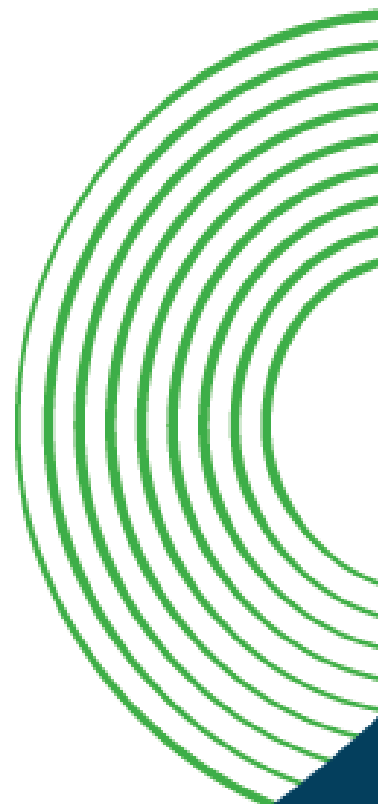

***Preporuke za Ministarstvo pravde i
članove radne grupe za izmenu
Zakona o tajnosti podataka***



Autorke:

Ana Toskić Cvetinović, Partneri Srbija

Kristina Obrenović, Partneri Srbija

Blažo Nedić

Prelom i dizajn:

Partneri Srbija

Izdavač:

Partneri Srbija

Beograd, decembar 2025.



Uvod

U sklopu istraživačkog rada organizacije Partneri Srbija u oblasti primene Zakona o tajnosti podataka, dostavljamo Vam analizu „**Tajnost podataka: pravni okvir i praksa**“. Cilj analize je da omogući što sveobuhvatnije sagledavanje normativnog okvira i prakse primene Zakona o tajnosti podataka i povezanih propisa, kao i da identifikuje ključne systemske i praktične izazove koji utiču na ostvarivanje prava na slobodan pristup informacijama od javnog značaja. Ovakav pregled posebno je značajan jer je Ministarstvo pravde formiralo radnu grupu za izmenu Zakona o tajnosti podataka, zbog čega analiza predstavlja pravovremen i argumentovan doprinos predstojećem reformskom procesu.

Polazeći od nalaza analize izradili smo i poseban set preporuka za Ministarstvo pravde i ostale članove radne grupe za izmenu Zakona o tajnosti podataka, u cilju unapređenja budućeg teksta Zakona.

Partneri Srbija ostaju otvoreni za sugestije i predloge, kao i posvećeni saradnji sa institucijama, civilnim društvom i stručnom javnošću, sa ciljem unapređenja normativnog i institucionalnog okvira u oblasti upravljanja informacijama i jačanja poverenja građana u rad javnih institucija.

“Izradu Preporuka omogućila je Misija OEBS-a u Srbiji u okviru projekta „Konsolidovanje procesa demokratizacije u sektoru bezbednosti u Republici Srbiji” koji je finansijski podržala Vlada Švedske.”¹

Preporuke

1. Učiniti reformu transparentnom i participativnom

Imajući u vidu obaveze transparentnosti i participativnosti u postupcima izrade i izmene javnih politika, neophodno je da Ministarstvo pravde objavi informacije o otpočinjanju rada na izmenama i dopunama Zakona o tajnosti podataka, kako na svojoj internet stranici, tako i putem Portala eKonsultacije. Ovo podrazumeva objavljivanje rešenja o obrazovanju radne grupe, njenog sastava, mandata i plana rada, kao i radnih verzija teksta zakona i obrazloženja predloženih normativnih rešenja.

¹ Ove preporuke, kao i sama analiza, izrađene su u okviru projekta Unapređivanje transparentnosti u sektoru bezbednosti, koji je podržala Misija OEBS-a u Srbiji.

Stavovi izrečeni u preporukama pripadaju isključivo autorima i ne predstavljaju nužno zvaničan stav Misije OEBS-a u Srbiji.

Svi pojmovi koji su u dokumentu upotrebljeni u muškom gramatičkom rodu obuhvataju muški i ženski rod lica na koja se odnose.

Pored toga, neophodno je obezbediti sprovođenje ranih javnih konsultacija i javne rasprave, kao i ciljanih konsultacija sa relevantnim akterima, uključujući Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, organizacije civilnog društva, istraživačke novinare i akademsku zajednicu. Ovakav pristup je posebno važan imajući u vidu da je radna grupa, prema dostupnim informacijama, sastavljena gotovo isključivo od predstavnika izvršne vlasti, kao i da pored Ministarstva pravde njen sastav pretežno čine predstavnici sektora bezbednosti.

2. Prebaciti ključne elemente režima tajnosti iz podzakonskih akata u Zakon o tajnosti podataka

Umanjiti oslanjanje na uredbu i pravilnike tako što će Zakon dodatno urediti ključne institute. Prekomerna razuđenost normativnih akata dovodi do pravne nesigurnosti i otežava doslednu primenu zakona, jer se ključni elementi sistema, uključujući kriterijume za klasifikaciju, postupke procene i zaštite tajnih podataka, postupke interne kontrole, nadzora koji sprovodi Ministarstvo pravde nalaze u uredbama i pravilnicima.

Dodatno, imajući u vidu da će izmene i dopune Zakona pratiti i izmena i dopuna podzakonskih akata, propisati da se podzakonski akti moraju doneti u jasno definisanim rokovima.

Ujedno, obezbediti da javnost bude uključena i u proces izmena i dopuna podzakonskih akata kroz objavljivanje nacрта ovih dokumenata i organizovanje javne rasprave.

3. Reformisati stepen tajnosti „INTERNO“

U procesu izmena i dopuna Zakona o tajnosti podataka neophodno je preispitati koncept i pravni režim stepena tajnosti „INTERNO“.

Stepen tajnosti „INTERNO“ definisan je previše široko i neprecizno kao stepen „koji se određuje radi sprečavanja nastanka štete za rad, odnosno obavljanje zadataka i poslova organa javne vlasti koji ih je odredio“. Međutim, ono što predstavlja štetu za rad organa ne mora nužno predstavljati štetu po državne interese, što je osnovni uslov za primenu tajnosti. Takve formulacije su izuzetno rastegljive, pa pod oznakom „INTERNO“ može završiti veliki broj informacija koje u međunarodnim praksama ne potpadaju pod tajnost. Ovaj stepen tajnosti stoga postaje mesto sudara između podataka od javnog značaja i tajnih podataka. Reč je o podacima koji po pravilu ne bi trebalo da budu tajni, ali ih organi često nastoje zaštititi kako bi ograničili pristup javnosti. Kako je upravo ovakvih podataka najviše u svakodnevnom radu uprave, to otvara i najveće mogućnosti za zloupotrebe.

Podzakonski akti, takođe ne definišu na adekvatan način kada se stepen tajnosti „INTERNO“ treba primenjivati. Stoga je neophodno da ovaj problem bude rešen prilikom procesa izmena

i dopuna Zakona o tajnosti podataka. Prilikom definisanja ovog stepena tajnosti u Zakonu, neophodno je stepen tajnosti interno dovesti u direktnu vezu sa nastupanjem posledica po interese koji se štite ovim Zakonom. Neophodno je propisati strože kriterijume, kraće rokove, obaveznu reviziju i jače mehanizme kontrole, uz jasnu zabranu klasifikovanja administrativno-organizacionih dokumenata kao tajnih bez procene štete po interese koji se štite Zakonom.

4. Uspostaviti i ojačati nadzor nad primenom Zakona

Neophodno je normativno otkloniti prepreke (odnos sa Zakonom o inspeksijskom nadzoru; pravo uvida u dokumenta i druge) na koje se Ministarstvo pravde poziva kao argumente za nesprovođenje nadzora u ovoj oblasti. Prilikom razmatranja ovog problema potrebno je razmotriti promenu modela nadzora, imajući u vidu da se dosadašnji model pokazao nefunkcionalnim:

- ili ozbiljno ojačati nadzornu funkciju u Ministarstvu pravde (kapaciteti, ovlašćenja, planovi, godišnji nadzori),
- ili preneti spoljašnji nadzor na specijalizovanu instituciju sa tehničkim i bezbednosnim kapacitetima po uzoru na "NSA" modele.

Ukoliko nadzor ostane kao deo ovlašćenja Ministarstva pravde, neophodno je detaljno propisati nadzorna ovlašćenja, postupak nadzora, uključujući i ovlašćenja za pristup sadržini tajnih dokumenata u meri potrebnoj za nadzor, uz obavezu čuvanja tajnosti. Preporuka je da tekst Zakona bude dopunjen odredbama koje se nalaze u Pravilniku o službenoj legitimaciji i načinu rada lica ovlašćenih za vršenje nadzora („Službeni glasnik RS”, br. 85/13 i 71/14)¹, poglavlje III- način rada, tako da ovlašćenja za nadzor i postupak nadzora, uključujući i obavezu izrade godišnjeg plana nadzora, i uvođenje odredaba o redovnom i vanrednom nadzoru budu definisane Zakonom.

5. Ukloniti konflikt interesa u unutrašnjoj kontroli

Zakon o tajnosti podataka predviđa da je za unutrašnju kontrolu nad primenom zakona odgovoran rukovodilac organa javne vlasti (član 84). Istovremeno, prema članu 9, upravo je rukovodilac jedan od ovlašćenih subjekata za određivanje tajnosti podataka, kao i za prenošenje ovlašćenja na druga lica u organu. Time se uspostavlja sistem u kojem isto lice koje donosi odluke o označavanju podataka stepenom tajnosti ujedno vrši i unutrašnju kontrolu zakonitosti i opravdanosti tih odluka.

Ovakvo rešenje otvara ozbiljan konflikt interesa: rukovodilac je istovremeno i klasifikator i nadzornik sopstvenog postupanja. U praksi to znači da je teško očekivati objektivnu procenu opravdanosti klasifikacije, a posebno identifikovanje grešaka ili zloupotreba u primeni tajnosti.

Stoga je neophodno izmeniti postojeći sistem unutrašnje kontrole tako što će se uvesti obaveza za sve organe javne vlasti da sistematizuju posebno radno mesto, ili da za obavljanje ovih zadataka i poslova oforme posebnu grupu/jedinicu unutar organa javne vlasti.

6. Uspostaviti delotvorne sankcije i odgovornost za nezakonitu

klasifikaciju

Neophodno je propisati strože sankcije i posledice za nezakonito, neopravdano ili zloupotrebom ovlašćenja izvršeno proglašavanje podataka tajnim, posebno kada ima za cilj izbegavanje javne kontrole ili prikrivanje nezakonitosti. Kaznene odredbe Zakona o tajnosti podataka zasnovane su na klasičnom, tradicionalnom shvatanju zaštite tajnih podataka, prema kojem je najveća opasnost neovlašćeno otkrivanje podataka koji već jesu zakonito klasifikovani. Međutim, Zakon gotovo potpuno izostavlja drugi, savremeni i jednako ozbiljan rizik: namerno ili neosnovano označavanje podataka kao tajnih. Iako ovakvo postupanje ne predstavlja otkrivanje tajnih podataka, njegova štetnost može biti jednaka ili čak veća, posebno u demokratskim društvima u kojima transparentnost predstavlja ključni mehanizam kontrole vlasti i sprečavanja korupcije.

Za razliku od krivičnih odredaba za otkrivanje tajnih podataka koje su visoke, sankcije za nezakonitu klasifikaciju svode se isključivo na prekršajnu odgovornost, i to u obliku novčane kazne od 5.000 do 50.000 dinara.

Na osnovu svega iznetog, predlažemo da se za nezakonito označavanje podataka kao tajnih Zakonom pored prekršajnih uvedu i krivične sankcije za situacije kada je nezakonito označavanje podataka dovelo do posledica po druge interese države koji se štite ustavom i zakonima (sakrivanje korupcije, zloupotreba službenog položaja, ugrožavanje javnog zdravlja, javne imovine, životne sredine i dr).

7. Zaustaviti širenje režima tajnosti kroz sektorske zakone

Jasno propisati da se tajnost ne određuje po vrsti dokumenta ili oblasti rada organa javne vlasti, već isključivo po sadržini dokumenta i proceni moguće štete. Uvesti normu koja sprečava da sektorski zakoni unapred proglašavaju čitave klase dokumenata tajnim osim u izuzetnim slučajevima uz stroge uslove i obrazloženje. Dosadašnja praksa da se drugim, sektorskim zakonima uvodi tajnost odstupa od osnovnog principa da se tajnost određuje na osnovu sadržine informacije i procene štete, a ne prema vrsti dokumenta ili oblasti rada organa javne vlasti. Na ovaj način kreiraju se čitave klase dokumenata koje se odnose na rad organa javne vlasti, a koje postaju izuzete iz jedinstvenog sistema slobode pristupa informacijama i sistema zaštite tajnih podataka, čime se narušava koherentnost pravnog okvira u ovoj oblasti. Ovakva praksa dodatno učvršćuju trend institucionalnog zatvaranja i stvaranja paralelnih režima tajnosti unutar sektora bezbednosti, čime se sužava prostor za

javni nadzor nad sektorom bezbednosti i otežava primena Zakona o slobodnom pristupu informacijama od javnog značaja.

8. Učiniti parlamentarni nadzor funkcionalnim

Neophodno je dopuniti i precizirati obavezu i odredbu da se godišnji izveštaji o primeni Zakona o tajnosti podataka dostavljaju Narodnoj skupštini u propisanim rokovima, uz standardizovan sadržaj izveštaja, i propisati sankcije za propuštanje izrade i dostavljanja godišnjih izveštaja Narodnoj skupštini.

9. Postupak izdavanja sertifikata za pristup tajnim podacima narodnim poslanicima i nezavisnim državnim organima

Prilikom procesa izmena i dopuna Zakona o tajnosti podataka neophodno je rešiti pitanje potencijalnog sukoba interesa u postupku izdavanja sertifikata narodnim poslanicima (posebno članovima nadzornih odbora) i nezavisnim državnim institucijama, i obezbediti da pristup informacijama potrebnim za vršenje parlamentarnog nadzora, i ovlašćenja nezavisnih institucija ne zavisi od organa koji su predmet nadzora.

Tokom godina primene Zakona o tajnosti podataka otvorilo se i pitanje na koji način narodni poslanici dobijaju sertifikate za pristup tajnim podacima. Poslanicima koji su članovi Odbora za odbranu i unutrašnje poslove i Odbora za kontrolu službi bezbednosti sertifikati su neophodni kako bi mogli da imaju uvid u tajne podatke koje im nadležni organi dostavljaju na razmatranje, uključujući izveštaje o stanju bezbednosti, izveštaje o radu službi bezbednosti i druga relevantna dokumenta.

Prema Zakonu o tajnosti podataka, bezbednosnu proveru za pristup tajnim podacima dokumentima stepena tajnosti „DRŽAVNA TAJNA“ i „STROGO POVERLJIVO“, koja prethodi izdavanju sertifikata za pristup tajnim podacima, sprovodi Bezbednosno-informativna agencija (BIA). Bezbednosnu proveru za pristup tajnim podacima i dokumentima stepena tajnosti „POVERLJIVO“ i „INTERNO“ sprovodi ministarstvo nadležno za unutrašnje poslove.

Ovakvo zakonsko rešenje otvara ozbiljno pitanje sukoba interesa i funkcionalne nezavisnosti parlamentarnog nadzora, budući da su upravo organi čiji rad narodni poslanici nadziru kroz skupštinske odbore ovlašćeni da sprovedu bezbednosne provere i, posredno, odlučuju o njihovom pristupu tajnim podacima. Time se stvara potencijal za institucionalnu zavisnost i narušava se osnovni princip kontrole izvršne vlasti od strane zakonodavne, jer pristup informacijama koje su ključne za efektivan nadzor može biti ograničen ili uslovljen odlukama organa koji su predmet tog nadzora. Isti princip važi i kada su u pitanju nezavisni državni organi poput Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, Zaštitnika građana, Agencije za sprečavanje korupcije i drugih, čiji rad nekada direktno zavisi od posedovanja sertifikata za pristup tajnim podacima.

