



Republika Srbija  
Ministarstvo pravde  
Nemanjina 22-26  
11000 Beograd

## Komentari na Nacrt zakona o zaštiti podataka o ličnosti

### -Uvod-

U skladu sa pozivom Ministarstva pravde Republike Srbije za učešće u javnoj raspravi o Nacrtu zakona o zaštiti podataka o ličnosti (*u daljem tekstu: „Nacrt zakona“*), čiji tekst je objavljen na sajtu Ministarstva<sup>1</sup>, organizacije civilnog društva i SHARE Fondacija dostavljaju svoje komentare sa ciljem unapređenja predstavljenog Nacrta.

Posvećene zaštiti prava i sloboda građana u digitalnom okruženju, organizacije civilnog društva smatraju unapređenje standarda zaštite podataka o ličnosti jednim od temeljnih uslova za puno ostvarivanje vladavine prava.<sup>2</sup>

Dužni smo da najpre skrenemo pažnju na činjenicu da je o sastavu i obavezama radne grupe za izradu Nacrta, koju je nadležno ministarstvo formiralo 2013. godine, zainteresovana javnost obavještena tek početkom 2015. godine, na osnovu zahteva za pristup informacijama od javnog značaja. Javnost je tada saznala da su za članove radne grupe za izradu Nacrta imenovani po jedan pripadnik Bezbednosno-informativne agencije i Vojno-bezbednosne agencije, dvoje službenika Ministarstva unutrašnjih poslova, jedan službenik Ministarstva odbrane, dvoje službenika tadašnjeg Ministarstva spoljne i unutrašnje trgovine i telekomunikacija, jedan službenik Ministarstva pravde, jedan službenik Vladine Kancelarije za ljudska i manjinska prava, te jedan docent pravnog fakulteta.

Podsećamo da obavezujuće Smernice za uključivanje organizacija civilnog društva u proces donošenja propisa<sup>3</sup>, dokument koji je Vlada Srbije usvojila sredinom 2014. godine, kao osnovni princip uzima „jedno od osnovnih načela evropskog upravljanja javnim poslovima“ – aktivno učešće organizacija civilnog društva (OCD) u svim fazama procesa donošenja propisa.

Smernicama se organima državne uprave nalaže da pravovremeno, potpuno i objektivno informišu organizacije civilnog društva „kako bi se olakšalo razumevanje problema kao i načini za njihovo rešavanje“. Od organa državne uprave se očekuje i da razmenjuju informacije sa

<sup>1</sup> <http://mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php>

<sup>2</sup> Za reference, upućujemo na istraživanja SHARE Fondacije dostupna na sajtu <http://shareconference.net/sh> i kolaborativnoj bazi znanja

[http://wiki.sharedefense.org/index.php/Za%C5%A1tita\\_podataka\\_o\\_li%C4%8Dnosti](http://wiki.sharedefense.org/index.php/Za%C5%A1tita_podataka_o_li%C4%8Dnosti)

<sup>3</sup> Smernice su dostupne na adresi: [http://www.civilnodrustvo.gov.rs/upload/old\\_site/2012/10/SR-smernice.pdf](http://www.civilnodrustvo.gov.rs/upload/old_site/2012/10/SR-smernice.pdf)

OCD „u svim fazama procesa“ (konsultacije u fazi planiranja i izrade strateških dokumenata, nacrtu/predloga propisa, javna rasprava). Organima državne uprave se takođe nalaže da uključe predstavnike OCD u proces izrade propisa, a kao primer se navodi članstvo u radnim grupama za izradu propisa. Kao najviši nivo saradnje i uzajamne odgovornosti, Smernice traže partnerstvo sa OCD u primeni propisa i odlučivanju.

Uzajamno poverenje koje se gradi „stalnim dijalogom“ te otvorenost i odgovornost, neki su od ključnih principa na kojima se zasniva rešenost Vlade Srbije da uključi OCD u proces donošenja propisa, na način kako je opisano u Smernicama.

Javna rasprava o Nacrtu zakona, budućem krovnom zakonu, trajala je svega mesec dana, dok je tom prilikom organizovan samo jedan formalni skup kojem zbog neblagovremenog poziva nisu prisustvovali svi zainteresovani.

U poslednjem Godišnjem izveštaju Evropske komisije o napretku Srbije<sup>4</sup> izričito se navodi: „Potrebno je usvojiti novi zakon o zaštiti podataka o ličnosti da bi se obezbedila potpuna usklađenost sa standardima EU.... Zakonodavstvo u oblasti obrade osetljivih podataka treba usvojiti po hitnom postupku“. Uvereni smo da hitnost postupka ne podrazumeva gotovo potpuno isključenje javnosti iz propisanih procedura izrade zakonskih rešenja od interesa za celokupno društvo.

Osim što u sastavu radne grupe gotovo da nije bilo predstavnika stručne zajednice ni organizacija za ljudska prava, te što je javna rasprava trajala svega mesec dana, postojeća radna grupa je bez obrazloženja prekršila jasno naznačenu obavezu iz rešenja ministra pravde, da tekst radne verzije novog zakona pripremi najkasnije do 1. maja 2013. godine.

Takođe, kao što je poznato, [Akcionim planom za Poglavlje 23](#)<sup>5</sup> u okviru pregovora Srbije o pridruživanju Evropskoj uniji utvrđeno je da Nacrt zakona treba da bude u skladu sa [Modelom](#)<sup>6</sup> koji je pre više od godinu dana Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti pripremio i stavio na raspolaganje Ministarstvu pravde i Vladi Srbije. Međutim, predloženi Nacrt bitno odstupa od ovog Modela, što je Poverenik [detaljno obrazložio](#).<sup>7</sup> Naš je stav da Model Poverenika za razliku od Nacrta zakona ipak predstavlja kvalitativan pomak u

<sup>4</sup> Dostupno na srpskom na adresi:

[http://www.seio.gov.rs/upload/documents/eu\\_dokumenta/godisnji\\_izvestaji\\_ek\\_o\\_napretku/izvestaj\\_o\\_na\\_pretku\\_nov\\_2015.pdf](http://www.seio.gov.rs/upload/documents/eu_dokumenta/godisnji_izvestaji_ek_o_napretku/izvestaj_o_na_pretku_nov_2015.pdf). Verzija na engleskom:

[http://ec.europa.eu/enlargement/pdf/key\\_documents/2015/20151110\\_report\\_serbia.pdf](http://ec.europa.eu/enlargement/pdf/key_documents/2015/20151110_report_serbia.pdf)

<sup>5</sup> Dostupno na: <http://www.mpravde.gov.rs/files/Akcioni%20plan%20PG%2023%20Treci%20nacrt-%20Konacna%20verzija1.pdf>

<sup>6</sup> Videti: <http://www.poverenik.rs/yu/saopstenja-i-aktuelnosti/1900-poverenik-stavio-na-raspolaganje-vladi-model-novog-zakona-o-zastiti-podataka-o-licnosti.html>

<sup>7</sup> Obrazloženje Poverenika možete pročitati na: <http://www.poverenik.rs/sr/saopstenja-i-aktuelnosti/2228-slab-nacrt-zakona-o-zastiti-podataka-o-licnosti.html>

odnosu na postojeće zakonsko rešenje, regulisanjem brojnih pitanja koja su trenutno izvan okvira zakona.

U nastavku su izloženi komentari na obrazloženje i sam tekst Nacrta zakona. S obzirom na kratak vremenski rok, u ovim komentarima nisu analizirani svi članovi Nacrta zakona, već samo oni za koje smo smatrali da mogu izazvati najviše nedoumica u primeni zakona.

## **-Komentari na Obrazloženje za donošenje Zakona o zaštiti podataka o ličnosti-**

### **• Odeljak II - Razlozi za donošenje Zakona**

U obrazloženju Nacrta zakona kao razlozi za donošenje ističu se „*potreba Republike Srbije, potreba za međunarodnom saradnjom, a pre svega proces pridruživanja Republike Srbije Evropskoj uniji.*“

Iako se članstvo Srbije u Evropskoj uniji u izvesnom smislu može smatrati opštim interesom, a manjkavost postojeće nacionalne regulative već donekle opštim mestom, obrazloženje Nacrta zakona o zaštiti podataka o ličnosti u kojem se osnovni razlozi iscrpljuju ovim argumentima, ukazuje na nerazumevanje privatnosti kao temeljnog ljudskog prava. Zaštita podataka o ličnosti predstavlja interes svih građana, i izvire iz prava koje prethodi kontingentim državnim sporazumima i trenutnim zakonskim rešenjima.

Usklađivanje sa pravnim tekovinama Evropske unije nesumnjiv je korak ka unapređenju standarda zaštite ljudskih prava u Srbiji, u čijem bi fokusu morao pre svega biti interes građana.

U delu obrazloženja Nacrta u kojem se analizira sadašnje stanje i problemi koje bi zakon trebalo da reši, objašnjava se *acquis* EU u ovoj oblasti, uz odluke institucija EU i pravne mehanizme kojima se unapređuje i garantuje zaštita podataka o ličnosti. Analiza postojećih pravnih prilika u Srbiji, međutim, svodi se na kraći, uopšten opis formalnih nedostataka.

Smatramo da je bolje razumevanje oblasti prikupljanja i obrade ličnih podataka od izuzetnog značaja. U doba kada tehnologija omogućava rukovanje neslućenom količinom podataka u veoma kratkim vremenskim intervalima, privatnost građana pokazuje se kao jedno od temeljnih pitanja pravnog poretka zasnovanog na poštovanju ljudskih prava.

Izričito pozivanje na interes građana i potrebu zaštite ljudskih prava, uvereni smo, više je od simboličkog izraza suštinskog opredeljenja zakonodavca.

Značajan deo obrazloženja predstavljenog Nacrta preuzet je iz obrazloženja Modela zakona koji je Vladi Srbije oktobra 2014. ustupila kancelarija Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti. Izostavljeni delovi, međutim, najčešće se tiču upravo analize postojećeg stanja u nacionalnoj regulativi i posledica koje neuređena oblast ima po zaštitu prava građana Srbije.

Odeljak obrazloženja Nacrta zakona koji se tiče razloga za njegovo donošenje, zaključen je konstatacijom da su prilikom izrade Nacrta između ostalog korišćena rešenja iz Modela zakona Poverenika. Sudeći po mišljenju Poverenika<sup>8</sup>, najbitnija rešenja iz Modela su izostavljena.

- **Odeljak IV - Procena finansijskih sredstava potrebnih za sprovođenje zakona**

Smatramo da obrazloženjem nisu na adekvatan način procenjena finansijska sredstva za njegovo sprovođenje i implementaciju novih rešenja, što će biti proces koji će trajati nekoliko godina, te je stoga neprikladna napomena na kraju obrazloženja da za sprovođenje zakona „*nije potrebno obezbediti dodatna sredstva u budžetu za 2015. godinu*“. Podsećamo da Poslovnik Vlade Republike Srbije u članu 39, stav 1, tačka 4 predviđa da Obrazloženje nacrta zakona mora da sadrži procenu finansijskih sredstava potrebnih za sprovođenje akta.

Nacrt predviđa značajne organizacione i tehničke uslove za sprovođenje zakonskih odredbi što podrazumeva odgovarajuća ulaganja.

U važećem zakonu (Zakon o zaštiti podataka o ličnosti, „Službeni glasnik RS“ br. 97/08, 104/09 – dr. zakon, 68/12 – US i 107/12), poglavlje o bezbednosti podataka (VI OBEZBEĐENJE PODATAKA) sadrži dva člana od kojih jedan reguliše obavezu čuvanja tajne (član 46) dok je organizacionim i tehničkim merama (član 47) posvećeno svega dva stava.

Predstavljen Nacrt zakona o zaštiti podataka o ličnosti utvrđuje opšte (član 47) i posebne obaveze rukovaoca (član 48) u zaštiti bezbednosti podataka, koje između ostalog podrazumevaju: procenu rizika narušavanja bezbednosti, zaštitu prostorija, opreme i systemske programske opreme, zaštitu baza podataka i programskih aplikacija, zaštitu od neovlašćenih radnji obrade, obuku zaposlenih na poslovima obrade.

U članu 52 Nacrta predviđeno je određivanje lica za zaštitu podataka sa odgovarajućim stručnim znanjem, koje može biti zaposleno ili angažovano na osnovu ugovora. Istim članom predviđena je i dužnost rukovaoca i obrađivača da licu za zaštitu podataka obezbede sticanje stručnog znanja.

Novo radno mesto i/ili edukacija takođe zahtevaju izdvajanje posebnih sredstava. Lice za zaštitu podataka (član 53) između ostalog periodično vrši procenu rizika od povrede bezbednosti podataka i učestvuje u obuci zaposlenih na poslovima obrade podataka. Takođe, članom 54 Nacrt predviđa formiranje i vođenje stručne evidencije o obradi podataka.

Sve nove obaveze rukovalaca i obrađivača podataka nužno povlače ulaganje dodatnih finansijskih sredstava, a obzirom da će se sve ove obaveze neizostavno odnositi i na državne

---

<sup>8</sup> Videti: <http://www.poverenik.rs/yy/saopstenja-i-aktuelnosti/2228-slab-nacrt-zakona-o-zastiti-podataka-o-licnosti.html>

organe, budžetom Republike Srbije ali i budžetima drugih korisnika javnih sredstava biće potrebno obezbediti dodatna finansijska sredstva. Takođe, i nedržavni subjekti na koje će se ovaj Zakon odnositi trebalo bi da budu što jasnije obavešteni o dodatnim troškovima i ulaganjima, kako bi se na vreme pripremili za njih.

## **-Komentari na tekst Nacrta zakona o zaštiti podataka o ličnosti-**

- **Član 4 - Primena zakona i teritorijalno važenje**

### **Stav 2**

Nacrtom zakona predviđeno je da se načini obrade koji se vrše u svrhu video nadzora, direktnog oglašavanja, pružanja zdravstvenih, odnosno finansijskih usluga, uređuju posebnim zakonom. Smatramo da ovo nije dobro rešenje iz sledećih razloga:

Pomenute radnje obrade su u savremenom društvu neki od najčešćih i za privatnost građana najintruizivnijih načina obrade podataka o ličnosti. Sve brži razvoj tehnologije, nove metode za prikupljanje podataka, nove svrhe u koje se ti podaci koriste, kao i neobaveštenost građana o ovoj oblasti otvaraju prostor za krupne zloupotrebe, pri čemu nedostatak jasnog pravnog okvira vodi u pravnu nesigurnost. Dovoljan je i laički pogled na pojedinačne segmente prikupljanja ličnih podataka da razjasni kakve se neslućene mogućnosti zloupotreba ukazuju (upućujemo na istraživanja SHARE Labs, Nevidljive infrastrukture: „Dozvole na mobilnim uređajima“<sup>9</sup> i „Onlajn pratioci“<sup>10</sup>).

Sa druge strane, Republika Srbija se načelno opredelila za primenu koncepta elektronske uprave (eGovernance), odnosno transfer komunikacije države između pojedinih institucija, kao i komunikacije sa građanima, u digitalno okruženje. Izvršavanje administrativnih poslova i međusobnih obaveza građana i institucija države višestruko su olakšani, a njihova cena značajno smanjena, ukoliko se obavljaju elektronskim putem. Elektronsko poslovanje još jedan je važan cilj čije puno ostvarenje Srbiju tek očekuje. Nijedna od ovih strukturnih promena nije moguća bez principijelnog i adekvatnog uređenja oblasti zaštite ličnih podataka.

Potreba za detaljnim regulisanjem ove oblasti je zbog brojnih nedoumica i zloupotreba postojala još od donošenja trenutno važećeg Zakona o zaštiti podataka o ličnosti, dok se u poslednjem Godišnjem izveštaju Evropske komisije o napretku Srbije<sup>11</sup> izričito navodi da je ova oblast (konkretno se pominju **video nadzor, biometrijski podaci, bezbednost podataka na Internetu, obrada i zaštita osetljivih podataka, kao i direktan marketing**) neadekvatno regulisana i da ostavlja značajan prostor za zloupotrebe.

<sup>9</sup> <http://labs.rs/sr/nevidljive-infrastrukture-dozvole-na-mobilnim-uredajima/>

<sup>10</sup> <http://labs.rs/sr/nevidljiva-infrastruktura-onlajn-pratioci/>

<sup>11</sup> Dostupno na:

[http://www.seio.gov.rs/upload/documents/eu\\_dokumenta/godisnji\\_izvestaji\\_ek\\_o\\_napretku/izvestaj\\_o\\_na\\_pretku\\_nov\\_2015.pdf](http://www.seio.gov.rs/upload/documents/eu_dokumenta/godisnji_izvestaji_ek_o_napretku/izvestaj_o_na_pretku_nov_2015.pdf)

Smatramo da je **neophodno da Zakon o zaštiti podataka o ličnosti, kao osnovni zakon, temeljnim načelima zaštite izričito obuhvati sve postojeće posebne vidove obrade**, i na taj način predupredi konfuziju, proizvoljnosti i umanjeње zaštite garantovanih prava u iščekivanju nekih budućih posebnih zakona.

Dodatno, načini obrade biometrijskih podataka, jedinstvenog matičnog broja građana, te podataka o ulasku i izlasku iz poslovnog prostora u Nacrtu zakona nisu predviđeni čak ni kao materija koja bi se obradila posebnim zakonom, čime se potpuno zanemaruje značaj i specifičnost ovakvih vidova obrade koji bi morali da se detaljnije regulišu u samom tekstu Nacrta zakona.

Urgentnost regulisanja svih pomenutih pitanja ne dopušta neizvesnost koju otvara ovakvo rešenje u Nacrtu, imajući u vidu da nije jasno ko bi bio nadležan za izradu posebnog zakona ni u kom roku se može očekivati njegovo usvajanje, kao i da ne postoje nikakve indicije da se na pripremi takvog propisa preduzimaju određeni koraci.

Dok je javni prostor već premrežen kamerama za nadzor, a procenat finansijskih transakcija preko Interneta stalno raste, segment zaštite ličnih podataka i dalje je neuređen. Usvajanje novog Zakona o zaštiti podataka prilika je da se, bar u načelnim crtama na jasan i jednostavan način, preduzme zaštita prava građana u ovom smislu te zbog toga smatramo da je ovako ozbiljan propust Nacrta nepotreban.

Imajući u vidu ove probleme, Model Poverenika u Poglavlju IV uređuje posebne vidove obrade podataka o ličnosti i to: biometriju, video-nadzor, neposredno oglašavanje, obradu podataka o ulasku i izlasku iz poslovnog prostora, kao i obradu jedinstvenog matičnog broja na Internetu i upotrebu ličnih identifikacionih dokumenata. Time bi se umnogome mogli preduprediti brojni problemi koji izviru iz zasad neuređenih oblasti, zbog čega smatramo da je rešenje Modela Poverenika znatno naprednije od predloženog u Nacrtu zakona.

### **Stav 3**

Kao organizacije i pojedinci posvećeni digitalnim pravima i slobodama na Internetu, smatramo da teritorijalno važenje zakona definisano članom 4, stav 3 Nacrta zakona izaziva brojne nedoumice i nije u skladu sa novom realnošću koje donosi digitalno doba. Naime, dok je u fizičkom svetu jasno određivo šta znači obrada na teritoriji Republike Srbije, u digitalnom okruženju to nije slučaj. Podaci o ličnosti „proputuju“ čitav svet u delu sekunde, prolazeći kroz brojne teritorije odnosno nadležnosti. **Dok se prikupljanje podataka građana Srbije može vršiti na teritoriji Srbije, mesto njihove dalje obrade ponekad je nemoguće utvrditi.**<sup>12</sup> Ovakvo regulisanje bi u praksi dovelo do niza paradoksa; npr. ukoliko bi domaća firma, koja

<sup>12</sup> Videti: SHARE Lab, Nevidljive infrastrukture: „Uzbudljiv život Internet paketa“ <http://labs.rs/sr/nevidljiva-infrastruktura-uzbudljiv-zivot-internet-paketa/>



poseduje veliki broj podataka o ličnosti građana Srbije, obrađivala te podatke preko *Cloud* servisa na serverima koji se nalaze izvan teritorije Republike Srbije, ova firma ne bi imala obavezu da u tim slučajevima primenjuje ovaj zakon, što smatramo u potpunosti neprihvatljivim. Sa druge strane, veliki broj kompanija čiji je model poslovanja zasnovan na prikupljanju podataka, kao što su *Google* i *Facebook*, rukuju podacima o ličnosti građana Srbije, pa je logično pitanje kada bi se i na koji način ovakva odredba primenjivala na te kompanije. Registracija građana Srbije na sajtu koji se bavi prodajom odevnih predmeta iz Latinske Amerike mogla bi se tumačiti kao radnja obrade koja je preduzeta na teritoriji Republike Srbije, ali ukoliko se ti podaci prosleđuju na dalju obradu na serverima koji se nalaze u Sjedinjenim Državama, postavlja se pitanje da li bi se ovakva zakonska odredba mogla primenjivati.

Prema [istraživanju SHARE Fondacije](#), od 100 najposećenijih veb-sajtova među Internet korisnicima u Srbiji, samo 27 je zapravo hostovano na teritoriji Republike Srbije. Od ostalih, 36% je hostovano u SAD, a 27% u zemljama Evropske unije, što znači da je preko 63% veb-sajtova koje korisnici iz Srbije najčešće posećuju fizički smešteno izvan teritorije Republike Srbije.

Upravo iz tih razloga, važeća [Direktiva EU o zaštiti podataka o ličnosti 95/46/EC](#)<sup>13</sup> (u daljem tekstu: „Direktiva“), [Predlog uredbe Evropskog parlamenta i Saveta o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i o slobodnom kretanju podataka](#)<sup>14</sup> (u daljem tekstu: „Predlog uredbe“), kao i Model zakona Poverenika prvenstveno **vezuju regulatornu nadležnost za sedište, odnosno stabilno prisustvo rukovaoca na određenoj teritoriji, kao kriterijum koji je jasno odrediv**, te smatramo da bi i ovaj Nacrt zakona morao da uzme u obzir ovako određen kriterijum. Dodatno, u pogledu podataka koje prikupljaju rukovaoci izvan Srbije opravdano je uspostavljanje regulatorne nadležnosti srpskog prava u slučajevima kada se vrši ponuda roba i usluga licima u Srbiji, kao i kada se vrši praćenje njihovog ponašanja.<sup>15</sup>

- **Član 6 - Osnovna načela u Nacrtu zakona o zaštiti podataka o ličnosti**

Dopuštenost obrade, koja obuhvata niz uslova, Nacrtom zakona regulisana je jednim članom i to nabrojanjem neprecizno određenih, nedovoljno razumljivih i uopštenih principa, što je neprihvatljivo za zakon od ovakvog značaja.

Za dva načela - bezbednost podataka i zabrana diskriminacije - posvećeni su zasebni članovi (7 i 8), gde se ovi suštinski principi posebno i na zadovoljavajući način tretiraju. Smatramo da bi na

<sup>13</sup> Direktiva 95/46/EC Evropskog parlamenta i Saveta o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i o slobodnom kretanju podataka, dostupna na engleskom jeziku: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

<sup>14</sup> Predlog uredbe Evropskog parlamenta i Saveta o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i o slobodnom kretanju podataka, dostupan na engleskom jeziku: [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

<sup>15</sup> Predlog uredbe Evropskog Parlamenta i Saveta o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i o slobodnom kretanju podataka, 3(2)(a) i 3(2)(b). Dostupno na: [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

taj način trebalo regulisati i načela iz člana 6, kao što su zakonitost, pravičnost, ograničenost svrhe, srazmernost, tačnost podataka i drugo.

Budući da su vrste obrade podataka o ličnosti brojne, te da ubrzan napredak tehnologije gotovo svakodnevno razvija nove načine obrade, nepotrebno je od regulative očekivati da ove vrste detaljno i ažurno tretira. Upravo zbog toga je uspostavljanje načela za obradu podataka o ličnosti od suštinskog značaja, kako bi rukovaoci podacima o ličnosti, ali i svi ostali na koje se zakon odnosi, mogli da u konkretnim situacijama ispravno tumače zakonske odredbe, te da postupe u duhu zakona. Smatramo da je **definisane osnovnih načela obrade iz člana 6 Nacrta nedovoljno precizno i da može stvoriti nedoumice u primeni Zakona**. Takođe smatramo da je osnovna načela potrebno detaljnije regulisati, kako je i ponuđeno u Modelu koji je izradio Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (članovi 4-9).

- **Član 10 - Obrada bez pristanka**

Uzimajući u obzir da u ovom slučaju ispunjenost uslova za obradu bez pristanka procenjuje rukovalac, potrebno je ove izuzetke od opšteg pravila definisati precizno i jasno kako bi rukovalac mogao da bude siguran kada je ovlašćen da obrađuje podatke bez saglasnosti lica, imajući u vidu da zloupotrebom ovih izuzetaka mogu biti ozbiljno ugrožena lična prava.

U pogledu izuzetaka predviđenih članom 10, stav 1, tačke 1), 2), 3), 5) i 6) neophodno je ove tačke dopuniti i utvrditi da je obrada „**Neophodna**“ za ostvarivanje pojedinačnih SVRHA definisanih ovim izuzecima. Ovo naročito ima smisla uzimajući u obzir da su pomenute tačke preuzete iz člana 7 Direktive u kome se izričito navodi da je za sve ove svrhe potrebno da budu „**Neophodne**“ (eng. *necessary*). Ovaj naizgled tehnički detalj je od izuzetne važnosti jer bi se u odsustvu „Neophodnosti“, mogućnosti za obradu bez pristanka i bez loše namere rukovaoca mogle izuzetno široko tumačiti. Naime, rukovalac ne bi imao većih problema da obrazloži da je obradu bez pristanka vršio zbog izvršenja ugovora ili izvršenja obaveza predviđenih zakonom, ako u tom slučaju ne bi morao da obrazloži da je takva obrada bila neophodna, što smatramo da nije bila namera pisca Nacrta, koji je obradu bez pristanka želeo da reguliše kao dozvoljenu u izuzetnim situacijama. Zbog svega navedenog ističemo i da „Neophodno“ treba tumačiti izuzetno restriktivno i ako se svrha obrade ne može ostvariti na drugi način odnosno „*ukoliko je prikladno i neophodno obraditi podatke u određenom kontekstu kako bi se ostvario legitiman interes*“.<sup>16</sup>

Smatramo da izuzetak predviđen stavom 1, tačka 4): „*obrada neophodna u cilju izvršenja zadataka radi ostvarivanja javnog interesa ili u cilju izvršavanja zakonskih ovlašćenja rukovaoca ili treće strane kojoj su podaci učinjeni dostupnim*“ treba brisati, jer je njegovo sprovođenje predviđeno članovima 11 i 22 Nacrta zakona.

---

<sup>16</sup> “It is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest” - Mišljenje 06/2014 o legitimnom interesu rukovaoca na osnovu člana 7 Direktive, usvojeno 9. aprila 2014, str. 13, dostupno na: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)



Dodatno, potrebno je predvideti sankciju za obradu bez pristanka kada nije ispunjen uslov „neophodnosti“, usled okolnosti da izuzeci predviđeni ovim članom mogu biti predmet brojnih zloupotreba kako od strane privatnog, tako i javnog sektora.

Takođe, **Nacrt zakona ne reguliše pravo na prigovor lica čiji se podaci obrađuju bez pristanka**, što smatramo da je izuzetno značajno iz razloga mogućnosti za gore pomenute zloupotrebe. Upravo zato Direktiva predviđa da lica moraju najmanje imati pravo na prigovor u slučaju obrade predviđenih tačkama 4) i 6) Nacrta zakona, dok Predlog uredbe ovome dodaje i tačku 1) Nacrta zakona što treba tumačiti kao novu tendenciju koju bi naš zakonodavac trebalo na vreme da uvaži.

- **Član 11 - Obrada od strane organa vlasti**

Ustav Republike Srbije u članu 42 navodi da je zabranjena i kažnjiva upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni, u skladu sa zakonom, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom.

I pored toga Nacrt zakona je u članu 11 sačuvao princip diskrecije organa vlasti uspostavljen važećim zakonom, umesto da, u skladu sa Ustavom, uredi odstupanja od zajemčene zaštite podataka o ličnosti, odnosno precizira granice ovlašćenja nadležnih organa u izuzetnim slučajevima kao što su vođenje krivičnog postupka ili zaštita nacionalne bezbednosti, procedure koje su organi vlasti dužni da preduzmu, vremenska ograničenja i vrste podataka koje se u tim slučajevima mogu obrađivati, i drugo.

Naime, gotovo identično kao u važećem zakonu, Nacrtom zakona obrada od strane organa vlasti je moguća i bez pristanka *„ako je obrada neophodna [...] u cilju zaštite nacionalne ili javne bezbednosti, odbrane Republike Srbije, sprečavanja, otkrivanja, istrage i gonjenja za krivična dela, zaštite važnih ekonomskih, odnosno finansijskih interesa države [...]“*. Štaviše, Nacrt zakona je proširio spisak okolnosti pod kojima je odstupanje od ustavne garancije moguće, dodajući pravno nejasnom pojmu (javnog) morala još i nepostojeći set „etičkih pravila“.

Smatramo da predloženo rešenje nije prihvatljivo jer u osnovi **prepušta državnim organima da potpuno samostalno i arbitrarno odluče da li imaju pravo da bez pristanka obrađuju podatke o ličnosti iz nekog od preširoko definisanih razloga**. Na taj način se otvara širok prostor za povredu privatnosti građana Srbije u ime zaštite koncepata koje bi neki državni organ u nekom datom trenutku mogao razumeti kao „etičko pravilo“, što smatramo da je u suprotnosti sa članom 42 Ustava Republike Srbije.

U tom smislu podržavamo rešenje iz Modela Poverenika, koji u članu 17 predviđa da organi vlasti mogu da obrađuju podatke o ličnosti samo ako je obrada uređena zakonom. Na ovaj način postojala bi pravna sigurnost i za građane i za državne organe, pogotovo što je obrada podataka za tako bitne svrhe kao što su bezbednost, odbrana i slično već regulisane zakonima,

a ukoliko bi neke druge svrhe bile od jednakog značaja za društvo, njih bi trebalo sistemski da utvrdi zakonodavac u skladu sa Ustavom, umesto da ih državni organi određuju u pojedinačnim slučajevima i stihijski.

- **Član 13 - Obrada posebnih (osetljivih) podataka**

Iako se u okviru definicija (član 3, stav 2, tačka 11) posebno definišu posebni podaci, član 13 koji detaljno reguliše obradu ovih podataka ne pruža garancije koje su predviđene u članu 17 postojećeg zakona, članu 21 Modela i članu 8 Direktive, u kojima stoji da je obrada posebnih podataka u principu zabranjena, osim ukoliko nisu ispunjeni posebni uslovi za primenu izuzetka (*processing of such data is in principle prohibited, subject to some exceptions* - [WP 27 mišljenje](#)).<sup>17</sup> Naime, **član 13 propušta da utvrdi izuzetke** od kojih osnovni predstavlja pravilo da se obrada posebnih podataka može vršiti isključivo na osnovu izričitog pristanka lica, kao i u izuzetnim usko definisanim situacijama. Postojeći član 13 samo definiše ograničenja otkrivanja posebnih podataka trećim licima.

Pravni okvir koji se uspostavlja predloženim članom 13 tako dozvoljava da se obrada posebnih podataka može ostvariti bez saglasnosti na osnovu izuzetaka iz člana 10 Nacrta zakona, što je u suprotnosti sa Direktivom (*This also means that a controller processing special categories of data may never invoke solely a legal ground under Article 7 to legitimise a data processing activity* - [WP 27 mišljenje](#)).<sup>18</sup> Obrada posebno osetljivih podataka bez pristanka dakle zahteva kumulativnu primenu izuzetaka iz člana 7 i 8 Direktive.

- **Član 15 - Pristanak za obradu**

Ovim članom je propisano da se pristanak može dati usmeno, pismeno i u elektronskom obliku sa kvalifikovanim elektronskim potpisom, u skladu sa zakonom kojim se uređuje elektronski potpis i dokument. **Ovako regulisan pristanak ni na koji način nije u skladu sa navikama i ponašanjem ljudi u digitalnom i fizičkom svetu.** Naime, gotovo zanemarljiv procenat građana Srbije poseduje elektronski potpis, ali sa druge strane i više od 65% naših građana koristi Internet na svakodnevnom nivou i tamo ostavlja svoje podatke rukovaocima. Ovakvo rešenje bi u tom smislu dovelo do ogromne sive zone jer pristanci za obradu koje svakodnevno dajemo preko svojih kompjutera, telefona i drugih elektronskih uređaja ne bi bili validni, a svaka dalja obrada bi se smatrala nezakonitom. Predloženo rešenje svakako ne odgovara stvarnosti, jer u velikom broju slučajeva može biti jasno da je pristanak dat i bez korišćenja elektronskog potpisa. Sa druge strane, to bi naravno dovelo do relativizacije problema zaštite podataka na

<sup>17</sup> Mišljenje 06/2014 o legitimnom interesu rukovaoca na osnovu člana 7 Direktive, usvojeno 9. aprila 2014, str. 14. Dostupno na: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)

<sup>18</sup> Mišljenje 06/2014 o legitimnom interesu rukovaoca na osnovu člana 7 Direktive, usvojeno 9. aprila 2014, str. 15. Dostupno na: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)

Internetu jer zapravo pravi problem predstavljaju situacije u kojima nije najjasnije da li je lice dalo pristanak za obradu podataka. Na primer, tzv. kolačići (eng. cookies) su datoteke koje koriste sajтови kako bi prikupljali naše podatke. Oni će prikupljati naše podatke čak i ako nismo dali saglasnost za to, već će u najboljem slučaju negde u uglu sajta malim slovima izaći obaveštenje da određeni sajt koristi kolačiće. Takođe, moraćemo dosta da se pomučimo kako bismo saznali koje tačno podatke o nama skupljaju i za šta ih koriste. Iz tih razloga pitanje pristanka treba regulisati na način da se uvek zahteva da je pristanak dat nedvosmisleno, no u današnje vreme zahtevanje elektronskog potpisa svakako nije adekvatno i proporcionalno rešenje. U tom smislu smatramo da je jedno od boljih rešenja sadržano u Predlogu uredbe, gde se u preambuli u tački 25 definiše pristanak, te se posebno navodi primer za davanje pristanka za obradu na Internetu:

*„(25) Pristanak se daje izričito bilo kojom odgovarajućom metodom koja omogućava slobodno dat konkretan i obavešten izraz želje subjekta podataka, bilo izjavom ili jasnom potvrdnom radnjom subjekta podataka, i kojom se nedvosmisleno utvrđuje da su pojedinci svesni da time daju svoj pristanak za obradu podataka o ličnosti, što uključuje označavanje kvadratića prilikom posete Internet stranici ili bilo koju drugu izjavu ili postupanje koji u ovom smislu jasno ukazuju da subjekt podataka prihvata predloženu obradu svojih ličnih podataka.“<sup>19</sup>*

- **Član 17 - Obrada podataka o detetu, odnosno maloletnika na osnovu saglasnosti**

Smatramo da stav 1 i 2 ovog člana nisu u skladu sa svrhom pojma posebnih podataka za koje se kroz čitav Nacrt zakona zahteva viši stepen zaštite nego za ostale podatke. U tom smislu, nelogično je da se za obradu posebnih podataka zahteva saglasnost samo roditelja, dok se za obradu ostalih podataka zahteva kumulativna saglasnost roditelja i deteta, što je stroži uslov.

Stav 1 člana 17: *„Za lice mlađe od 18 godina **saglasnost za obradu posebnih podataka daje roditelj, usvojitelj, odnosno staratelj.***

Stav 2 člana 17: *„Ostali podaci o licu koje je starije od 12 godina ne mogu se obrađivati **bez njegove saglasnosti i saglasnosti roditelja, usvojitelja, odnosno staratelja.**“*

Ovom prilikom mora se uzeti u obzir odredba Porodičnog zakona iz člana 64, stav 1 sa kojim su pomenute odredbe Nacrta zakona u očiglednoj koliziji:

---

<sup>19</sup> (25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Dostupno na: [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

*„Dete koje nije navršilo 14. godinu života (mlađi maloletnik) može preduzimati pravne poslove kojima pribavlja isključivo prava, pravne poslove kojima ne stiče ni prava ni obaveze i pravne poslove malog značaja.“*

Može se razmotriti mogućnost da se detetu da ovlašćenje da samo daje saglasnost za obradu podataka koji ne predstavljaju posebne podatke. Iako podložno diskusiji, prihvatanje opštih pravila o poslovnoj sposobnosti maloletnika bi odgovaralo specifičnostima informacionog društva u kome **maloletnici učestalo koriste društvene mreže, mobilne aplikacije i druge Internet servise, čije korišćenje bi im formalno bilo onemogućeno bez saglasnosti roditelja, što u praksi ne bi bilo moguće sprovesti.** I pored duboke zabrinutosti za podatke koje maloletnici ustupaju Internet kompanijama, smatramo da njihovo rigorozno ograničavanje da pre 18. godine koriste Internet servise takođe predstavlja neprimereno rešenje, kojim se prvenstveno ograničava pristup znanju i savremenim društvenim tokovima. Sa druge strane, treba imati u vidu da na Internetu dominantno pravilo po pitanju saglasnosti maloletnika za obradu podataka proizlazi iz američkog akta [“COPPA - Children's Online Privacy Protection Act”](#)<sup>20</sup> koji predviđa da se saglasnost roditelja zahteva isključivo za decu mlađu od 13 godina. Uzimajući da su rešenja iz COPPA-e prihvaćena od strane najvećeg broja kompanija, usled njihovog američkog porekla, čini se da regulisanje na drugačiji način od COPPA-e u praksi neće imati praktičnog značaja, barem kada su Internet servisi u pitanju.

Takođe u pogledu stava 4 člana 17, a u vezi sa članom 64, stav 1 Porodičnog zakona, licu starijem od 14 (a ne 15) godina treba omogućiti da samostalno zahteva zaštitu podataka o ličnosti.

Potreba posebne zaštite maloletnika se treba ispoljiti kroz posebne mere, poput obaveze sprovođenja prethodne procene rizika (član 50), donošenja opšteg akta o zaštiti podataka (član 51) i određivanja lica za zaštitu podataka (član 52) kod rukovalaca koji obrađuju podatke o maloletnicima. Poslednje, ali ne i najmanje važno, strateškim dokumentima u svim oblastima treba podsticati digitalnu pismenost, posebno mladih - kako kroz formalno tako i kroz neformalno obrazovanje.

- **Član 22 - Ustupanje podataka primaocu**

Novina koju Nacrt zakona predviđa je članom 22 posebno definisan postupak za pristup podacima od strane primaoca, uključujući organe vlasti. Pored definisane obaveze rukovaoca da podatke učini dostupnim na osnovu pismenog zahteva koji sadrži ime primaoca, svrhu, pravni osnov i podatke koji se potražuju, Nacrt predviđa određene problematične izuzetke.

Prvi izuzetak predviđa mogućnost ustupanja podataka na osnovu usmenog zahteva „*ako razlozi hitnosti i svrha potraživanja to opravdavaju, a ne postoji sumnja u pogledu osnova potraživanja*“ (stav 4), što **na rukovaoca prenosi odgovornost procene pravnog osnova i utvrđivanja**

<sup>20</sup> <http://www.coppa.org/coppa.htm>

**opravdanosti ovakvog zahteva, a da se pritom ne propisuju jasni kriterijumi.** Nacrt dodatno u stavu 5 utvrđuje obavezu primaoca da u roku od 24 časa dostavi pismeno obrazloženje, ali u kaznenim odredbama ne predviđa sankciju ukoliko primalac ovu obavezu ne ispuni.

Posebno je problematično omogućavanje pristupa podacima bez pismenog zahteva a „u cilju zaštite nacionalne bezbednosti, odbrane ili sprečavanja, otkrivanja i gonjenja učinilaca krivičnih dela u skladu sa odredbama posebnog zakona“ (stav 2). Budući da je problematično sa stanovišta ustavnih normi zaštite podataka o ličnosti, te da se u obrazloženju uopšte ne spominje ovaj izuzetak, nije jasan *ratio* za njegovo predlaganje. Nejasno je i koji se „poseban zakon“ ovim stavom predviđa, odnosno da li neki od važećih zakona reguliše ovaj izuzetak ili će se time baviti neki zakon koji će tek biti usvojen. Na ovaj način se otvara prostor za pravni vakuum i narušava princip predvidljivosti i izvesnosti, što ostavlja mogućnost za zloupotrebe i povećanje nepoverenja koje građani imaju u državne organe.

Pritom, **Nacrt zakona izostavlja napomenu o alternativnom, odnosno usmenom obliku zahteva**, pa se iz ovog stava može zaključiti da nikakav zahtev u predviđenim okolnostima nije ni potreban, već da se od rukovaoca – na primer, telefonskog ili Internet operatora – očekuje samo registrovanje pristupa podacima o ličnosti.

Sa stanovišta prava i sloboda građana, **neprihvatljivo je da državni organi poseduju mehanizam za prikupljanje informacija o najintimnijim detaljima njihovog privatnog života, a u pojedinim okolnostima i bez njihovog znanja.** Naime, iako u ovom slučaju rukovalac vodi evidenciju o pristupu (stav 2), podaci iz ove evidencije mogu ostati skriveni za lice čiji se podaci traže u neodređenom vremenskom periodu (stav 6).

Za razliku od tajnosti pisama i drugih sredstava komuniciranja, od čije se nepovredivosti može odstupiti samo na osnovu sudske odluke, Ustav ne pruža ovu vrstu garancije zaštiti podataka o ličnosti, prepuštajući zakonu da uredi način upotrebe podataka kojim se narušava privatnost građana.

Predloženi Nacrt, međutim, ne precizira ovlašćenja podnosioca pisanog ili usmenog zahteva za pristup privatnim podacima, odnosno njihovo ustupanje, vrstu podataka koje je u pojedinim slučajevima opravdano učiniti dostupnim, vremensko ograničenje dostupnosti podataka, kao ni rukovanje odnosno brisanje podataka pošto su prestale posebne okolnosti koje su omogućile njihovo ustupanje bez saglasnosti.

S obzirom na to da podaci o ličnosti, osim urođenih, porodičnih i socio-kulturoloških karakteristika i drugih beležaka o životu, obuhvataju i automatski generisane podatke o kretanju osobe u fizičkom i virtuelnom prostoru, predloženi Nacrt u ovom delu propušta da obezbedi odgovarajuću pravnu zaštitu građanima, kako od arbitrarnog tumačenja koncepta nacionalne bezbednosti ili opravdanih mera za „sprečavanje“ krivičnih dela, tako i od zloupotreba ličnih podataka u komercijalne svrhe.



Poslednje istraživanje SHARE Fondacije<sup>21</sup> o prikupljanju, obradi i zloupotrebama metapodataka, odnosno automatski generisanih zabeleški o aktivnostima korisnika, nedvosmisleno ukazuje na značaj odgovarajuće pravne zaštite podataka.

- **Član 24 - Naknada štete**

U stavu 4 propisano je da se rukovalac, odnosno obrađivač, može osloboditi odgovornosti za naknadu štete ukoliko dokaže da je postupao u skladu sa ovim zakonom. **Ovim pravilom se odstupa od opštih pravila deliktne odgovornosti i naknade štete** iz člana 154 Zakona o obligacionim odnosima: „*Ko drugome prouzrokuje štetu dužan je naknaditi je, ukoliko ne dokaže da je šteta nastala bez njegove krivice*“, pravila po kome bi rukovalac morao da dokaže da je šteta nastala bez njegove krivice, što je značajno viši standard od postupanja u skladu sa zakonom.

U praksi to znači da bi rukovalac dokazivanjem da je preduzeo sve mere predviđene zakonom prebacio teret dokazivanja na oštećenog da dokaže da je došlo do povrede zakona. Time bi oštećeni došao u izuzetno tešku poziciju da mora da prikupi dokaze o poslovanju rukovaoca i njegove organizacije, kako bi uspostavio odgovornost od koje se rukovalac ne može osloboditi. Uzimajući u obzir da su rukovaoci najmoćnije državne organizacije i korporacije, čini se da običan pojedinac ne bi imao mnogo izgleda za uspeh. Ovo može biti posebno problematično u situaciji ako hakerskim napadom budu ugroženi obimni podaci koje neka velika kompanija radi svog poslovanja prikuplja o pojedincima. U takvoj situaciji bi građani čija je intima postala javna potencijalno bili obespravljeni u zahtevu za naknadu štete.

Ostavljanje ovako širokog prostora za oslobođenje od odgovornosti, bez jasnog definisanja na koji način se dokazuje i na koji način se može tumačiti postupanje u skladu sa zakonom, predstavlja veliku pravnu nesigurnost.

- **Član 31 - Postupanje po zahtevu za ostvarivanje prava lica**

Za razliku od važećeg zakona kojim je za rukovaoca predviđen rok od 30 dana samo za postupanje po zahtevu za uvid ili izdavanje kopije, Nacrtom zakona ovakav rok se utvrđuje i kada rukovaoci postupaju po zahtevu za ostvarivanje prava na obaveštenje, što odstupa od trenutnog rešenja koje iznosi svega 15 dana.

Iako uvažavamo da u određenim situacijama rukovalac mora uložiti više vremena za postupanje po zahtevu za obaveštenje, smatramo da **predloženo rešenje (rok od 30 dana) može negativno uticati na ostvarivanje prava iz ovog zakona**. Prema istraživanju koje je organizacija Partneri za demokratske promene Srbija (Partneri Srbija) sproveda u cilju analize

---

<sup>21</sup> SHARE Labs: Metadata Investigation - Inside Hacking Team, oktobar 2015. Dostupno na: <http://labs.rs/en/metadata/>

primene Zakona o zaštiti podataka o ličnosti<sup>22</sup>, utvrđeno je da su po upućenom Zahtevu za obaveštenje rukovaoci mahom postupali u roku koji je utvrđen zakonom. Iako uvažavamo da drugi subjekti mogu imati drugačija iskustva, ukazujemo da je rešenje iz postojećeg zakona od 15 dana odgovarajuće, imajući u vidu da rukovalac ima pravo da u postojanju opravdanih okolnosti ovaj rok produži za još 30 dana.

U prilog ovom stavu ide i novina iz Nacrta zakona koja za nezanemarljiv krug rukovalaca predviđa obavezu donošenja opšteg akta o zaštiti podataka i određivanja lica za zaštitu podataka, kao i nadležnosti ovog lica. Ovakva rešenja upravo su i izrađena kako bi rukovaoci izgradili interne kapacitete i procedure za postupanje po upućenim zahtevima, te se može očekivati da će oni biti u stanju da postupaju i u vremenskim okvirima utvrđenim postojećim zakonom.

Poverenik i akteri civilnog sektora učestalo ukazuju da je neophodno stimulisati građane da se aktivno uključe u ostvarivanje svojih prava iz oblasti zaštite podataka o ličnosti, i to iz najmanje dva razloga. Prvi je to što građani nemaju dovoljno informacija o načinu na koji rukovaoci obrađuju podatke o njima, te da bi korišćenjem prava iz Zakona stekli takve informacije i posredno unapredili svest o značaju prava na privatnost. Drugi jednako važan razlog odnosi se na uočenu pojavu da brojni rukovaoci postaju svesni sopstvenih obaveza iz Zakona tek nakon što im građanin uputi zahtev za obaveštenje. **Zato smatramo da bi produženje roka za ostvarivanje ovakvog bazičnog prava negativno uticalo na građane i njihovu motivaciju da zatraže informaciju o obradi podataka o njima**, čime bi se posredno umanjio željeni efekat u pogledu povećanja svesti rukovalaca o neophodnosti zaštite podataka.

- **Članovi 40 i 41 – Zaštita prava lica**

Članom 40 Nacrta zakona utvrđuje se različit postupak zaštite prava u zavisnosti od toga da li je rukovalac organ javne vlasti. Žalba se izjavljuje u odnosu na postupanje organa javne vlasti, dok se u odnosu na postupanje drugih rukovalaca izjavljuje pritužba. Konkretno, **predloženo rešenje može stvoriti konfuziju kod građana koji žele da zaštite prava pred Poverenikom**, budući da oni ponekad ne znaju razliku između dve vrste pravnih subjekata. Ovo se naročito može odnositi na subjekte koji nisu organi javne vlasti, ali su uključeni u javno-privatna partnerstva ili su im poverena javna ovlašćenja, zatim na tzv. tradicionalna udruženja građana, sportske saveze, privredna društva čiji je osnivač delimično ili u celosti organ javne vlasti, i sl. Iz tog razloga, Poverenik će biti prinuđen da odbaci žalbu ukoliko je trebalo izjaviti pritužbu, i obrnuto. Ovakva praksa može imati dve negativne posledice. Prva se odnosi na dodatno usporavanje procesa zaštite prava. Druga se odnosi na potencijalno obeshrabrivanje građana da preduzmu naredni korak u cilju zaštite prava, izjavljivanjem pritužbe umesto žalbe (ili obrnuto) u novom postupku pred Poverenikom.

---

<sup>22</sup> Partneri za demokratske promene Srbija, Zaštita privatnosti u Srbiji – Analiza primene Zakona o zaštiti podataka o ličnosti. Dostupno na:  
<http://www.partners-serbia.org/zastita-privatnosti-u-srbiji-analiza-primene-zakona-o-zastiti-podataka-o-licnosti/>

Član 41 Nacrta zakona utvrđuje rok za postupanje Poverenika po žalbi, odnosno pritužbi. Za razliku od odredbe važećeg zakona koja nalaže da Poverenik postupi po žalbi u roku od 30 dana (član 39, stav 1), Nacrt predviđa znatno duži rok od 60 dana.

Smatramo da **ovakva promena, zajedno sa promenom predloženom članom 31 može negativno uticati na angažovanje građana u cilju ostvarivanja prava na zaštitu podataka o ličnosti**, a time i na opšte stanje u ovoj oblasti u Srbiji, iz razloga koji su ranije navedeni.

Ukoliko je navedeno rešenje iz člana 41 izrađeno zbog nedovoljnih resursa kojima Poverenik raspolaže, smatramo da je bilo bolje zadržati postojeće rešenje, a istovremeno obezbediti dodatna sredstva kojima bi resursi Poverenika bili dovedeni na odgovarajući nivo. Ovakvo rešenje bi bilo u skladu sa Akcionim planom za poglavlje 23 koji predviđa jačanje kadrovskih kapaciteta Poverenika. Na problem nedovoljnih resursa iz godine u godinu ukazuje se u izveštajima Evropske komisije o napretku Srbije i godišnjim izveštajima Poverenika-<sup>23</sup> Nedavno je na ovaj problem ukazao Poverenik, informišući javnost da je, na osnovu „za sada poznatih projekcija Budžeta za 2016. godinu [...] planirani fond za plate zaposlenih u službi Poverenika za skoro 30% manji od fonda koji je Poverenik imao na raspolaganju tokom 2015. godine.“<sup>24</sup> Čini se da predloženo rešenje legitimizuje dugogodišnji problem limitiranih resursa koji (ni)su Povereniku stavljeni na raspolaganje, a sve na štetu građana, odnosno ostvarivanja njihovih prava.

Sveukupno, kada se predložena rešenja iz Nacrta zakona uporede sa rešenjima iz važećeg zakona, može se zaključiti da predložena rešenja dovode to znatno dužeg procesa ostvarivanja i zaštite prava.

|  | Važeći zakon | Nacrt zakona |
|--|--------------|--------------|
| Rok za postupanje po zahtevu za obaveštenje o obradi         | 15 + 30      | 30 + 30      |
| Rok za postupanje po zahtevu za uvid ili izdavanje kopije    | 30 + 30      | 30 + 30      |
| Rok za postupanje Poverenika po žalbi (ili pritužbi - Nacrt) | 30           | 60           |
| Ukupno   | 75 – 135     | 120 - 180    |

<sup>23</sup> Na primer, Godišnji izveštaj Poverenika za 2014. godinu, str. 80. Dostupno na:

<http://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2015/latg.izvestaj2014.pdf>

<sup>24</sup> Videti: <http://www.poverenik.rs/you/saopštenja-i-aktuelnosti/2230-kreatori-budzeta-neprincipijelno-a-radikalno-pogorsavaju-uslove-za-funkcionisanje-poverenika.html>

- **Član 44 - Suspeživno dejstvo pokretanja upravnog spora**

Neophodno je osvrnuti se i na član 44 Nacrta koji u stavu 2 predviđa da pokretanje upravnog spora odlaže izvršenje rešenja Poverenika. Ukoliko imamo na umu da su rešenja Poverenika obavezujuća, konačna i izvršna, a da je članom 23 Zakona o upravnim sporovima („Sl. glasnik RS“, br 111/2009) u stavu 1 navedeno da tužba, po pravilu, ne odlaže izvršenje upravnog akta protiv koga je podneta, tj. da se samo u izuzetnim situacijama odlaže izvršenje upravnog akta, ovakvo rešenje bi dodatno ugrozilo nezavisnost institucije Poverenika.

- **Član 45 - Ostale odredbe postupka**

Nactrom zakona u članu 45 predviđeno je da se na postupak odlučivanja Poverenika primenjuju odredbe zakona kojima se uređuje opšti upravni postupak, dok se izvršenje rešenja Poverenika sprovodi u skladu sa zakonom koji uređuje izvršenje i obezbeđenje. Nejasno je zbog čega se Radna grupa prilikom izrade Nacrta zakona opredelila za ovakvo rešenje, tj. zbog čega se za izvršenje rešenja donetih u upravnom postupku primenjuju odredbe Zakona o izvršenju i obezbeđenju pošto se ovim Zakonom uređuje postupak prinudnog ostvarivanja potraživanja i obezbeđivanja potraživanja na osnovu izvršne isprave. U članu 13 stav 1 tačka 2 Zakon o izvršenju i obezbeđenju („Sl. glasnik RS“, br. 31/2011, 99/2011 - dr. zakon, 109/2013 - odluka US, 55/2014 i 139/2014) navodi se da izvršna isprava može biti pravnosnažna odluka doneta u upravnom postupku, ali ako glasi na ispunjenje novčane obaveze i ako posebnim zakonom nije drugačije određeno. Uzmimo za primer da je rukovalac (podacima) rešenjem odbio zahtev podnosioca za ostvarivanje prava na uvid podataka koji se na njega odnose. Podnosilac može podneti žalbu na rešenje rukovaoca Povereniku kao drugostepenom organu koji, ukoliko utvrdi da je zahtev osnovan, rešenjem nalaže rukovaocu da po njemu postupi. Navedeni primer se nikako ne može podvesti pod odredbe Zakona o izvršenju i obezbeđenju zato što rešenje Poverenika ne glasi na novčanu obavezu (rukovalac i podnosilac zahteva nisu u obligaciono-pravnom odnosu), već se njime nalaže rukovaocu da obezbedi uvid u podatke podnosiocu zahteva. Pritom, treba imati u vidu da je Zakonom o opštem upravnom postupku („Sl. list SRJ“, br. 33/97 I 31/2001 I „Sl. glasnik RS“, br. 30/2010) regulisan postupak administrativnog izvršenja, odnosno izvršenja radi ispunjenja nenovčanih obaveza.

- **Članovi 48-50 - Bezbednost podataka**

U članu 48, stavu 2, propisane su mere bezbednosti, gde se u tački 1 propisuje zaštita prostorija, opreme i sistemske programske opreme, uključujući i ulazno-izlazne jedinice. Zbog značaja uloge (čuvanje podataka), potrebno je dodati i jedinice za skladištenje podataka.

Dalje, u stavu 2, tačka 2, propisuje se zaštita baza podataka i programskih aplikacija sprečavanjem neovlašćenog pristupa podacima tokom prosleđivanja podataka, uključujući prosleđivanje putem elektronskih komunikacionih mreža. Zbog stepena rizika, trebalo bi dodati i sprečavanje neovlašćenog pristupa podacima tokom čuvanja (skladištenja), a ne samo tokom

prosleđivanja. Takođe, zbog specifičnosti uloge smatramo da pored prosleđivanja putem elektronskih komunikacionih mreža, treba navesti i prosleđivanje putem prenosnih medijuma (CD, DVD, USB fleš memorije, eksterni hard diskovi i sl). Neophodno je dodatno definisati i da se prosleđivanje putem elektronskih komunikacionih mreža može obavljati samo kada je sadržaj prilikom prosleđivanja šifriran (enkriptovan).

U stavu 2, tačka 4, definiše se obezbeđivanje mogućnosti da se naknadno utvrdi obrađivač, vreme i mesto obrade, kao i radnja obrade u roku u kojem je zakonom propisano ostvarivanje i zaštita prava lica. Na ovom mestu **potrebno je definisati najkraći rok čuvanja podataka koji omogućava da se naknadno utvrdi obrađivač, vreme i mesto obrade, kao i radnja obrade**, a koji neće biti kraći od 6 meseci. Naime, neovlašćene radnje često se detektuju relativno kasno u odnosu na period kad su se dogodile, te ovi podaci predstavljaju glavni dokazni materijal koji dokazuje neovlašćenje radnje.

U stavu 2, tačka 5, predviđa se obuka zaposlenih na poslovima obrade, kao i organizovanje poslova obrade na način koji obezbeđuje pristup podacima samo ovlašćenim licima. Potrebno je **preciznije definisati obaveze obuke, utvrditi standard, te ustanoviti obavezu praćenja uspešnosti obuke** za svakog zaposlenog, što bi predstavljalo kriterijum za zaposlenje na radnom mestu koje podrazumeva rad sa podacima o ličnosti.

U članu 48, stav 3, navodi se da se mere bezbednosti primenjuju u skladu sa Zakonom o informacionoj bezbednosti, koji u Republici Srbiji nije na snazi. Odredba na taj način dovodi do pravne nesigurnosti, s obzirom da trenutno ne postoji zakon kojim se bliže uređuje ovo pitanje.

Smatramo da zakonom treba predvideti dodatne mere koje propisuje Poverenik za rukovaoce podacima koji obrađuju podatke za veći broj lica (više od 500 lica) i za rukovaoce koji obrađuju posebne podatke o ličnosti. Pored mera koje predlaže Poverenik, ovi rukovaoci bi trebalo da usvoje poseban program za zaštitu bezbednosti podataka na osnovu izvršene procene rizika po prava lica čiji se podaci obrađuju. Takođe, posebne podatke o ličnosti tokom obrađivanja potrebno je posebno obeležiti i zaštititi, kako bi se sprečio neovlašćeni pristup.

U članu 50, stav 1, definiše se procena rizika ako bi zbog prirode, načina, odnosno cilja obrade moglo da dođe do povrede prava, slobode ili zaštićenog interesa. U ovom stavu bi trebalo precizirati ko može vršiti procenu rizika u smislu da bi to mogla da budu samo lica koja imaju određena znanja za ovu procenu, kao i kakva je odgovornost lica koja su izvršila procenu ukoliko se ispostavi da procena rizika nije izvršena profesionalno i s dužnom pažnjom.

U članu 50, stav 5, iz obaveza propisanih u stavu 1 i 3 ovog člana (Procena rizika i mišljenje lica na koja se akt o proceni rizika odnosi) izuzumaju se rukovaoci koji su organi vlasti, a koji obrađuju podatke na osnovu zakonskog ovlašćenja. Smatramo da s obzirom na to da se radi o specifičnim situacijama koje su definisane u stavu 1, tačka 1-6 ovog člana, u kojima obrada može imati ozbiljne posledice, kako što je propisano u članu 49, stav 1 ovog Nacrta zakona, **ne**



**postoji legitiman razlog da bilo ko bude izuzet od ovih obaveza, a posebno organi vlasti kao značajni rukovaoci koje obrađuju veliki broj podataka o ličnosti.**

- **Član 52 - Određivanje lica za zaštitu podataka**

Utvrđivanje obaveze za određene rukovaoce da odrede lica za obavljanje poslova zaštite podataka smatramo kao izuzetno dobru novinu koja je regulisana članom 52 Nacrta zakona. Ipak, smatramo da **kriterijum da to lice mora imati „odgovarajuće stručno znanje neophodno za obavljanje poslova zaštite podataka“ nije adekvatan i suviše je neodređen.** Postavlja se pitanje šta bi u konkretnom slučaju to značilo, naročito imajući u vidu da u Srbiji ne postoji obrazovna ustanova koja konkretno obrađuje ovo pitanje, te da ne postoji stručni profil koji bi ova znanja posedovao. Stoga, postojanje ovog pravnog standarda u samom Nacrtu zakona zapravo ništa ne znači.

**Smatramo da bi određeni vid obuke i sertifikacije morao da postoji,** što je i regulisano u Modelu Poverenika u članovima 64, 66 i 67. Imajući u vidu da prema proceni Poverenika u Srbiji ima oko 350 000 pravnih lica koja prikupljaju podatke o ličnosti, ovo pitanje se mora na adekvatan način regulisati, naročito imajući u vidu iskustvo sa Zakonom o privatnom obezbeđenju koji je usvojen još 2013. godine, ali obuka oko 40 000 lica, koliko je procenjeno da ima lica koja se bave privatnim obezbeđenjem, i dalje nije sprovedena, te je rok za sprovođenje iste produžen za još godinu dana, dakle ukupno 3 godine od usvajanja Zakona. Imajući u vidu ove probleme smatramo da bi se Nacrtom zakona moralo regulisati donošenje podzakonskog akta kojim će se urediti odgovarajuće stručno znanje koje će se sticati kroz obuku i verifikaciju od strane kompetentnog organa, rok za donošenje ovog akta (najduže 6 meseci), rok za završetak procesa obuke i sertifikacije, te visinu troškova obuke i verifikacije, kao i označavanje lica koja snose te troškove, u skladu sa članom 49 Zakona o radu.

Takođe, ni na koji način **nije regulisana odgovornost lica zaštitu podataka u slučaju da ne obavlja svoje poslove u skladu sa obavezama** koje su propisane Nacrtom zakona, što smatramo da je izuzetno bitno imajući u vidu ogromnu odgovornost koju ovo lice ima. Pored novčane i prekršajne sankcije, u slučaju postojanja sertifikata sankcija bi mogla biti i oduzimanje istog.

- **Članovi 59 i 60 - Iznošenje podataka iz Republike Srbije**

Smatramo da pored uslova za iznošenje podataka koji su navedeni u članu 59 stav 1, a u cilju fleksibilnijeg regulisanja ove promenljive oblasti, ali i osiguravanja sveobuhvatne zaštite podataka prilikom njihovog iznošenja i razmene, treba dodati da se podaci o ličnosti mogu iznositi u države ili međunarodne organizacije koje imaju odgovarajuće uređenu zaštitu podataka o ličnosti, kako je i predloženo u Modelu Poverenika, a propisano Direktivom i Predlogom uredbe. Jednako je važno precizno definisati koje države ispunjavaju uslov adekvatno uređene zaštite podataka o ličnosti, te smatramo da je predlog iz člana 74, stav 3 Modela Poverenika da to svakako budu države članice Evropske unije i države ili međunarodne

organizacije za koje je Evropska unija utvrdila da imaju odgovarajuće uređenu zaštitu podataka o ličnosti, sasvim zadovoljavajući, pre svega iz razloga visokog nivoa svesti institucija Evropske unije po ovom pitanju, ali i zbog toga što bi to bio korak kojim usklađujemo naše zakonodavstvo sa pravnim okvirom Evropske unije.

Dok postojećim Zakonom o zaštiti podataka o ličnosti Poverenik utvrđuje da li su ispunjeni uslovi i sprovedene mere zaštite podataka prilikom njihovog iznošenja iz zemlje, ta uloga mu je Nacrtom zakona oduzeta, što može biti problematično u slučajevima iznošenja podataka u države ili međunarodne organizacije koje ne spadaju u navedene kategorije i za koje nije utvrđeno da garantuju odgovarajuće uređenu zaštitu podataka. Smatramo da **Poverenik mora imati ključnu ulogu u ovakvim slučajevima i smatramo neophodnim uvođenje odgovarajućih mera zaštite podataka, koje je važno jasno definisati novim zakonom** i čije bi sprovođenje bilo u nadležnosti Poverenika. Ove mere zaštite bi se sprovodile u precizno utvrđenom postupku odlučivanja Poverenika po zahtevu rukovodca za iznošenje podataka. Na ovaj način bi Poverenik utvrđivao rizike po bezbednost podataka čije se iznošenje namerava i u skladu sa njima odobravao ili odbijao zahteve.

Takođe, smatramo da predloženi postupak, definisan članom 76 u Modelu Poverenika, ispunjava uslove i sprovodi adekvatne mere zaštite podataka prilikom iznošenja iz zemlje, i tako prati načela propisana Direktivom i Predlogom uredbe EU, kao što su utvrđivanje da li je propisom ili na osnovu ugovora o prenosu podataka, država ili međunarodna organizacija u koju se zahteva iznošenje podataka obezbedila odgovarajući stepen zaštite podataka; sprovođenje postupka nadzora nad rukovodcem koji je podneo zahtev radi potpunog utvrđivanja činjeničnog stanja.

Dalje, članom 60 uređuju se posebni slučajevi iznošenja podataka i definišu uslovi pod kojima je moguće da podaci budu izneti u države i međunarodne organizacije koje nemaju odgovarajuće uređenu zaštitu podataka i bez sprovođenja odgovarajućih mera zaštite podataka. Određene uslove je neophodno dodatno definisati. Stav 1, tačka 1, dozvoljava iznošenje podataka ukoliko je lice na nesumnjiv način izrazilo saglasnost za iznošenje podataka. **Smatramo da je potrebno dodati da lice daje saglasnost nakon što je obavešteno o rizicima** iznošenja podataka zbog odsustva odgovarajućih mera zaštite podataka i adekvatno uređene zaštite podataka u predmetnoj državi.

U članu 60, stav 1, tačka 5, propisano je da se mogu izneti podaci iz javnog registra koji su dostupni svima, odnosno licu koje u konkretnom slučaju ima opravdan interes da do njih dođe. Potrebno je dodatno definisati da u ovom slučaju iznošenje podataka ne obuhvata sve podatke o ličnosti ili celokupne kategorije podataka o ličnosti sadržanih u registru, kao i da se iznošenje podataka koji su dostupni licima koja imaju opravdan interes izvršava isključivo na zahtev tih lica ili ukoliko su oni budući primaoci.

Članom 60, stav 2, predviđeno je da rukovodac bez odlaganja obaveštava Poverenika i lice na koje se podaci odnose da su podaci izneti iz Republike Srbije. Sama uloga Poverenika, koja se

prevashodno sastoji u tome da obezbeđuje zaštitu podataka o ličnosti, na ovaj način se negira, budući da je obaveštavanje predviđeno tek nakon što su podaci izneti iz zemlje. Bez obzira na to što posebni slučajevi iznošenja podataka ne zahtevaju prethodnu odluku Poverenika kojom se ono odobrava, predlažemo mogućnost podnošenja zahteva Povereniku i u ovim slučajevima, kako bi sve odgovarajuće mere za zaštitu podataka bile preduzete i obezbeđene.

## **-Zaključak-**

Imajući u vidu da je Strategija zaštite podataka o ličnosti<sup>25</sup> usvojena još 2010. godine, a da Akcioni plan za sprovođenje te Strategije nikada nije donet, iako je to bila obaveza Vlade, smatramo da je potrebno u najkraćem roku doneti novu Strategiju koja će odgovoriti na izazove digitalnog društva, posebne vidove obrade, kao i ostale probleme obrade podataka o ličnosti u modernom društvu koje smo izneli u komentarima. Nakon toga bi bez odlaganja trebalo doneti i Akcioni plan za sprovođenje Strategije. Takođe, Strategijom i Akcionim planom je potrebno predvideti ulaganja u obrazovanje radi boljeg razumevanja zaštite podataka o ličnosti svih aktera na koje se Zakon odnosi, kako rukovalaca i obrađivača, tako i samih građana, kao i ulaganja koja su potrebna za bolju implementaciju temeljnih načela Zakona.

Predloženi Nacrt zakona o zaštiti podataka o ličnosti sadrži niz nejasnih odredbi kojima se javnim i privatnim akterima ostavljaju široka i proizvoljna ovlašćenja u pristupu ličnim podacima građana, bez odgovarajuće kontrole. Takođe, pojedina načela ali i konkretna rešenja uspostavljena predloženim Nacrtom praktično su neprimenjiva na Internetu, okruženju u kom se danas odvija daleko najveći segment prikupljanja i obrade podataka o ličnosti. Pored toga, predloženi Nacrt propušta da uredi neke od najvažnijih i danas najčešćih procedura prikupljanja i obrade podataka o ličnosti kao što su video-nadzor, obrada biometrijskih podataka, direktan marketing i slično. Sve to čini da Nacrt zakona ne predstavlja nikakav napredak u regulisanju ove dinamične oblasti, unosi pravnu nesigurnost, snižava već usvojene standarde zaštite, te se postavlja pitanje njegovog donošenja u ovom obliku.

Zbog konkretnih propusta opisanih u komentarima, kao i odsustva adekvatne i za ovako važan zakon primerene javne rasprave, stava smo da je Nacrt zakona potrebno **vratiti na doradu** kako bi se pored otklanjanja opisanih nedostataka, pravno uredile oblasti koje su izostavljene.

---

<sup>25</sup> Strategija zaštite podataka o ličnosti („Službeni glasnik RS”, br. 58/2010 od 20.08.2010. godine): <http://www.poverenik.rs/yu/pravni-okvir-zp/podzakonski-akti-zp/942-strategija-zastite-podataka-o-licnosti.html>