

10. септембар 2026. године

Г. Ненад Вујић
Министар правде
Министарство правде Републике Србије
Немањина 22-26, 11000 Београд, Република Србија

Копија: Повереник за информације од јавног значаја и заштиту података о личности
Министарство науке, технолошког развоја и иновација

**Предмет: Коментари АСТ-а на Нацрт закона о заштити података о личности (јавна
расправа од 30. јула до 10. септембра 2026. године)**

Association for Competitive Technology (ACT) захваљује на прилици да достави коментаре на Нацрт закона о заштити података о личности (у даљем тексту: Нацрт закона), који је Министарство правде објавило ради спровођења јавне расправе,¹ и ове коментаре достављамо на адресу konsultacije@mpravde.gov.rs. Похваљујемо Министарство што је приступило свеобухватној ревизији Закона о заштити података о личности из 2018. године,² што је Нацрт закона засновало на појмовима Опште уредбе ЕУ о заштити података (GDPR)³ које српска привреда и њени страни партнери већ примењују, што је стандардне уговорне клаузуле проширило на сва четири односа у којима се подаци преносе, што је увело структурисан тест за обраду у друге сврхе (члан 31) и што није усвојило новчане казне изражене као проценат укупног светског промета. Ова решења су у складу са приступом који АСТ препоручује владама широм света, а циљ наших препорука у наставку је да помогну да Нацрт закона оствари своје циљеве без повећања трошкова усклађивања за мала предузећа која у Србији развијају и продају софтвер или га из иностранства продају корисницима у Србији.

I. Увод и изјава о интересу

АСТ је непрофитно глобално пословно удружење које представља глобалну заједницу малих предузећа која развијају технологију. Наше чланице су предузетници, независни програмери и мала предузећа која развијају софтверске апликације и повезане уређаје које потрошачи и привреда користе у готово свим секторима привреде, укључујући здравство, образовање, финансијске услуге и јавне услуге, а многе од њих послују у Србији или из иностранства пружају услуге корисницима у Србији. Мали програмери зависе од јасних правила, предвидиве примене прописа и могућности да преносе податке преко граница како би

¹ Министарство правде Републике Србије, јавна расправа о Нацрту закона о заштити података о личности (од 30. јула до 10. септембра 2026. године), <https://mpravde.gov.rs/javne-rasprave>; в. и Paragraf, Rasprava će trajati do 10. septembra 2026. godine, <https://www.paragraf.rs/dnevne-vesti/310726/310726-vest8.html>. Текст Нацрта закона доступан је на <https://www.paragraf.rs/dnevne-vesti/310726/310726-vest13.html>, а упућивања на чланове у овим коментарима односе се на тај текст.

² Закон о заштити података о личности („Службени гласник РС“, број 87/18).

³ Уредба (ЕУ) 2016/679 (Општа уредба о заштити података), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

дошли до корисника и користили услуге рачунарства у облаку, а уједно су и предузећа која најтеже могу да поднесу трошкове усклађивања који нису сразмерни стварним ризицима или да одржавају један скуп пракси за Србију, а други за Европску унију.

Наше конкретне коментаре изложили смо редоследом одредби Нацрта закона, а пре њих дајемо преглед наших препорука и општих начела која АСТ примењује на прописе о заштити података у свим јурисдикцијама.

II. Преглед препорука

Ради лакшег обједињавања ставова учесника у јавној расправи, наше главне препоруке наводимо у наставку, а свака од њих је детаљније образложена у деловима који следе.

1. Ограничити део Нацрта закона о вештачкој интелигенцији (ВИ) на правни основ за коришћење података о личности ради развоја и рада система ВИ и на начин на који се права лица примењују на обучене моделе, а свако питање класификације система ВИ и обавеза обавештавања или означавања препустити посебном поступку који се односи на вештачку интелигенцију, у коме би најпре требало утврдити како се постојећи прописи већ примењују (чл. 52-53).
2. Признати легитимни интерес као редован правни основ за развој и рад система ВИ, уз исти тест одмеравања интереса који се према члану 20. примењује на другу обраду, уместо као основ који је доступан само у изузетним случајевима, и дозволити успутну обраду посебно осетљивих података о личности у скуповима података за обуку када програмер предузима разумне мере да их избегне и уклони (члан 32. и члан 52. став 1).
3. Задржати признање из члана 52. да се одређена права не могу на уобичајен начин применити на обучене моделе, технички основ овог решења објаснити у образложењу и прецизирати да се обавеза брисања по остварењу сврхе односи на податке за обуку, а не на сам модел (члан 52. ст. 3-5).
4. За обраду помоћу ВИ примењивати општа правила о процени утицаја и претходном мишљењу Повереника уместо захтева да Повереник даје мишљење о сваком високоризичном систему, а обавезе обавештавања о интеракцији са ВИ и означавања уклонити из Нацрта закона или их, ако се задрже, распоредити према улози учесника, уз изузетке који постоје у упоредивим прописима (члан 53).
5. За одлуке засноване искључиво на аутоматизованој обради примењивати само члан 62, без обзира на то да ли се користи ВИ, и у складу са тим ограничити члан 53. ст. 4-5 (чл. 53. и 62).
6. Из дефиниције легитимног интереса уклонити услов претходно успостављеног односа и у дефиницију профилисања вратити реч „аутоматизоване“, тако да оба појма прате GDPR (члан 4).
7. Територијално важење закона за стране руковооце одредити према критеријумима из Закона из 2018. године и GDPR-а, односно према понуди робе или услуга лицима у Србији или праћењу њиховог понашања, и задржати изузетак од обавезе именовања представника за повремену обраду ниског ризика (члан 3. и одредбе о представнику).

8. Прецизирати да апликација која се ослања на биометријску аутентификацију уграђену у уређај, и која никада не прима биометријске податке, не обрађује биометријске податке, као и да ПИН или лозинка испуњавају обавезу нуђења алтернативе (члан 32).
9. Прецизирати да испоручиоци камера, софтвера и складишног простора које корисници користе за сопствени видео надзор нису руковођаи тог видео надзора (чл. 45-51).
10. Омогућити да се захтев за српске стандардне уговорне клаузуле испуни коришћењем клаузула Европске комисије уз кратак српски додатак и признати одлуке о примереном нивоу заштите, обавезујућа пословна правила и сертификате признате у другим поузданим системима (чл. 103-108).
11. Усвојити праг заснован на ризику за обавештавање Повереника о повреди података о личности, обавезати Повереника да објави листе и обрасце за процену утицаја усклађене са онима који се користе у ЕУ и објавити методологију за израчунавање нових сразмерних новчаних казни.
12. Предвидети прелазни период од најмање 18 месеци пре почетка примене материјалних обавеза, при чему би примена одредби о ВИ била повезана са законом о ВИ, а инструменти за пренос који су већ у употреби остали би на снази.

III. Општи ставови АСТ-а о заштити података

АСТ подржава снажну и примењиву заштиту приватности, јер мали програмери које представљамо могу да успеју само ако им корисници поверавају своје податке о личности. Предлажемо да Министарство Нацрт закона провери у односу на следећа начела, која АСТ примењује на прописе о заштити података у свим јурисдикцијама.

- **Интероперабилност.** Србија је кандидат за чланство у Европској унији, а многа српска предузећа послују са корисницима у ЕУ, па практична вредност Нацрта закона зависи од тога колико доследно прати GDPR и правац реформи у ЕУ. Тамо где се дефиниције или правни основи разликују, мала предузећа морају да воде одвојене програме усклађивања за тесно повезана тржишта, што је трошак који велика предузећа могу да поднесу, а мала не могу.
- **Обавезе засноване на ризику и прилагођене величини.** Обавезе би требало да буду сразмерне ризику обраде и величини организације, а обавезе вођења документације, процене и обавештавања требало би усмерити на случајеве у којима је настанак штете вероватан.
- **Поуздани токови података.** Мали програмери се ослањају на услуге рачунарства у облаку и међународне партнере и не могу себи да приуште удвостручавање складиштења и обраде на сваком тржишту на коме стекну корисника, па их захтеви за локализацију података најтеже погађају, а пропис о заштити података требало би да понуди више законитих основа за прекогранични пренос.⁴ Поздрављамо то што Нацрт закона не прописује локализацију и предлажемо Министарству да такво решење задржи.

⁴ B. ACT, Digital Trade for Small Tech, <https://actonline.org/wp-content/uploads/Digital-Trade.pdf>.

- **Јасна правила за податке који се користе у ВИ.** Прописи о заштити података требало би да штите податке о личности, а да притом не стварају непотребне препреке прикупљању и обради података од којих зависи развој ВИ, уз примену разумних захтева у погледу минимизације података, пристанка и права потрошача и уз јасне смернице програмерима о правним основима на које се могу ослонити, укључујући легитимни интерес.⁵
- **Одговорност према улози.** Обавезе би требало да сноси онај учесник који је стварно у стању да их испуни, па мало предузеће које развија апликацију на моделу или платформи другог испоручиоца не би требало да преузме обавезе које само тај испоручилац може да испуни.⁶
- **Предвидива примена и довољно времена за усклађивање.** Мала предузећа се најбоље усклађују када су смернице, стандардне клаузуле и обрасци доступни пре почетка примене обавеза и када надзорни органи за прве, ненамерне грешке учињене у доброј вери користе корективне мере.

IV. Конкретни коментари АСТ-а на Нацрт закона

1. Обим одредби о ВИ (чл. 52-53)

Нацрт закона уводи одељак о обради заснованој на вештачкој интелигенцији, у коме се разликују високоризични системи, системи који непосредно комуницирају са физичким лицима и системи минималног ризика, и прописује означавање синтетичког аудио и видео садржаја. Истовремено, радна група при Министарству науке, технолошког развоја и иновација припрема посебан Закон о вештачкој интелигенцији са сопственим категоријама ризика и обавезама транспарентности.⁷ Ако два закона класификују исте системе према ризику, са различитим дефиницијама и под надзором различитих органа, програмери неће знати која се класификација примењује и можда ће морати да исти производ процењују два пута.

Велики део питања којима се баве чланови 52. и 53. већ је уређен општим одредбама Нацрта закона, које се на податке о личности које обрађује систем ВИ примењују на исти начин као и на сваку другу обраду, укључујући правила о правним основима, процени утицаја и аутоматизованом доношењу одлука. Стога предлагемо Министарству да одељак о ВИ ограничи на питања која су специфична за заштиту података и на која програмерима треба одговор, а то су правни основ за коришћење података о личности ради развоја и рада система ВИ и начин на који се права лица примењују на обучене моделе, и да из Нацрта закона уклони класификацију система

⁵ B. ACT, Policy Principles for Artificial Intelligence (16. новембар 2023), <https://actonline.org/wp-content/uploads/2023-11-16-ACT-AI-Policy-Principles-FINAL.pdf>; ACT, Digital Omnibus, <https://actonline.org/digital-omnibus/>.

⁶ B. ACT, AI Roles & Interdependency Framework, прилог уз Comments of ACT on the Development of an Artificial Intelligence Action Plan (14. март 2025), <https://actonline.org/wp-content/uploads/ACT-Comment-re-AI-Action-Plan-14-Mar-2025-w-appendix.pdf>.

⁷ NALED, Srbija dobija Zakon o veštačkoj inteligenciji – Balans između inovacija i odgovornosti (11. јун 2026), <https://naled.rs/vest-srbija-dobija-zakon-o-vestackoj-inteligenciji-balans-izmedju-inovacija-i-odgovornosti-12196>.

ВИ, обавезе обавештавања о интеракцији и захтев за означавање. Питање да ли су Србији уопште потребне такве обавезе специфичне за ВИ требало би размотрити у посебном поступку који се односи на вештачку интелигенцију, који би требало да почне утврђивањем начина на који се прописи о заштити потрошача, безбедности производа, заштити података и други постојећи прописи већ примењују на поступање о коме је реч.⁸

2. Правни основ и права лица у развоју ВИ (члан 52)

Чланом 52. став 1. дозвољава се обрада ради развоја, тестирања и примене система ВИ када је у складу са првобитном сврхом прикупљања и, изузетно, на основу легитимног интереса руковоаца или треће стране који претеже над правима и слободама лица на која се подаци односе. Према нашем тумачењу, тиме се обрће редовни тест из члана 20, према коме је обрада законита осим ако интереси или основна права лица на које се подаци односе не претежу над интересом руковоаца, па би се на легитимни интерес било теже ослонити код ВИ него код било које друге врсте обраде. Европски одбор за заштиту података (EDPB) закључио је да легитимни интерес може бити правни основ за развој и примену модела ВИ када руковалац утврди легитимни интерес, покаже да је обрада неопходна за његово остваривање и спроведе тест одмеравања интереса којим се узимају у обзир разумна очекивања лица на која се подаци односе и примењене заштитне мере,⁹ а предлогом Европске комисије познатим као Digital Omnibus у самом GDPR-у би се потврдило да се руковоаци могу ослонити на легитимни интерес како би обрађивали податке о личности ради развоја и рада система ВИ, уз заштитне мере,¹⁰ што су EDPB и Европски супервизор за заштиту података (EDPS) оценили као непотребну измену јер GDPR то већ дозвољава.¹¹

Предлажемо Министарству да члан 52. став 1. усклади са тим приступом тако што ће брисати реч „изузетно“ и услов да интерес претеже над правима лица на која се подаци односе и применити редовни тест из члана 20, заједно са заштитним мерама које су већ наведене у члану 52. став 2, као што су псеудонимизација и минимизација података. Ова разлика је важна за мале програмере јер је пристанак ретко изводљив када су подаци за обуку прикупљени из много извора, а програмер који се на легитимни интерес може ослонити у ЕУ, али не и у Србији, вероватно ће развојне активности обављати негде другде. Из истог разлога предлажемо Министарству да

⁸ ACT, Policy Principles for Artificial Intelligence, нав. у фусноти 5 (препурука да доносиоци прописа утврде како се постојећи прописи већ примењују пре него што усвоје правила специфична за ВИ).

⁹ Европски одбор за заштиту података, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (децембар 2024), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.

¹⁰ Европска комисија, Предлог уредбе о измени, између осталог, Уредбе (ЕУ) 2016/679 (Digital Omnibus), COM(2025) 837 final (19. новембар 2025), предложени члан 88с и измене чл. 33. и 35. В. Европски парламент, Legislative Train Schedule, The Digital Omnibus Regulation Proposal, <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-digital-package>.

¹¹ EDPB-EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) (фебруар 2026), https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en.

уреди питање посебно осетљивих података о личности који се успутно нађу у великим скуповима података за обуку упркос напорима програмера да их искључи, тако што ће дозволити њихову обраду када програмер предузима одговарајуће мере да избегне прикупљање таквих података, уклања их чим их идентификује, осим ако би уклањање захтевало несразмеран напор, и на други начин спречава да се они користе у резултатима модела, што је приступ који је Европска комисија предложила у оквиру предлога Digital Omnibus и са којим су се EDPB и EDPS делимично сложили.¹² Без такве одредбе, општа забрана из члана 32. могла би знатно да отежа обуку модела на великим и разноврсним скуповима података који су потребни многим апликацијама.

Чланом 52. став 4. прописује се да се право на исправку, брисање, ограничење обраде и преносивост, као и заштита у вези са аутоматизованим доношењем одлука, не примењују на обраду засновану на ВИ, а чланом 52. став 3. дозвољава се одбијање захтева за приступ и приговора када би они знатно отежали остваривање сврхе обраде. Подржавамо то што Министарство препознаје да се подаци о личности често не могу издвојити и уклонити из обученог модела и да се права осмишљена за записе у бази података не могу увек на исти начин применити на параметре модела, што потврђује и став EDPB-а да модел обучен на подацима о личности може и сам бити анониман када је вероватноћа издвајања података о личности из њега занемарљива.¹³ Будући да ће одредба ове врсте вероватно бити предмет пажљивог преиспитивања, предлагемо Министарству да је задржи, да њен технички основ објасни у образложењу и да потврди да руковооци и даље могу да одговоре на захтеве практичним мерама, као што су искључивање података из будуће обуке или филтрирање резултата, када су у могућности да то учине. Заштита у вези са одлукама заснованим искључиво на аутоматизованој обради другачије је природе, јер се односи на одлуке донете о лицу, а не на модел, па предлагемо Министарству да ту заштиту препусти члану 62, који се примењује без обзира на то да ли се користи ВИ, како објашњавамо у делу 3.

Чланом 52. став 5. прописује се да се подаци о личности бришу када се оствари сврха обраде засноване на ВИ. Предлагемо Министарству да прецизира да се ова обавеза односи на скупове података за обуку, валидацију и тестирање, а не на обучени модел, да дозволи руковооцима да чувају податке онолико дуго колико је потребно за документовање, ревизију и праћење тачности система и штетне пристрасности, и да у члану 31. потврди да је обрада у друге сврхе ради тестирања, евалуације и обезбеђивања система ВИ, укључујући тестирање на пристрасност, у складу са сврхом због које су подаци прикупљени.

3. Категорије ризика ВИ, транспарентност и аутоматизовано доношење одлука (чл. 53. и 62)

Чланом 53. став 1. прописује се процена утицаја за сваки високоризични систем ВИ и предвиђа да се о свакој таквој процени прибавља мишљење Повереника. Општа правила Нацрта закона већ прописују процену утицаја за обраду која ће вероватно

¹² Предлог Digital Omnibus, нав. у фусноти 10, предложени члан 9. став 2. тачка к) и став 5; EDPB-EDPS Joint Opinion 2/2026, нав. у фусноти 11.

¹³ EDPB Opinion 28/2024, нав. у фусноти 9.

проузроковати висок ризик, без обзира на то да ли се користи ВИ, а претходно мишљење Повереника предвиђају само за случајеве у којима процена покаже висок преостали ризик који руковалац не може да умањи (члан 85). Посебан захтев специфичан за ВИ створио би ред чекања за сваку примену која се сврстава у високоризичне, укључујући и примену добро познатих алата од стране малих предузећа, и одвукао би ресурсе Повереника од случајева којима су ти ресурси заиста потребни. Предлажемо Министарству да брише посебан захтев за процену и мишљење у вези са ВИ и да се ослони на општа правила из чл. 84-87, као и да пропише да ће Повереник приликом оцене организационих мера описаних у процени утицаја узети у обзир то што је руковалац применио стандард ISO/IEC 42001,¹⁴ како сертифицировано предузеће не би морало два пута да документује исте праксе.

Чланом 53. ст. 2, 3. и 6. руковаоцима би се прописала обавеза да физичка лица обавесте када су у интеракцији са системом ВИ и да означе синтетички аудио и видео садржај. Ове обавезе се примењују без обзира на то да ли се обрађују подаци о личности, а обавезе транспарентности ове врсте требало би да следе доказе о околностима у којима оне заиста помажу да се одговори на неки ризик,¹⁵ па предлажемо Министарству да их уклони из Нацрта закона из разлога наведених у делу 1. Ако Министарство ипак одлучи да их задржи, предлажемо да их распореди према улози учесника, тако да мали програмер који развија апликацију на моделу опште намене буде одговоран да сопствене кориснике обавести да комуницирају са ВИ, док би пружалац модела био одговоран за евентуално означавање резултата модела, и да уклони обавезу обавештавања за моделе ВИ опште намене, који сами не комуницирају са физичким лицима. У том случају предлажемо и да Министарство пропише изузетке за ситуације у којима је употреба ВИ очигледна из контекста, за системе који обављају помоћну функцију уређивања или суштински не мењају улазне податке и за очигледно уметничка, сатирична или фиктивна дела, да прихвати машински читљиво означавање засновано на отвореним техничким стандардима за утврђивање порекла садржаја уместо видљиве ознаке на сваком резултату и да сваку обавезу означавања ограничи на садржај који би могао да доведе у заблуду разумно лице у погледу своје аутентичности. Свако од ових ограничења постоји у члану 50. Акта о вештачкој интелигенцији ЕУ,¹⁶ а српско правило без њих било би строже од правила саме ЕУ.

Члан 53. став 4. другим речима понавља правило из члана 62. о одлукама заснованим искључиво на аутоматизованој обради које производе правне последице или на сличан начин значајно утичу на лице, а изгледа да члан 53. став 5. дозвољава потпуно аутоматизовану обраду помоћу ВИ само у статистичке, научне или историјске сврхе. Ако би се члан 53. став 5. тумачио тако да обухвата сваку потпуно аутоматизовану обраду, а не само такве одлуке, њиме би се забраниле рутинске функције као што су

¹⁴ ISO/IEC 42001:2023, Artificial intelligence management systems, <https://www.iso.org/standard/81230.html>.

¹⁵ АСТ, Policy Principles for Artificial Intelligence, нав. у фусноти 5 (позив на истраживање трошкова и користи транспарентности како би се утврдило како и под којим околностима би обавезе транспарентности помогле у отклањању ризика).

¹⁶ Уредба (ЕУ) 2024/1689 (Акт о вештачкој интелигенцији), члан 50, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

филтрирање нежељене поште, откривање превара и безбедносни надзор, а сумњамо да је то намера Министарства. Предлажемо Министарству да се за аутоматизовано доношење одлука ослони само на члан 62, примењујући га на исти начин без обзира на то да ли се користи ВИ, и да брише члан 53. ст. 4-5 или га изричито ограничи на одлуке које производе правне последице или на сличан начин значајно утичу на лице.

4. Дефиниције и правни основи (чл. 4, 14. и 20)

Поздрављамо одлуку Министарства да легитимни интерес дефинише позивањем на неопходност, подобност, сразмерност и разумна очекивања лица на која се подаци односе, што одражава начин на који се тест из GDPR-а примењује у пракси. Међутим, према предложеном тексту дефиниција се односи само на обраду која се врши у оквиру већ успостављеног односа са лицем на које се подаци односе. Такав услов би искључио многе случајеве у којима претходни однос не постоји, као што су провере које се врше пре закључења уговора и развој модела ВИ на подацима из много извора, па чак и неке од сврха које сама дефиниција наводи као примере, јер се спречавање превара и безбедност информација често односе на лица која немају никакав однос са руковооцем, а GDPR све ове случајеве признаје као случајеве који се могу заснивати на легитимном интересу (уводне изјаве 47-49). Предлажемо Министарству да брише упућивање на успостављени однос и да постојање и природу евентуалног односа третира као чинилац у тесту одмеравања интереса, а не као предуслов. Будући да Нацрт закона у члану 14. мења и редослед правних основа, предлажемо Министарству да у члан 14. дода одредбу којом се прописује да су сви наведени основи једнаке снаге и да редослед којим су наведени не утврђује предност ниједног од њих.

Дефиниција профилисања из члана 4. више не упућује на аутоматизовану обраду и стога би обухватила¹⁷ сваку оцену својстава личности, укључујући и уобичајено ручно разматрање пријаве за посао или захтева за кредит. Будући да профилисање активира заштиту из члана 62. и повезане обавезе транспарентности, предлажемо Министарству да врати реч „аутоматизоване“, у складу са чланом 4. тачка 4) GDPR-а и Законом из 2018. године, како би се та заштита и даље примењивала у случајевима за које је осмишљена.

5. Територијално важење и представници (члан 3)

Чланом 3. прописује се да се Нацрт закона примењује на руковооце и обрађиваче који имају седиште у Србији, а када је реч о онима који седиште имају у иностранству, на обраду података лица која имају пребивалиште или боравиште у Србији ако се обрада врши „у оквиру активности на територији Републике Србије“. Тај израз би се могао тумачити или тако да захтева оперативно присуство у Србији или тако да обухвата сваку услугу коју користе лица са пребивалиштем у Србији, а мали програмер изван

¹⁷ Нацрт закона, члан 4 („профилисање је сваки облик обраде који се користи да би се оценило одређено својство личности“). Упоредити са чланом 4. тачка 4) GDPR-а (у енглеској верзији: „any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person“).

Србије чију апликацију преузме неколико корисника из Србије не може на основу њега да утврди да ли је обухваћен законом. Предлажемо Министарству да се врати критеријумима из Закона из 2018. године и члана 3. став 2. GDPR-а, према којима је страни руковац обухваћен законом ако лицима у Србији нуди робу или услуге или прати њихово понашање у Србији, јер су ови критеријуми познати предузећима широм света и разјашњени смерницама и судском праксом. Такође предлажемо Министарству да задржи изузетак, који постоји у Закону из 2018. године и у члану 27. став 2. GDPR-а, од обавезе именовања представника у Србији за обраду која је повремена, не обухвата посебно осетљиве податке у великом обиму и вероватно неће проузроковати ризик за физичка лица.

6. Посебно осетљиви и биометријски подаци (члан 32)

Чланом 32. прописује се да се, када се биометријски подаци обрађују ради идентификације на основу пристанка, лицу мора понудити алтернатива која мање задире у приватност. Многе апликације омогућавају корисницима да се пријаве путем биометријске аутентификације уграђене у њихов телефон или рачунар, при чему отисак прста или шаблон лица остаје на уређају под контролом корисника, а апликација прима само потврду да је аутентификација успела. Предлажемо Министарству да прецизира да апликација која користи такву функцију не обрађује биометријске податке у смислу Нацрта закона и да је за сваког руковаоца ПИН, лозинка или приступни код довољна алтернатива. Ово појашњење би подстакло употребу метода аутентификације које су безбедније и боље штите приватност од самих лозинки.

7. Видео надзор (чл. 45-51)

Нови одељак о видео надзору обавезе у погледу обавештења, писаних одлука, евиденција и чувања снимака ставља на лице које одлучи да постави систем и да њиме управља, што подржавамо. Многа мала предузећа испоручују камере, апликације и складиште у облаку које домаћинства и привредни субјекти користе за управљање сопственим системима, па предлажемо Министарству да изричито пропише да испоручилац хардвера, софтвера или складишног простора који снимке обрађује искључиво по налогу свог корисника има својство обрађивача, односно да не потпада под Нацрт закона ако нема приступ снимцима, и да не сноси обавезе руковаоца из чл. 45-51.

8. Прекогранични пренос података (чл. 103-108)

Поздрављамо проширење стандардних уговорних клаузула на пренос од руковаоца руковаоцу, од руковаоца обрађивачу, од обрађивача обрађивачу и од обрађивача руковаоцу, као и изричиту обавезу Повереника да их припреми и објави. Већина српских предузећа која преносе податке у иностранство, као и већина страних предузећа која их примају, већ користи стандардне уговорне клаузуле Европске

комисије,¹⁸ а други скуп клаузула са другачијим текстом повећао би трошкове без повећања заштите. Предлажемо Министарству да пропише да стране могу да испуне српски захтев коришћењем клаузула Европске комисије уз кратак српски додаток, као што је то учинило Уједињено Краљевство својим додатком уз клаузуле ЕУ.¹⁹

Такође предлажемо Министарству да потврди да се за јурисдикције и оквире обухваћене одлуком Европске комисије о примереном нивоу заштите, укључујући организације сертифициране у оквиру Оквира за приватност података ЕУ и САД (EU-U.S. Data Privacy Framework),²⁰ сматра да обезбеђују примерен ниво заштите без потребе за посебним националним списком, да призна обавезујућа пословна правила која су одобрили надзорни органи ЕУ и да омогући да механизми сертификације, укључујући систем Global Cross-Border Privacy Rules,²¹ служе као основ за пренос. Када је реч о одступању за повремени пренос заснован на уверљивом легитимном интересу (члан 108), предлажемо да Повереник објави смернице о томе када се сматра да се пренос „не понавља“ и шта треба да садржи прописано обавештење, јер је значење овог израза у одговарајућој одредби GDPR-а изазвало несигурност код малих предузећа.²²

87) 9. Обавештавање о повреди података о личности и процена утицаја (чл. 82. и 84-

Нацрт закона задржава обавезу да се Повереник обавести о повреди података о личности у року од 72 часа. Обавештавање о повредама ниског ризика троши време и малих предузећа и надзорних органа, а не побољшава исходе за физичка лица, док је Европска комисија у оквиру предлога Digital Omnibus предложила да се надзорни орган обавештава само о повредама које ће вероватно проузроковати висок ризик и да се за припрему обавештења остави више времена.²³ Предлажемо Министарству да усвоји исти праг и рок, како би предузеће које послује на оба тржишта могло да примењује јединствен план за одговор на инциденте.

Када је реч о процени утицаја, предлажемо да Повереник објави листе радњи обраде за које је процена потребна и за које није, усклађене са листама на нивоу ЕУ које би увео предлог Digital Omnibus, заједно са кратким обрасцем прилагођеним малим

¹⁸ Сprovedбена одлука Комисије (ЕУ) 2021/914 од 4. јуна 2021. године о стандардним уговорним клаузулама за пренос података о личности у треће земље, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

¹⁹ Канцеларија повереника за информације Уједињеног Краљевства (ICO), What are standard data protection clauses (the UK IDTA and the Addendum)?, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/appropriate-safeguards/what-are-standard-data-protection-clauses-the-uk-idta-and-the-addendum/>.

²⁰ Сprovedбена одлука Комисије (ЕУ) 2023/1795 од 10. јула 2023. године о примереном нивоу заштите података о личности у оквиру Оквира за приватност података ЕУ и САД, https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj.

²¹ Global Cross-Border Privacy Rules Forum, <https://www.globalcbpr.org/>.

²² B. ACT, Comments to the Article 29 Working Party re Guidelines on Article 49 of Regulation 2016/679 (26. март 2018), https://actonline.org/wp-content/uploads/03262018_ACT_Filing_WP29_Art49-FINAL.pdf.

²³ Предлог Digital Omnibus, нав. у фусноти 10, предложене измене члана 33; в. и EDPB-EDPS Joint Opinion 2/2026, нав. у фусноти 11 (сагласност са вишим прагом и дужим роком).

предузећима. Јасне листе смањују и претерано усклађивање опрезних предузећа и недовољно усклађивање предузећа која не знају да се правила на њих примењују.

10. Казнене одредбе

Подржавамо одлуку Министарства да највиши износ новчане казне за правна лица задржи на постојећем нивоу и да не уведе казне засноване на укупном светском промету. Нацрт закона уводи и сразмерну новчану казну до двадесетоструког износа проузроковане штете или неиспуњене обавезе, ограничену на петоструки износ највише прописане казне.²⁴ Предлажемо Министарству да у закону пропише, или да обавезе Повереника да објави, методологију за утврђивање вредности штете и неиспуњених обавеза, уз јасно одређење да се под штетом подразумева штета утврђена у поступку, а не штета која се само тврди, и да пропише да се у обзир узимају величина предузећа, савесност и сарадња. Такође предлажемо Министарству да изричито овласти Повереника да, уместо новчане казне, изрекне упозорење или корективну меру за прву, ненамерну повреду коју учини микро или мало предузеће, чиме би се примена прописа усмерила на усклађивање уместо на кажњавање када је то бољи исход.

11. Ступање на снагу и прелазни период

Према нашем разумевању, Нацрт закона би ступио на снагу осмог дана од дана објављивања, без прелазног периода за материјалне обавезе, док би за доношење подзаконских аката био предвиђен рок од девет месеци. Руковаоци би стога морали да испуне нове обавезе, укључујући евиденције о видео надзору, процене утицаја за ВИ и нове клаузуле за пренос, пре него што Повереник објави клаузуле, листе и смернице од којих усклађивање зависи, док је Закон из 2018. године предвидео девет месеци, а GDPR две године пре почетка примене обавеза.

Предлажемо Министарству да предвиди прелазни период од најмање 18 месеци пре почетка примене материјалних обавеза, да примену одредби о ВИ повеже са одговарајућим обавезама из закона о ВИ и да пропише да уговори и клаузуле за пренос закључени према Закону из 2018. године остају на снази током разумног периода, на пример 12 месеци, након што Повереник објави нове клаузуле. Такође предлажемо Министарству да затражи од Повереника да објави смернице о главним новим обавезама пре почетка њихове примене.

V. Закључак

АСТ подржава циљ Министарства да донесе савремен закон о заштити података који штити физичка лица, подржава дигиталну економију Србије и приближава српско право праву Европске уније. Предлажемо Министарству да препоруке изнете у овом документу унесе у коначни текст, посебно тако што ће одредбе о ВИ ограничити на питања заштите података,

²⁴ Petar Mijatović, Serbia's draft Personal Data Protection Law: What changes are on the table, IAPP (6. август 2026), <https://iapp.org/news/a/serbia-s-draft-personal-data-protection-law-what-changes-are-on-the-table>.

признати легитимни интерес као редован основ за развој ВИ, задржати усклађеност дефиниција и инструмената за пренос са GDPR-ом и оставити довољно времена малим предузећима да се ускладе. Захваљујемо на прилици да допринесемо овој јавној расправи и радо ћемо са Министарством разговарати о овим коментарима и поделити искуства малих програмера са других тржишта која су применила упоредиве прописе.

С поштовањем,

Brian Scarpelli
Виши саветник за глобалне јавне политике

Chapin Gregor
Саветник за јавне политике

Association for Competitive Technology