

Име и презиме, односно назив организације и институције: Партнери за демократске промене Србија (Партнери Србија)

Контакт телефон: (+381 11) 32 31 551, (+381 11) 32 31 552

Е-пошта: office@partners-serbia.org

Назив закона на који упућујете предлоге, примедбе и сугестије: Нацрт закона о заштити података о личности

Датум: 9. 9. 2026.

1. Општи коментари и сугестије у односу на Нацрт закона као целину

Партнери Србија поздрављају одлуку да се, уместо парцијалних измена, приступи изради новог Закона о заштити података о личности, као и нормирању области које важећи Закон о заштити података о личности („Службени гласник РС”, бр. 87/18, у даљем тексту: ЗЗПЛ) није препознао. Посебно поздрављамо издвајање обраде коју надлежни органи врше у посебне сврхе у засебан део закона, уређивање видео надзора као целине, као и изричиту забрану даљинске, масовне и неселективне биометријске идентификације лица употребом система видео надзора у оквиру обраде у посебне сврхе.

Ипак, Нацрт Закона о заштити података о личности (у даљем тексту: Нацрт) садржи и решења која, по нашем мишљењу, могу довести до смањења достигнутог нивоа заштите у односу на важећи ЗЗПЛ, што отвара питање њихове усклађености са чланом 20. став 2. Устава Републике Србије, у вези са уставном заштитом података о личности из члана 42. Устава. Имајући у виду да је важећи ЗЗПЛ у великој мери заснован на стандардима Опште уредбе ЕУ о заштити података (GDPR) и Директиве (ЕУ) 2016/680, сматрамо да измене не би смеле да доведу до удаљавања од ових стандарда. Због тога указујемо на то да свако решење којим се сужава обим примене закона, ограничавају права лица или слаби правна заштита мора бити посебно образложено и засновано на тесту неопходности и сразмерности.

2. Конкретан део Нацрта закона чију измену предлагете и Ваш предлог за измену

Члан 3. – територијална примена Закона је неоправдано сужена Предлог за измену: Предлажемо да се задрже постојећи критеријуми понуде робе или услуга и праћења активности лица у Републици Србији, односно да се задржи одредба из важећег закона.
Члан 4. тач. 16 и 17 – појам ризика не сме се свести само на безбедност података Предлог за измену: Предлажемо да се појам ризика дефинише шире, тако да обухвати све могуће негативне последице обраде по права и слободе лица, док би нарушавање безбедности представљало само једну од врста ризика.
"Значајан јавни интерес" као основ за обраду осетљивих података (чл. 32. ст. 2. тач. 7) Предлог за измену: Предлажемо да се појам, или бар захтеви за пропис који уређује значајни јавни интерес, додатно прецизирају у тексту.
Члан 4. тачка 34 – посебан режим обраде не треба аутоматски ширити на све прекршаје Предлог за измену: Уколико постоји потреба да се поједине категорије прекршаја обухвате посебним режимом, закон би морао да их прецизно одреди и образложи зашто је такво проширење неопходно и сразмерно. Опште укључивање свих прекршаја сматрамо прешироким.
Чланови 39–41 – ограничења права код архивирања, истраживања и статистике су прешироко постављена Предлог за измену: Предлажемо да се круг права од којих је могуће одступити и услови за одступање прецизно ускладе са чланом 89. GDPR-а, а да се статусни услов из члана 40. став 2. преиспита и заштита права лица првенствено заснује на садржинским мерама заштите, нарочито минимизацији података, псеудонимизацији или анонимизацији када је то могуће, ограничењу приступа и рокова чувања, као и процени утицаја на заштиту података када обрада може представљати висок ризик по права и слободе физичких лица.
7. Члан 44. – обрада ради остваривања или одбране правног захтева не може бити изузета од осталих начела заштите података Предлог за измену: Предлажемо да се јасно пропише да се и на обраду ради остваривања или одбране правног захтева примењују сва начела из чл. 5–13. Нацрта, уз само она конкретна ограничења која су прописана законом и неопходна за вођење одређеног поступка.
8. Члан 48. – видео надзор запослених захтева строже гаранције, а изузеци за државне органе не могу бити општи Предлог за измену: Надзор рада запослених мора остати изузетна мера, за прецизно одређене сврхе и уз строго документован тест неопходности и сразмерности. Зато предлажемо да се изузеци за државне органе везују за конкретан заштићени интерес и конкретан случај, а не за саму категорију органа.
9. Чланови 52. и 53. – обрада података коришћењем вештачке интелигенције не оправдава опште ограничење права лица Предлог за измену: Предлажемо да се опште искључивање права из члана 52. став 4. брише, да се преиспита и ограничење из става 3, а да се у чл. 52. и 53. јасно потврди пуна примена општих правила ЗЗПЛ-а, уз додатне гаранције код високоризичних система, обраде података деце, биометријских и других посебно осетљивих података.
10. Чланови 159–161 – право на притужбу Поверенику је неоправдано сужено Предлог за измену: Предлажемо да се задржи опште право на притужбу због сваке повреде Закона, док претходно обраћање руковоцу може бити услов само када се притужба односи управо на непоступање по захтеву лица.
11. Члан 164. – потребно је ојачати улогу организација цивилног друштва у заштити од системских повреда Предлог за измену: Предвидети посебно право квалификоване организације да поступке из чл. 159, 160. и 163. Нацрта покрене и без појединачног овлашћења, у складу са могућношћу коју предвиђа члан 80. став 2. GDPR-а.

12. Члан 156. и чл. 166–168 – потребно је обезбедити делотворнији систем санкционисања повреда Закона

Предлог за измену: Предлажемо да се Поверенику, у оквиру корективних мера из члана 156. Нацрта, омогући да у управном поступку самостално изриче новчане мере за повреде Закона, уз обезбеђену судску контролу, и да се њихов износ одмерава тако да буде делотворан, сразмеран и одвраћајући, узимајући у обзир, између осталог, тежину повреде и економску снагу руковоца или обрађивача.

13. Чланови 172–175 – потребно је предвидети одложени почетак примене Закона

Предлог за измену: Предлажемо да се и у овом случају раздвоје ступање на снагу и почетак примене, како би се сви обвезници закона и релевантни актери упознали са новим одредбама, уз одговарајући период за доношење подзаконских аката, усклађивање других прописа и припрему руковалаца и надлежних институција.

3. Образложење упућеног предлога за измену Нацрта закона

2. Члан 3. – територијална примена Закона је неоправдано сужена

Важећи ЗЗПЛ примењује се и на руководе и обрађиваче који немају седиште у Републици Србији када су њихове радње обраде повезане са понудом робе или услуга лицима у Србији или са праћењем њихових активности у Србији. Нацрт ове критеријуме више не садржи, већ примену на стране руководе везује за то да се радње обраде врше „у оквиру активности на територији Републике Србије“.

Оваква формулација може значајно сузити примену Закона на стране дигиталне платформе и друге пружаоце услуга који немају пословно присуство у Србији, али своје услуге нуде грађанима Србије или прате њихово понашање. Иако Образложење уз Нацрт (стр. 4) наводи да се предложеном изменом заправо проширује поље примене Закона, језичко тумачење оваквог решења наводи управо на супротан закључак - оно односно одступа од члана 3. став 2. GDPR-а, али и од важећег ЗЗПЛ-а, те представља корак уназад у погледу практичне заштите грађана. Утисак је да се оваквим решењем законодавац одриче чак и могућности да домаћи органи успоставе надлежност над страним дигиталним платформама, које обрађују личне податке наших грађана у великом обиму. Тиме се грађани остављају готово без икакве заштите у ситуацијама када је њихово право на заштиту података о личности угрожено од стране великих технолошких компанија, као што је то случај са незаконитом обрадом података од стране компаније Meta за потребе развоја AI модела,¹ који и даље нема свој институционални исход.

Значај задржавања овакве територијалне примене посебно је видљив имајући у виду обим коришћења страних дигиталних платформи у Србији. Према подацима портала World Population Review, Facebook у Србији има око 4,8 милиона корисника², док Instagram има око 3,3 милиона корисника.³ Имајући у виду број грађана чији се подаци обрађују путем ових платформи, важно је да Закон недвосмислено обезбеди своју примену и надлежност Повереника и у односу на руководе који немају пословно присуство у Србији, али нуде услуге лицима у Србији или прате њихово понашање. Ово питање не би требало оставити даљем тумачењу опште формулације о активностима на територији Републике Србије, јер би такво решење стварало правну несигурност како за грађане, тако и за руководе и Повереника, а делотворност заштите права зависила би од тога како ће се домет Закона накнадно тумачити у појединачним случајевима. Подсећамо да од 2024. Године компанија Meta незаконито обрађује податке грађана Србије за потребе тренирања модела вештачке интелигенције, те да до данас грађани нису добили информације о овим активностима, нити су надлежни органи предузели адекватне мере за заштиту права корисника и корисница.⁴ Прецизно законско одређење је зато важно како би унапред било јасно у којим случајевима грађани могу да остваре права пред домаћим надзорним органом. Зато предлагемо да се задрже постојећи критеријуми понуде робе или услуга и праћења активности лица у Републици Србији, односно да се задржи одредба из важећег закона.

3. Члан 4. тач. 16 и 17 – појам ризика не сме се свести само на безбедност података

Нацрт дефинише „ризик“ као стварну могућност нарушавања безбедности података о личности, док се и „управљање ризицима безбедности података о личности“ ограничава на догађаје који могу утицати на безбедност података. Међутим, обрада података може произвести озбиљне последице по права и слободе лица и када није дошло до повреде безбедности – на пример дискриминацију, неоправдани надзор, профилисање, губитак контроле над подацима или ускраћивање одређених права.

¹ <https://www.otvorenavratapravosudja.rs teme/ostalo/nasi-podaci-u-rukama-ai-kako-meta-koristi-podatke-bez-naseg-pristanka>

² [Facebook Users by Country 2026](#)

³ [Instagram Users by Country 2026](#)

⁴ Према наводима Повереника, активности институције фокусиране су на успостављање контакта са представницима компаније Meta ([Активности Повереника у вези са неовлашћеном обрадом података о личности од стране компанија Meta и X Corp - Правни Портал](#)), али до данас није покренут ни један поступак у вези са овим случајем.

Оваква дефиниција није усклађена са приступом GDPR-а, који не садржи дефиницију самог ризика, али га посматра у односу на права и слободе физичких лица. Нацрт је у том погледу и интерно недоследан, јер чл. 67. и 78, који уређују обавезе руковођаца и безбедност обраде, такође говоре о ризику „за права и слободе физичких лица“. Зато предлагемо да се појам ризика дефинише шире, тако да обухвати све могуће негативне последице обраде по права и слободе лица, док би нарушавање безбедности представљало само једну од врста ризика.

4. "Значајан јавни интерес" као основ за обраду осетљивих података (чл. 32. ст. 2. тач. 7)

Формулација "остваривање значајног јавног интереса, одређеног законом" јесте дословно преузета из GDPR чл. 9(2)(g), али GDPR то препушта државама чланицама уз јасан захтев сразмерности и посебних мера заштите. У Србији је управо ова врста опште клаузуле коришћена за ширење овлашћења безбедносних органа без накнадне контроле, те предлагемо да се појам, или бар захтеви за пропис који уређује значајни јавни интерес, додатно прецизирају у тексту.

5. Члан 4. тачка 34 – посебан режим обраде не треба аутоматски ширити на све прекршаје

Нацрт у појам „надлежних органа“ укључује и органе надлежне за спречавање, истрагу и откривање прекршаја, чиме се посебан режим обраде проширује и на обраду података у вези са прекршајима. Није јасно због чега би сви прекршаји, без обзира на њихову природу и тежину, требало да буду обухваћени режимом који омогућава ширира ограничења права лица.

Директива (ЕУ) 2016/680 односи се на обраду коју надлежни органи врше у сврху спречавања, истраге, откривања или гоњења кривичних дела и извршења кривичних санкција, укључујући заштиту од претњи јавној безбедности и њихово спречавање. Појам „кривичног дела“ у смислу Директиве представља аутономан појам права ЕУ, из чега, међутим, не произлази да се сви прекршаји предвиђени домаћим правом могу аутоматски подвести под овај режим. Уколико постоји потреба да се поједине категорије прекршаја обухвате посебним режимом, закон би морао да их прецизно одреди и образложи зашто је такво проширење неопходно и сразмерно. Опште укључивање свих прекршаја сматрамо прешироким.

6. Чланови 39–41 – ограничења права код архивирања, истраживања и статистике су прешироко постављена

Нацрт предвиђа више одступања од права лица у случају обраде у сврхе архивирања, научног или историјског истраживања и статистике. Посебно је проблематичан члан 41. став 4, који код обраде у статистичке сврхе унапред искључује право на ограничење обраде, обавештавање у вези са исправком, брисањем или ограничењем, преносивост података, приговор и права у вези са аутоматизованим доношењем одлука. Члан 89. став 2. GDPR-а, међутим, за научна или историјска истраживања и статистичке сврхе допушта одступања само од права из чл. 15, 16, 18. и 21. GDPR-а, и то када би остваривање тих права вероватно онемогућило или озбиљно угрозило остваривање конкретне сврхе и када је одступање неопходно. Члан 39. став 5. Нацрта код архивирања укључује и одступање од права у вези са аутоматизованим доношењем одлука, иако члан 89. став 3. GDPR-а допушта одступања од права из чл. 15, 16, 18, 19, 20. и 21, али не и од члана 22. GDPR-а. Истовремено, члан 40. став 2. могућност прибављања података у сврхе научног или историјског истраживања условљава формалним статусом истраживача, односно научноистраживачке или високошколске установе и одлуком одговарајућег етичког одбора, чиме се могу неоправдано искључити организације цивилног друштва и независни истраживачи који спроводе методолошки утемељена истраживања од јавног интереса.

Члан 89. став 1. GDPR-а захтева да обрада у ове сврхе буде праћена одговарајућим техничким и организационим мерама, нарочито мерама које обезбеђују поштовање начела минимизације података, укључујући псеудонимизацију када је то могуће. Предлагемо да се круг права од којих је могуће одступити и услови за одступање прецизно ускладе са чланом 89. GDPR-а, а да се статусни услов из члана 40. став 2. преиспита и заштита права лица првенствено заснује на садржинским мерама заштите, нарочито минимизацији података, псеудонимизацији или анонимизацији када је то могуће, ограничењу приступа и рокова чувања, као и процени утицаја на заштиту података када обрада може представљати висок ризик по права и слободе физичких лица.

7. Члан 44. – обрада ради остваривања или одбране правног захтева не може бити изузета од осталих начела заштите података

Члан 44. прописује да се на обраду података која је неопходна ради подношења, остваривања или одбране правног захтева примењују процесни прописи, уз примену одредаба овог закона које се односе на заштиту права у случају повреде начела минимизације. Оваква формулација може се тумачити тако да се на ову обраду не примењују друга основна начела, попут законитости, ограничења сврхе, тачности, ограничења чувања и интегритета и поверљивости.

Потреба за подношењем, остваривањем или одбраном правног захтева може бити релевантна за законитост конкретне обраде и представља основ за поједине изузетке у односу на права лица, али не искључује примену основних начела заштите података нити потребу за одговарајућим правним основом обраде. Зато предлагемо да се јасно пропише да се и на обраду ради остваривања или одбране правног захтева примењују сва начела из чл. 5–13. Нацрта, уз само она конкретна ограничења која су прописана законом и неопходна за вођење одређеног поступка.

8. Члан 48. – видео надзор запослених захтева строже гаранције, а изузеци за државне органе не могу бити општи

Члан 48. став 7. допушта коришћење видео надзора у сврху праћења рада запослених када интереси из става 1. или „други јавни интереси утврђени законом“ претегну над правима и слободама запослених. Имајући у виду изразиту неравнотежу моћи у радном односу, сматрамо да је овакав стандард прешироки и да надзор рада запослених мора остати изузетна мера, за прецизно одређене сврхе и уз строго документован тест неопходности и сразмерности.

Додатно, став 8. за широк круг државних органа искључује примену ст. 3–6. овог члана, односно обавезу да се у одлуци документују разлози за увођење надзора и разматране мање инвазивне мере, обавештавање репрезентативног синдиката и претходно писано информисање запослених. Иако обавеза из става 2. да се размотре други механизми формално остаје, изостанак обавезе да се таква процена документује значајно отежава контролу неопходности и сразмерности надзора. Члан 88. став 2. GDPR-а захтева да правила која државе чланице доносе на основу става 1. тог члана садрже посебне мере заштите људског достојанства, легитимних интереса и основних права запослених, нарочито у вези са системима надзора на радном месту. Зато предлагемо да се изузеци за државне органе везују за конкретан заштићени интерес и конкретан случај, а не за саму категорију органа.

9. Чланови 52. и 53. – обрада података коришћењем вештачке интелигенције не оправдава опште ограничење права лица

Посебно проблематичним сматрамо решења из члана 52. Став 1. може се разумети као широка дозвола да се постојећи подаци користе за развој и тестирање система вештачке интелигенције када се нова сврха сматра усклађеном са првобитном, односно „у изузетним случајевима“ на основу легитимног интереса. Истовремено, став 3. допушта ограничење права на приступ и приговор ако би њихово остваривање значајно отежало остваривање сврхе обраде, али и ако руковалац не може да идентификује лице, док став 4. унапред искључује права на исправку, ограничење, брисање, преносивост и заштиту у вези са аутоматизованим доношењем одлука.

Сама сврха развоја, тренирања или тестирања система вештачке интелигенције не представља самосталан правни основ за обраду нити може сама по себи оправдати ограничење права лица. Уредба (ЕУ) 2024/1689 (AI Act) у члану 2. став 7. изричито потврђује да се прописи ЕУ о заштити података примењују на обраду података у вези са правима и обавезама из те уредбе. Ограничења права из GDPR-а могу се прописати само под условима из члана 23. GDPR-а, уз поштовање суштине основних права и принципа неопходности и сразмерности. Такође, европска пракса (мишљења Европског одбора за заштиту података о AI тренинг подацима⁵) инсистира на строгој,

⁵ European Data Protection Board (EDPB), *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, усвојено 17. децембра 2024.

документованој тест-процени пре почетка обраде, док Нацрт ту проверу не везује обавезно за претходну процену утицаја на заштиту података, нити за мишљење Повереника. Зато предлагемо да се опште искључивање права из члана 52. став 4. брише, да се преиспита и ограничење из става 3, а да се у чл. 52. и 53. јасно потврди пуна примена општих правила ЗЗПЛ-а, уз додатне гаранције код високоризичних система, обраде података деце, биометријских и других посебно осетљивих података.

Додатно, члан 53. користи појмове „систем вештачке интелигенције“, „модел опште намене“, „високоризични систем вештачке интелигенције“ и „систем са минималним ризиком“, које Нацрт не дефинише. Код високоризичних система одредба се додатно позива на процену утицаја на основна људска права и слободе „у складу са посебним законом“, без прецизирања тог нормативног оквира. Сматрамо да овакво решење не обезбеђује довољну правну предвидљивост у погледу тога на које системе се поједине обавезе примењују и под којим условима.

10. Чланови 159–161 – право на притужбу Поверенику је неоправдано сужено

Члан 159. везује право на притужбу Поверенику само за случај у којем руковалац није правилно поступио по претходном захтеву лица за остваривање права, уз обавезу достављања копије тог захтева. Друге повреде Закона – на пример обрада без правног основа, прекомерно прикупљање, незаконит пренос или системски надзор – пребацују се у режим „представке“ из члана 161.

Овакво решење представља значајну промену у односу на важећи члан 82. ЗЗПЛ-а и члан 77. став 1. GDPR-а, према којима лице има право да поднесе притужбу надзорном органу када сматра да обрада његових података није у складу са прописима. Члан 78. став 2. GDPR-а додатно гарантује делотворан судски правни лек када надзорни орган не поступи по притужби или у року од три месеца не обавести лице о току или исходу поступка. Зато предлагемо да се задржи опште право на притужбу због сваке повреде Закона, док претходно обраћање руковаоцу може бити услов само када се притужба односи управо на непоступање по захтеву лица.

11. Члан 164. – потребно је ојачати улогу организација цивилног друштва у заштити од системских повреда

Поздрављамо решење којим се лицу омогућава да овласти непрофитну организацију или удружење које се бави заштитом права и слобода да га без накнаде заступа у поступцима пред Повереником и судом. Ипак, када је реч о остваривању правних средстава из чл. 159, 160. и 163. Нацрта, организација може поступати у име лица само на основу његовог овлашћења, док Нацрт не предвиђа посебно право квалификоване организације да ове поступке покрене без појединачног овлашћења.

Код масовних, системских и технолошки сложених обрада повреду често није могуће ефикасно открити и доказати искључиво на нивоу једног лица. Члан 80. став 2. GDPR-а државама чланицама оставља могућност да непрофитним организацијама које испуњавају услове из става 1. тог члана омогуће да, и без појединачног овлашћења, покрену одређене поступке када сматрају да су права лица повређена обрадом.

12. Члан 156. и чл. 166–168 – потребно је обезбедити делотворнији систем санкционисања повреда Закона

Поздрављамо то што Нацрт повећава минималне новчане казне, проширује круг санкционисаних повреда и предвиђа петогодишњи рок за покретање и вођење прекршајног поступка. Међутим, основни модел санкционисања остаје непромењен: Повереник може непосредно изрећи новчану казну само издавањем прекршајног налога за прекршаје за које је прописана казна у фиксном износу, док се за остале повреде и даље ослања на прекршајни поступак пред судом. Основни

распон казне за правна лица из члана 167. став 1. износи од 200.000 до 2.000.000 динара, уз могућност изрицања више казне у случајевима из става 2, али овакав систем, нарочито у односу на велике привредне субјекте и међународне технолошке компаније, и даље не гарантује да ће санкција имати стварни одвраћајући ефекат. Досадашња пракса од 2019. године показује да ни јавни ни приватни сектор немају стварну мотивацију за доследно поштовање закона, а поступци пред прекршајним судовима су спори и често се окончавају застарелошћу.

Потреба за другачијим моделом већ је препозната у Стратегији заштите података о личности за период 2023–2030. године, у оквиру мере 5.1.1, где се као релевантан домаћи модел наводи Комисија за заштиту конкуренције и могућност изрицања управних мера у облику обавезе плаћања новчаног износа, управо ради веће ефективности надзора над применом ЗЗПЛ-а. Нацрт ову стратешку опредељеност не спроводи. То одступа и од основног модела GDPR-а, према којем надзорни орган има овлашћење да изрекне административну новчану казну, самостално или заједно са другим корективним мерама, при чему санкција мора бити делотворна, сразмерна и одвраћајућа. Зато предлажемо да се Поверенику омогући непосредно изрицање управних новчаних мера, уз јасне критеријуме за њихово одмеравање и судску контролу, као и да се приликом одређивања њиховог максималног износа узме у обзир економска снага руковоца, како санкција за велике субјекте не би представљала занемарљив трошак пословања.

13. Чланови 172–175 – потребно је предвидети одложени почетак примене Закона

Нацрт предвиђа да нови закон ступи на снагу осмог дана од објављивања и да истог дана престане да важи важећи ЗЗПЛ, док је за доношење подзаконских аката предвиђен рок од девет месеци, а за усклађивање других закона рок од годину дана. То значи да би нови режим почео да се примењује у периоду у којем његов нормативни оквир још није комплетан и у којем велики број секторских прописа може остати неусаглашен.

Такво решење ствара ризик правне несигурности и неуједначене праксе руковалаца, Повереника и судова. Посебно указујемо да је важећи ЗЗПЛ из 2018. године предвидео деветомесечни период до почетка примене, који свакако није био довољан за све неопходне припремне радње. Зато предлажемо да се и у овом случају раздвоје ступање на снагу и почетак примене, како би се сви обвезници закона и релевантни актери упознали са новим одредбама, уз одговарајући период за доношење подзаконских аката, усклађивање других прописа и припрему руковалаца и надлежних институција.