM3 користи у систему Trusted Introducer, то је тачно.

Ако се, међутим, наводи или сугерише да је SIM3:

- универзални услов за „чланство у Trusted Introducer-у“;
- истоветан услов за листирање, акредитацију и сертификацију;
- правно обавезујући европски стандард;
- довољан доказ компетентности без независне провере,

такво представљање није прецизно.

Тачнија формулација била би:

> „SIM3 се користи као модел зрелости у појединим поступцима FIRST-a и Trusted Introducer-a, нарочито у поступку Trusted Introducer сертификације, при чему ти професионални поступци садрже и додатне елементе провере који нису истоветни самопроцени предвиђеној овим правилником.“

---

13. ISO/IEC стандарди

13.1. Правна природа

ISO/IEC стандарди су по правилу добровољни. Постају правно обавезујући само ако:

- пропис изричито на њих упути;
- буду преузети као обавезни технички услов;
- уговором буду прихваћени;
- представљају услов сертификације коју је субјект добровољно затражио.

За анализу су релевантни нарочито:

- **ISO/IEC 27001:2022** — систем управљања информационом безбедношћу; (ISO)
- **ISO/IEC 27035-1:2023** — принципи и процес управљања безбедносним инцидентима; (ISO)
- **ISO/IEC 27035-2:2023** — планирање, припрема и учење из инцидената; (ISO)
- **ISO/IEC 29147:2018** — откривање рањивости; (ISO)
- **ISO/IEC 30111:2019** — поступање са рањивостима; (ISO)

И NIS2 у својим уводним разматрањима упућује на стандарде ISO/IEC 30111 и ISO/IEC 29147 као релевантне смернице за координисано откривање и поступање са рањивостима. (Eur-Lex)

13.2. Однос са Нацртом

Нацрт је посредно усклађен са овим стандардима кроз:

- организациону процену;
- документовање услуга;
- планове унапређења;
- управљање инцидентима.

Ипак, не уређује:

- систем управљања ризиком;
- контролни оквир;
- циклус планирање–примена–провера–унапређење;
- доказе о тестирању;
- CVD процедуре;
- поступање са произвођачима;
- критеријуме затварања рањивости;
- безбедност доказне документације.

Оцена

Примена ISO/IEC стандарда у Нацрту је **само посредна и селективна**.

Не би било сразмерно да Правилник о Евиденцији свим посебним ЦЕРТ-овима наложи обавезну ISO сертификацију. Прикладније је:

- користити стандарде као упоредна мерила;
- преузети релевантне контролне циљеве;
- оставити избор начина доказивања;

- омогућити да сертификат буде један од могућих доказа, а не једини доказ.

---

14. Посебна оцена образложења SIM3–FIRST–Trusted Introducer

14.1. Шта је оправдано

Оправдано је навести да:

- SIM3 има широку професионалну примену;
- ENISA га користи као основу оквира зрелости;
- FIRST га користи у поступку пријема нових чланова;
- Trusted Introducer га користи у поступку сертификације;
- модел може допринети упоредивости и развоју тимова.

14.2. Шта није довољно прецизно

Није оправдано изједначити:

- SIM3 самопроцену и независни аудит;
- домаћи упис и FIRST чланство;
- домаћи упис и TI сертификацију;
- TI акредитацију и TI сертификацију;
- добровољни професионални услов и законску обавезу;
- употребу модела у пракси и правну обавезност модела.

14.3. Кључни доказни недостатак

Чињеница да професионална организација користи SIM3 не доказује сама по себи:

1. да је SIM3 једини погодан модел за домаћи систем;
2. да сваки посебан ЦЕРТ мора применити све параметре;
3. да сваки параметар испод нивоа 2 мора имати план унапређења;
4. да је рок од 15 дана сразмеран;
5. да недостављање треба да води брисању;
6. да је спољни онлајн алат неопходан;
7. да је модел правно доступан и стабилан за дугорочну нормативну примену.

14.4. Коначна оцена

Образложење је **стручно засновано у основном избору SIM3**, али је:

- правно непотпуно;
- упоредноправно поједностављено;
- терминолошки непрецизно у погледу Trusted Introducer статуса;
- недовољно за оправдање обавезног домаћег режима.

---

15. Предлози измена ради међународне и европске усклађености

1. Унети одредбу о правној природи стандарда

> „RFC 2350 и SIM3 представљају техничке и стручне референтне оквире. Њихова обавезна примена у поступку уписа заснива се искључиво на овом правилнику и

не представља FIRST чланство, Trusted Introducer акредитацију или сертификацију, нити независну потврду компетентности.“

2. Фиксирати SIM3 верзију

Навести:

- пун назив;
- верзију;
- датум;
- параметре;
- нивое;
- домаћи меродавни прилог.

Будућа измена модела не сме аутоматски мењати домаће обавезе.

3. Увести офлајн алтернативу

Резултат самопроцене мора се моћи доставити:

- у домаћем обрасцу;
- без обавезног чувања код спољног сервиса;
- уз проверљиву архивску копију.

4. Раздвојити самопроцену и стручну проверу

Нацрт мора јасно разликовати:

- самопроцену;
- административну проверу потпуности;
- проверу конзистентности;
- peer review;
- независни аудит;
- сертификацију.

5. Ускладити електронску доставу са eIDAS приступом

Увести:

- безбедан портал;
- електронску идентификацију;
- електронски потпис или печат;
- временски жиг;
- доказиви пријем;
- електронску доставу решења.

6. Спровести процену утицаја на заштиту података

Процена треба да обухвати:

- јавну адресу;
- контакте одговорног лица;
- SIM3;
- планове унапређења;
- спољни алат;
- логове;
- рокове чувања;
- прекограничне токове;
- повреду података.

7. Уредити нивое поверљивости

Прописати:

- јавни ниво;
- ниво за овлашћене ЦЕРТ-ове;
- ниво за Национални ЦЕРТ;
- строго ограничени ниво;
- агрегирано и анонимизовано објављивање.

8. Увести јавни RFC минимум и поверљиви анекс

Јавни профил треба да омогући корисницима да:

- идентификују тим;
- пријаве инцидент;
- разумеју услуге;
- провере мандат.

Оперативно осетљиви подаци морају бити издвојени.

9. Увести правила координисаног откривања рањивости

Најмање у RFC профилу треба одредити:

- да ли се пријаве примају;
- безбедни контакт;
- политику откривања;
- однос према Националном ЦЕРТ-у;
- заштиту поверљивости;
- поступање са анонимним пријавама.

10. Ускладити поступак брисања са европским стандардима владавине права

Брисање мора бити:

- законито;
- предвидиво;
- засновано на исцрпним разлозима;
- сразмерно;
- последња мера;
- донето образложеним решењем;
- подложно правном средству и судској контроли.

---

16. Закључна оцена

Споразум о стабилизацији и придруживању

Нацрт прати општи правац усклађивања у области информационог друштва и сајбер-безбедности, али не садржи довољну анализу правних тековина, трошкова, спровођења и заштите података.

Оцена: делимична усклађеност.

NIS2

Нацрт доприноси идентификацији и развоју ЦЕРТ-ова, али:

- не преноси NIS2 у целини;
- поједине NIS2 обавезе нису применљиве на све посебне ЦЕРТ-ове;
- SIM3 режим у појединим деловима иде изнад NIS2;

- безбедност комуникације и поверљивост остају испод стандарда.

Оцена: селективна усклађеност, без еквивалентности.

Заштита података и право на приватност

Нејасна адреса одговорног лица, непостојање рокова, неуређени спољни сервис и одсуство процене утицаја представљају значајне недостатке.

Оцена: испод европског и конвенцијског стандарда док се не унесу битне измене.

eIDAS

Признавање електронских докумената је позитивно, али електронска пошта без поузданог идентитета, интегритета, времена и потврде пријема није довољна.

Оцена: делимична усклађеност.

RFC 2350

Избор је стручно оправдан, али треба ограничити јавни садржај и обезбедити домаћи профил, превод, верзионирање и аутентичност.

Оцена: усклађен у циљу, селективан у примени.

SIM3

Избор је стручно релевантан, али модел није довољно правно идентификован и употребљен је са статусним последицама које професионални системи не заснивају само на самопроцени.

Оцена: стручно оправдан, правно непотпуно и прекомерно уграђен.

FIRST и Trusted Introducer

Образложење исправно препознаје њихову везу са SIM3, али не приказује:

- додатне механизме провере;
- различите профиле;
- добровољни карактер;
- разлике између чланства, листирања, акредитације и сертификације.

Оцена: делимично тачно, али материјално непотпуно и терминолошки непрецизно.

Коначни међународни и европски тест

Нацрт се може оценити као усклађен са међународним обавезама и европским правцем тек ако:

1. јасно раздвоји правно обавезујуће изворе од добровољних стандарда;
2. фиксира SIM3 верзију;
3. спречи аутоматско преузимање будућих измена;
4. уведе безбедну и доказиву електронску доставу;
5. спроведе процену утицаја на заштиту података;
6. ограничи јавност физичких и оперативних података;
7. уреди поверљивост, рокове и приступ;
8. разликује самопроцену од независне верификације;
9. уреди поступак брисања и правну заштиту;
10. исправи образложење односа SIM3–FIRST–Trusted Introducer.

Синтетичка оцена

Нацрт је усмерен ка европском моделу развоја CSIRT капацитета, али га не преузима потпуно и доследно. Правно обавезујући стандарди приватности, предвидивости и сразмерности нису у потпуности обезбеђени, док су добровољни професионални стандарди делимично претворени у обавезне домаће услове без довољне нормативне и ефектне анализе.

Зато је закључак:

Нацрт је прихватљив са становишта међународних обавеза и европских интеграција само уз битне измене.