



ANALIZA RADA AGENCIJE ZA ZAŠTITU OSOBNIH PODATAKA

Politiscope, veljača 2021.

UVOD

U odgovoru na izazove četvrte tehnološke revolucije Europska unija je nadogradila svoje unutarnje tržište kreiranjem zajedničkog europskog prostora prikupljanja i obrade podataka. Globalno liderstvo Europe u zaštiti privatnosti i digitalnih prava građana od velikih IT kompanija, dijelom je bilo potaknuto željom za kreiranjem novih poticaja za razvoj europske digitalne ekonomije. Europski decentralizirani institucionalni okvir zaštite digitalnih prava saždan je na mreži nacionalnih nadzornih tijela u svakoj od država članica EU. Nadzorna tijela za zaštitu podataka su samostalne i neovisne institucije čija je temeljna zadaća osigurati legalnu i legitimnu obradu podataka te tako štititi privatnost i digitalna prava građana. Agencija za zaštitu osobnih podataka provodi nadzor nad prikupljanjem i obradom podataka građana RH, kao i državljana EU čiji podaci se prikupljaju i obrađuju u Hrvatskoj.

Ova kratka analiza usmjerena je na ocjenu rada Agencije za zaštitu osobnih podataka (dalje u tekstu: AZOP), s nekoliko ključnih fokusa analize: samostalnost i neovisnost institucije, uloga u COVID pandemiji, kapacitiranost za nadzor suvremenih tehnoloških praksi prikupljanja i obrade podataka, manjkavosti Zakona o provedbi Opće uredbe o zaštiti podataka. Analiza je namijenjena donositeljima odluka u izvršnoj vlasti koji putem kadrovskih odluka ostvaruju utjecaj na rad Agencije, zastupnicima Hrvatskog sabora koji usvajaju kadrovske odluke Vlade i provode nadzor nad radom Agencije te medijima i široj javnosti pred kojima nositelji javnih funkcija u institucijama koje štite digitalna prava polažu račune za vlastiti rad. Analiza sadrži preporuke za poboljšanje zakonodavnog i institucionalnog okvira za zaštitu osobnih podataka.



NESAMOSTALNOST I OVISNOST SAMOSTALNE I NEOVISNE INSTITUCIJE

Netom pred izbore, na posljednji dan sjednice i tadašnjeg saziva, [Hrvatski sabor prihvatio je Vladin prijedlog](#) te za ravnatelja Agencije imenovao izvjesnog Zdravka Vukića. Iako je ovo imenovanje ostalo zapamćeno zbog bizarnog hobija gospodina Vukića (trećerazredni avanturistički romani o hrvatskom tajnom agentu [Borni Vitezu](#)), daleko je više problematična njegova bliska povezanost s vladajućom strankom te potpuni izostanak relevantnog profesionalnog iskustva, zbog čega ne ispunjava minimalne zakonske uvjete. Bio je ukupno član čak četiri političke stranke, a na čelo institucije koja bi trebala biti samostalna i neovisna, dolazi kao [HDZ-ov](#) pomoćnik ministra graditeljstva. Jedino relevantno Vukićevo radno iskustvo je obavljanje pravnih poslova u tvrtki Cesting, koja se bavila održavanjem lokalnih i državnih cesta te je bila česti gost novinskih članaka koji se bave [korupcijom](#) u [Slavoniji](#). Zbog toga što njegove osobne povezanosti stvaraju percepciju ovisnosti neovisne institucije o Vladi RH i stranci HDZ, Zdravko Vukić se nalazi u trajnom sukobu interesa koji urušava povjerenje građana i javnosti. Dodatno tome, padu javnog ugleda doprinosi činjenica da je Vukić imenovan za ravnatelja iako ne ispunjava minimalne zakonom propisane uvjete – Vukić nema adekvatno stručno znanje te nije prepoznati stručnjak u području zaštite podataka.

Zbog Vukićeva imenovanja, Politiscope je pred Europskom komisijom [pokrenuo postupak protiv RH zbog kršenja prava EU](#). Komisija je prigovor odbila navodeći da imenovanje gospodina Vukića ne predstavlja kršenje Opće uredbe o zaštiti podataka (dalje u tekstu: Uredba), istaknuvši pritom da svaka država-članica samostalno definira kriterije imenovanja. Dodatno tome, osvrćući se na navode prigovora da Vukić ne ispunjava zakonske uvjete jer nije [„istaknuti stručnjak s priznatim profesionalnim ugledom“](#), Komisija je istaknula kako se ne može očitovati o eventualnim kršenjima odredbi nacionalnih propisa. Imajući na umu da je rasap vladavine prava na istoku Europske unije jedan od akutnih političkih problema, Politiscope je o urušavanju neovisnosti Agencije izvijestio Europski parlament i Europski odbor za zaštitu podataka. Politiscope je predložio izdavanje preporuka o uvođenju *cooling-off* perioda za ravnatelje europskih nadzornih tijela za zaštitu podataka, odnosno uvođenje obveznog minimalnog vremenskog perioda političke neaktivnosti prethodno kandidiranju za funkciju ravnatelja tijela.

Nekoliko je kritičnih slučajeva koji ukazuju na zaključak kako se ne radi samo o slučaju permanentnog sukoba interesa ravnatelja koji urušava javni ugled institucije, već i o slučaju stvarne ovisnosti i podređenosti neovisne institucije izvršnoj grani vlasti. Većina spornih slučajeva je izložena u dijelu analize koji razmatra ulogu AZOP-a u pandemijskom prikupljanju i obradi podataka: digitalni asistent Andrija, STOP-COVID aplikacija, slučaj Badrić-Beroš,

nereagirane na nelegalnost pandemijskih praksi obrade podataka. Slučajevi ukazuju na zaključak da se AZOP nalazi u neprimjerenom podređenom odnosu prema Vladi RH.

PANDEMIJA POLTRONSTVA

Imajući na umu sklonost autoritarnih režima i režima defektnih demokracija u korištenju digitalnih oblika nadzora građana, pandemija Corona virusa je prepoznata kao realna opasnost za privatnost građana i liberalnu demokraciju. S tim ciljem, **Europska komisija je izdala preporuku** državama članicama o provođenju konzultacija s nacionalnim nadzornim tijelima prilikom uspostave novih praksi prikupljanja i obrade podataka izazvane potrebom uspješnog upravljanja pandemijom, posebice kod razvoja digitalnih rješenja s ciljem zaštite javnog zdravlja. Upravo se kroz Vladino ignoriranje i izigravanje ove preporuke, odnosno kroz ignoriranje i neuključenje nadzornog tijela, razotkriva podređeni položaj AZOP-a. Tako je Vlada, bez uključenja AZOP-a, pokrenula digitalnog asistenta Andriju, **propustivši pritom objaviti politiku privatnosti**, čime je prekršila osnovne odredbe i načela Uredbe. No, i naknadno objavljena Politika privatnosti je imala ozbiljnih propusta – između ostalog, prikupljala se prekomjerna količina podataka (poput broja mobitela) te je korištena platforma tvrtke obilježene skandalima vezanima uz privatnost (Whatsapp, Facebook).

Prilikom lansiranja Stop COVID-19 aplikacije izbjegnuto je ponavljanje iste greške potpunog ignoriranja AZOP-a te je ovog puta održan radni sastanak između predstavnika AZOP-a i Vlade RH. Taj sastanak održao se jedan tjedan prije javnog pokretanja aplikacije, pred same parlamentarne izbore. Tada negdje, prije izbora, je bio i posljednji put kada su nositelji javnih funkcija isticali aplikaciju kao vrijedan alat upravljanja pandemijom. AZOP je izdao **priopćenje o održanom sastanku**, u kojem je propustio iznijeti jasan stav o aplikaciji iz perspektive zaštite privatnosti i osobnih podataka građana. Android verzije aplikacija, izrađene na temelju Google-Apple API, imaju značajnih propusta u zaštiti privatnosti, što se smatra jednim od bitnih objašnjenja za niske razine korištenja aplikacija u Europskoj uniji. Naime, velikom broju potencijalnih korisnika postalo je jasno kako je Google podbacio u svom obećanju potpune zaštite privatnosti korisnika. Svega mjesec i pol dana nakon navedenog sastanka AZOP-a i Vlade, nadzorno tijelo Nizozemske je **svojoj vladi savjetovalo** da se aplikacija ne koristi sve dok se ne odstrane sve zabrinutosti o nedovoljnoj zaštiti privatnosti korisnika.

Vili Beroš je bio primoran raditi kontrolu štete nakon što su u javnost dospjele fotografije s privatne zabave, na kojima se ministar zdravlja ne pridržava pravila socijalne distance, izdanih od Hrvatskog zavoda za javno zdravstvo. Posebnu pažnju javnosti dobila je slika Beroša i Nine Badrić jer su mediji raspolagali informacijom da je pjevačica bila u kontaktu s Covid pozitivnom osobom. S ciljem zaštite osobne reputacije, ministar je u intervju za **N1 televiziju** izjavio da nitko od sudionika privatne zabave nije pozitivan, uključujući poznatu pjevačicu

Ninu Badrić. Beroš je pritom javnost upoznao s činjenicom da je informacije dobio u telefonskom razgovoru s epidemiologinjom Hrvatskog zavoda za javno zdravstvo. Svrha prikupljanja i obrade zdravstvenih podataka o osobama zaraženima virusom te njihovim kontaktima zasigurno nije da ministar, s ciljem umanjivanja političke štete načinjene vlastitim neodgovornim ponašanjem, telefonskim pozivom provjerava jesu li određeni pojedinci zaraženi ili ne, te onda iste informacije iznosi u javnost. Činjenica da **AZOP smatra kako navedeni postupak nije problematičan** dodatno je skandalozna te samo potvrđuje opravdanost sumnji u neovisnost tijela, koje su dodatno osnažene imenovanjem bivšeg državnog dužnosnika u Ministarstvu graditeljstva i bivšeg člana HDZ-a na mjesto ravnatelja agencije.

Izostanak ikakve proaktivnosti i agilnosti u radu AZOP-a glavni je krivac za košmarnu situaciju u kojoj su se našli saloni (frizerski, za pedikuru, manikuru, masažu), nakon što je **Hrvatski zavod za javno zdravstvo izdao upute o prikupljanju podataka klijenata**. Minimalni doprinos AZOP je mogao dati kroz objavu mišljenja u kojem se zauzima jasan stav o tome koji je točan opseg podataka koje saloni trebaju prikupljati, s kojom pravnom osnovom, kako podatke čuvati, i do kada. Većina salona je kao pravnu osnovu za obradu podataka izabrala privolu ispitanika, koju su sami tražili od klijenata prethodno uzimanju podataka. U slučaju nedavanja privole, klijentima se ne bi pružila usluga, što predstavlja kršenje osnovnih odredbi Uredbe, čime se poslovni subjekti nepotrebno izlažu riziku financijskih penala od strane AZOP-a. Način objave uputa o prikupljanju podataka za salone, koji ne uključuje detaljne informacije o zaštiti podataka, te potpuna pasivnost AZOP-a doprinijeli su uspostavljanju nelegitimne i nezakonite prakse obrade podataka. Potvrda za ovaj zaključak je došla u obliku **obrasca za prikupljanje podataka klijenata** kojeg je Obrtnička komora dostavila svim salonima, vjerojatno s ciljem da salonima olakša poslovanje i prikupljanje podataka. No, u obrascu se pogrešno navodi pravna osnova za prikupljanje podataka (privola), prikuplja se prekomjerna količina podataka (uključujući osjetljive podatke) te se ujedno povećava rizik gubitka ili otuđenja podataka (nepotrebno kreiranje fizičkih dokumenata koji sadrže osjetljive informacije klijenata). AZOP je **mišljenje s jasnim uputama** izdao tek nakon što je obrazac Obrtničke komore izazvao veliki interes, ali i negodovanje javnosti.

Ključni instrument osiguranja zaštite privatnosti građana u pandemiji je Opća uredba o zaštiti podataka. Uredba predviđa i situacije poput pandemije, u kojima postoji visok javni i društveni interes za prikupljanje i obradu podataka građana. U slučaju pandemije, prikupljanje i obrada podataka o kontaktima su opravdani svrhom zaštite javnog zdravlja. No, **recital 45. Uredbe** jasno ističe kako je u ovakvim slučajevima potrebno stvoriti zakonski okvir koji regulira prikupljanje i obradu podataka, između ostalog – svrhu i opseg prikupljanja podataka, načine zaštite, rok čuvanja, obvezu uništenja podataka. Tijekom 2020. godine pokrenute su dvije izmjene Zakona o zaštiti pučanstva od zaraznih bolesti, no iste nisu predviđale uređenje zakonskog okvira za pandemijsku obradu podataka s ciljem zaštite javnog zdravlja. Samim time, sve upute izdane od strane HZJZ-a javnim ustanovama i poslovnim subjektima, a vezane uz prikupljanje osobnih podataka korisnika njihovih usluga su – nelegalne i

nelegitimne. Naime, prikupljanje osobnih podataka građana bez privole s ciljem zaštite javnog zdravlja predstavlja ograničenje temeljnih prava te je isto potrebno urediti zasebnim zakonskim propisom, što je obveza definirana recitalima 45. i 52. Uredbe. U nereagiraju AZOP-a na navedenu situaciju još jednom se razotkriva podređeni odnos prema Vladi RH. Naime, AZOP je trebao izdati mišljenje u kojem Vladu upozorava, savjetuje ili preporuča hitno usvajanje zakonskog okvira za pandemijsko prikupljanje i obradu podataka, uz dostavu popisa svih obveznih elemenata takvog zakonskog okvira, koji su jasno definirani recitalom 45. Uredbe.

TEHNOLOŠKA POTKAPACITIRANOST



Globalni IT divovi stvorili su kapitalizam nadzora ([surveillance capitalism](#)) – ekonomski model baziran na masovnom nadzoru korisnika, u kojem se financijska vrijednost izvlači iz prodaje podataka koji nastaju kao nusprodukt korištenja digitalnih proizvoda. Iako početno kreiran s ciljem targetiranog oglašavanja, postojeći digitalni ekosustav izrastao je u sustav za promjenu ponašanja, odnosno kritičnije rečeno – sustav za manipuliranje ljudima. Algoritamska obrada osobnih podataka uključujući i podataka o online ponašanju te sustav manipuliranja izgrađen na uvjetovanju ponašanja prikrivenim sustavom nagrada i kazni, stvorio je učinkovit i izvrstan alat za promjenu ponašanja, stavova i vrijednosti. Krajnji problem ovakvog digitalnog ekosustava jest da amplificira negativne emocije i narrative. Naime, upravo sadržaji koji su natopljeni negativnim emocijama i ekstremnim narativima izazivaju bržu reakciju (*engagement*) te ih algoritam dodatno promovira, s krajnjim ciljem distribucije sadržaja koja izaziva reakcije i zadržava pažnju korisnika. Dakle, postoje sistemski poticaji za širenje lažnih vijesti, teorija urote, govora mržnje, govora nasilja, nacionalističkog i rasističkog narativa. U ovako neprijateljskom okruženju za privatnost, Uredba bi trebala stvoriti digitalni štiti koji državljane EU štiti od nelegitimnih praksi obrade podataka, koje nam sistemski pružatelji digitalnih usluga (poput tvrtki Facebook, Google, Amazon) nameću kroz svoje nezakonite politike privatnosti. Zbog toga što produbljuju postojeće društvene i političke rascjepke do točke prenaprezanja za samo društvo i politički sustav, društvene mreže i obrada podataka postale su jedan od nezaobilaznih instrumenata geopolitike te jedno od ključnih pitanja nacionalne sigurnosti. Stoga, sva nacionalna nadzorna tijela za zaštitu podataka moraju biti tehnološki i kadrovski kapacitirana za provedbu nadzora nad suvremenim tehnološkim praksama obrade i prikupljanja podataka. Adekvatni tehnološki kapaciteti nadzornih tijela (u koje ubrajamo i AZOP), preduvjet su za zaštitu digitalnih prava građana EU i obuzdavanje brojnih negativnih društvenih i političkih fenomena.

Ukoliko AZOP bude djelovao kao samostalna, neovisna, proaktivna i tehnološki kapacitirana institucija, može razviti kapacitete za nadzor praksi prikupljanja i obrade podataka koju provode IT divovi. Francusko nadzorno tijelo za obradu podataka [CNIL izdalo je kaznu Googleu u visini od 100 milijuna dolara](#) zbog kršenja najosnovnijih načela obrade podataka. Google svojim korisnicima nije pružio dovoljno informacija o politici privatnosti niti im je dao adekvatnu kontrolu nad time kako se njihove informacije koriste. Unatoč pravnom osporavanju, kazna je potvrđena na višim sudovima jer je vrlo lako argumentirati i potkrijepiti nalaze o nezakonitosti Googleovog sustava obrade podataka. Snažna zaštita temeljnih prava građana RH, u vidu financijskog kažnjavanja globalnih IT divova, imala bi tako i direktne pozitivne financijske učinke na proračun RH.

Tvrtka Brave Software, globalno prepoznata prema jednom od najboljih Internet preglednika iz perspektive zaštite privatnosti (*privacy web browser*), objavila je [studiju o tehnološkim kapacitetima nadzornih tijela](#) za zaštitu podataka svih država članica EU, uključujući i AZOP. Cilj studije je bio pružiti uvid u spremnost europskih nadzornih tijela za nadzor suvremenih tehnoloških praksi prikupljanja i obrade podataka. Istraživanje iz 2020. godine navodi da AZOP ima 5 osoba koji su „tech specialist“.

S ciljem utvrđivanja stvarnog broja zaposlenika AZOP-a koji rade na tehnološkom nadzoru, analizirani su godišnji izvještaji o radu. Prilikom povećanja broja zaposlenih zbog novih obveza tijelu nametnutih Uredbom, nedovoljna pažnja se posvetila osiguranju adekvatnih tehnoloških kapaciteta. Broj pravnika se 2017. godine povećao s 11 na 21 zaposlenog, dok se broj zaposlenika u kategoriji „informatičke ili tehničke ili kriminalističke znanosti povećao s 4 na 6. [AZOP u izvještaju za 2019. godinu](#) navodi kako u navedenoj grupnoj kategoriji ima ukupno 7 zaposlenika.

Iznimno je uočljivo da su gotovo sve kategorije zaposlenika jasno definirane (pravnik, društvene znanosti, ekonomske znanosti) izuzev kategorije zaposlenika u kojoj se nalaze IT eksperti – *informatičke ili tehničke ili kriminalističke znanosti*. Budući da iz neuobičajeno definirane kategorije zaposlenika nije moguće ustanoviti broj IT stručnjaka, udruga Politiscope uputila je AZOP-u zahtjeve za pravom na pristup informacijama u kojima je tražila dodatne informacije o poslovima koje ti zaposlenici obavljaju i njihovoj stručnoj spremi. Nastavljajući na nalaze Brave analize koja navodi 5 „tech specialista“ u AZOP-u, Politiscope ističe da se na temelju dostavljenih informacija, može zaključiti da se svega jedna ili dvije osobe mogu smatrati IT stručnjacima koji imaju kapacitete za obavljanje nadzora suvremenih tehnoloških praksi obrade podataka. Dodatno tome, iznimno je upitno koliko stvarnih sati rada otpada na ovakve zadatke, budući da osobe koje su navedene kao IT stručnjaci obavljaju druge, nevezane poslove unutar Agencije. Na primjer, jedan od IT stručnjaka je specijaliziran europsku suradnju u razmjeni *kaznenih, viznih* podataka čime AZOP ispunjava obveze definirane raznim europskim uredbama. Jedan IT stručnjak, uz druge radne odgovornosti, pruža IT podršku zaposlenicima, dok jedna IT stručnjakinja zaposlena na poslovima međunarodne suradnje ujedno održava Internetske stranice Agencije.

Pohvalan je AZOP-ov pristup upravljanju prepoznatim rizicima manjka tehnoloških kapaciteta. Naime, u odgovoru na postavljeni zahtjev za pravom na pristup informacijama, AZOP je dostavio detaljne informacije o svojevrsnom neformalnom horizontalnom radnom procesu unutar Agencije, u kojeg se povremeno i po potrebi, uključuju tehnološki kapacitirani zaposlenici, neovisno o konkretnom radnom mjestu kojeg obnašaju. Ovakav pristup zasigurno doprinosi smanjenju negativnosti koje proizlaze iz tehnološke potkapacitiranosti institucije. S druge strane, Politiscope smatra iznimno pogrešnim pristup u kojem se nastoji kamufilirati istina o tehnološkoj potkapacitiranosti institucije, kroz stvaranje lažne slike o postojanju tima IT stručnjaka koji rade na IT poslovima. Upravo suprotno, AZOP mora u svojim izvještajima o radu iskreno progovarati o nedostatnim ljudskim resursima, što je preduvjet da se Hrvatski sabor uopće upusti u raspravu o mogućnosti povećanja sredstava koje AZOP dobije iz državnog proračuna. Također, ovo je i preduvjet za hrabri zahvat u sistematizaciju radnih mjesta koja za cilj mora imati privlačenje kvalitetnih IT stručnjaka kapacitiranih za nadzor tehnoloških praksi obrade podataka.

Nužno je da AZOP kreira plan upravljanja ljudskim resursima i razvoja tehnoloških kapaciteta za nadzor suvremenih tehnoloških praksi prikupljanja i obrade podataka. Ukoliko institucija uistinu bude djelovala kao samostalno i nadzorno tijelo, za takav iskorak u razvoju institucije je nužno osigurati adekvatna sredstva u državnom proračunu. AZOP mora biti u stanju privući IT stručnjake, nudeći im dobro plaćena radna mjesta u javnoj instituciji koja uživa ugled i povjerenje, u kojoj postoji ugodno radno okruženje te posvećenost zaštiti digitalnih prava građana i ostvarenju ciljeva Uredbe. Naposljetku, preduvjet za ove iskorake jest da AZOP u svojim godišnjim izvještajima o radu daje vjeran i iskren uvid u vlastite ljudske i tehnološke kapacitete te dokine sklonost friziranju tih podataka.

MANJKAVOSTI ZAKONSKOG OKVIRA

Za potrebe ove analize nije izrađena opsežna analiza Zakona o provedbi Uredbe već se analiziraju dvije ključne zakonske manjkavosti koje ozbiljno doprinose neostvarenju ciljeva i svrhe zakona – nepostojanje upravnih kazni za javna tijela, neobjavljivanje nepravomoćnih upravnih novčanih kazni. Zakon o provedbi Opće uredbe o zaštiti podataka definira „Isključenje primjene upravnih novčanih kazni na tijela javne vlasti“ (čl. 47.). Iznimka je uvedena pod izlikom argumenta izbjegavanja nepotrebnog prelijevanja novca iz jednog javnog proračuna u drugi. No, sasvim očekivano, kao i kod drugih zakonskih odredbi za čije kršenje ne postoje financijske kazne, centralna tijela izvršne vlasti se ponašaju kao da nisu obveznici zakona. Tako na primjer, Hrvatski zavod za javno zdravstvo salonima izdaje upute o prikupljanju osobnih podataka klijenata, iako recital 45. Uredbe obvezuje na prethodno



kreiranje zasebnog nacionalnog zakonskog propisa. Na [web stranicama grada Vukovara](#) se objavljuje snimka djece pripadnika nacionalne manjine koja se na stadionu nisu ustala na hrvatsku himnu. Ovaj slučaj je kandidat za najgori europski primjer kršenja Uredbe otkad je ista na snazi – objava video snimke je dovela do fizičkog napada na djecu od strane njihovih vršnjaka. Vladin digitalni asistent Andrija, objavljen je bez Politike privatnosti. U pokušaju kontroliranja štete javne reputacije, [bolnica iznosi osobne podatke pacijenta](#), političarke koja za saborskom govornicom kritizira tretman kojeg je imala kao pacijentica i trudnica. Nepostojanje upravnih novčanih kazni stvorilo je osjećaj nekažnjivosti kod tijela javne vlasti, zbog čega su upravo ona odgovorna za najvidljivije primjere kršenja Uredbe u Hrvatskoj.

Zakonom o provedbi je također definirano kako će se upravne novčane kazne objaviti neanonimizirane tek po pravomoćnosti rješenja, odnosno tek nakon isteka roka za podnošenje tužbe ili pravomoćne odluke upravnog suda povodom pokretanja upravnog spora. AZOP je u ožujku 2020. [objavio odluku](#) o izricanju novčane upravne kazne jednoj banci, no sukladno zakonu, odluka je anonimizirana jer nije pravomoćna te nije navedeno o kojoj se banci radi niti koliki je iznos kazne. U navedenom slučaju, banka je čak nekoliko tisuća klijenata odbila omogućiti pristup njihovim osobnim podacima. Klijenti su tražili dostavu kreditne dokumentacije koja se odnosi na sklopljene ugovore o kreditu u švicarskim francima. AZOP je prije donošenja odluke o upravnoj novčanoj kazni donio čak 34 rješenja kojima je naložio banci ispunjenje zahtjeva ispitanika za ostvarenjem Uredbom zajamčenog prava, koje je banka ignorirala. Anonimiziranjem podataka o voditelju obrade koji je grubo prekršio temeljna prava svojih klijenata, ne ostvaruje se jedna od osnovnih svrha ideje o sankcioniranju kršitelja Uredbe – upoznavanje građana s nezakonitim praksama Voditelja obrade. Naime, drugi građani koji su trenutni ili potencijalni klijenti te banke ne znaju da ista uporno, drsko i masovno krši jedno od najosnovnijih prava ispitanika, i pritom ignorira naloge nadzornog tijela. Također, ostaje potpuno nejasno koja je točno svrha tajnosti preciznog iznosa dodijeljene novčane kazne. Ističemo kako je praksa niza nadzornih tijela za zaštitu podataka u EU objavljivanje odluka o upravnim novčanim kaznama s punim nazivima voditelja obrade te iznosom kazne.

Hrvatski Zakon o provedbi Uredbe zahtjeva ozbiljne i hitne izmjene. Osim što isključenje primjene upravnih novčanih kazni na tijela javne vlasti te anonimiziranje kršitelja Uredbe do pravomoćnosti dovodi do brojnih nepoželjnih praksi, ujedno je riječ o aktu koji ne ispunjava svoju osnovnu svrhu. Naime, sama Uredba predviđa mogućnost propisivanja većeg broja iznimki i dodatnog proširivanja odredbi Uredbe kroz nacionalno zakonodavstvo. No, ova prilika nije iskorištena, izuzev za jedno jedino područje – videonadzora. Ne iznenađuje stoga da se među stručnjacima za zaštitu podataka Zakon o provedbi Uredbe kolokvijalno naziva i Zakonom o videonadzoru, budući da je to praktički jedino područje, izuzev ustroja i rada AZOP-a, koje Zakon detaljnije normira.

PREPORUKE:

- **Pandemijska obrada i prikupljanje podataka**
 - hitnim izmjenama Zakona o zaštiti pučanstva od zaraznih bolesti ispuniti sve obveze predviđene recitalom 45., kojim se definiraju elementi nužnog zakonskog okvira za prikupljanje podataka građana u svrhu zaštite javnog zdravlja

- **Samostalnost i neovisnost nadzornog tijela za zaštitu podataka**
 - Hrvatski sabor mora odbijanjem izvješća o radu Agencije za zaštitu osobnih podataka za 2019. i 2020. godinu poslati jasnu poruku o nužnosti izbora novog čelnika institucije, s ciljem uspostave funkcionalnog sustava za zaštitu digitalnih prava građana RH i EU te zaustavljanja daljnjeg rasapa vladavine prava kroz političko zarobljavanje samostalnih i neovisnih nadzornih institucija
 - uvođenje strožih zakonskih uvjeta za mjesto čelnika institucije – nije član političke stranke najmanje tri godine (u slučaju kandidature dužnosnika, kao datum prestanka članstva uzima se datum evidentiranja izmjene statusa u *imovinskoj kartici*)

- **Zakon o provedbi Opće uredbe o zaštiti podataka:**
 - ukidanje „Isključenja primjene upravnih novčanih kazni na tijela javne vlasti“ (čl. 47.)
 - objava nepravomoćnih neanonimiziranih odluka o kaznama kako bi se ostvarila svrha Uredbe (izmjena čl. 48.)
 - proširiti Zakon dodatnim odredbama s ciljem uklanjanja pravne nesigurnosti za građane i pravne subjekte, budući da je takva mogućnost predviđena samom Uredbom

- **Agencija za zaštitu osobnih podataka:**
 - izrada plana upravljanja ljudskim resursima i razvoja institucionalnih kapaciteta za nadzor suvremenih tehnoloških praksi prikupljanja i obrade podataka
 - osiguranje sredstava u državnom proračunu za provedbu plana
 - razvoj kapaciteta za sankcioniranje nelegitimnih i nezakonitih praksi globalnih IT divova zbog kršenja osnovnih pravila Uredbe





Iceland 
Liechtenstein **Active**
Norway **citizens fund**



Projekt "Privatnost u doba Corone" je podržan s 4.973 € financijske podrške Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova.

Kreiranje ove analize omogućeno je financijskom podrškom Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova. Sadržaj ove analize isključiva je odgovornost udruge Politscope i ne odražava nužno stavove država donatorica i Upravitelja Fonda.