Petar Mrkonjić*

Opća uredba Europske unije o zaštiti osobnih podataka sa osvrtom na kompatibilnost bosanskohercegovačkog sustava zaštite osobnih podataka sa novim europskim okvirom

Sadržaj

* Autor je magistar prava i prokurist u kompaniji EOS MATRIX d.o.o. Sarajevo.

1. Uvod

The era of privacy is over[1], izjava je osnivača društvene mreže Facebook Marka Zuckerberga iz 2010. godine. Zuckerberg tvrdi da su ljudi postali sretni što dijele osobne podatke na društvenim mrežama i da je vrijeme da se percepcija privatnosti prilagodi novom vremenu velikog opsega razmjene osobnih podataka. Sa sedmogodišnje vremenske distance, čini se da je Zuckerberg malo požurio sa odbacivanjem koncepta poštivanja ljudske privatnosti. U međuvremenu su ljudi, koristeći društvene mreže i dijeleći svoje podatke na druge načine, spoznali sve negativne učinke koje manjak privatnosti na internetu može donijeti. Na toj osnovi su se razvili građanski pokreti sa incijativama da se velikim korporacijama i državnim agencijama ograniči samovolja prilikom obrade podataka, te da se građanima ponovno povrati kontrola nad njihovim osobnim podacima, tj. nad njihovom privatnošću. Nedugo nakon Zuckerbergove izjave, točnije 2011. godine Europska komisija pokrenula je incijativu za donošenje propisa iz oblasti obrade i zaštite podataka za digitalno doba koja će rezultirati usvajanjem *Opće uredbe o zaštiti podataka* (EU) *2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ* (u daljnjem tekstu: Uredba)[2]. Uredba[3] je propis koji vraća nadu u poštivanje prava na privatnost čak i u ovo vrijeme sveprisutne digitalne automatizirane obrade podataka i kada se čini da, kao pojedinci i društvo, gubimo bitku za svoju privatnost. To je revolucionarni pravni akt koji Europsku uniju određuje kao prostor slobodnog protoka osobnih podataka, uz najvišu moguću razinu poštivanja prava na privatnost, uzimajući u obzir interese, prije svega, građana EU, ali i interese nacionalne sigurnosti i ekonomije. Prema njenoj preambuli, Uredbom se želi doprinijeti uspostavi područja slobode, sigurnosti i pravde, te gospodarske unije, gospodarskom i socijalnom napretku, jačanju i približavanju gospodarstava na unutarnjem tržištu i dobrobiti pojedinaca, a sama obrada osobnih podataka *trebala bi biti osmišljena tako da bude u službi čovječanstva*. U ovoj analizi ću se baviti pitanjima konteksta donošenja Uredbe, novim legislativnim rješenjima u dijelu prava nositelja podataka i dužnostima kontrolora i obrađivača, te primjenom Uredbe, uz poseban osvrt na stanje zaštite osobnih podataka u Bosni i Hercegovini.

2. Pregled osnovnih pojmova prava zaštite osobnih podataka[4]

Osobni podaci su svi oni podaci na osnovu kojih se može, izravno ili neizravno, utvrditi identitet pojedinca. Takvi podaci mogu biti: ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili podaci vezani za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet nekog pojedinca[5]. Pojačanu zaštitu uživaju tzv. posebne kategorije osobnih podataka kao i osobni podaci djece[6].

---

[1] Prijevod: Era privatnosti je završena!
[2] *Sl. l. EU* L 119/1.
[3] Uredba dostupna: http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=HR, očitanje: 07. 12. 2017.
[4] Službeni prijevod Uredbe na hrvatskom jeziku (RH) koristi pojmove voditelja obrade za kontrolora, izvršitelj obrade za obrađivača, a ispitanika za nositelja osobnih podataka. Nazivi kontrolor, obrađivač i nositelj osobnih podataka su pojmovi koji se koriste u sve tri jezičke verzije Zakona o zaštiti osobnih podataka Bosne i Hercegovine, zbog čega ću se u daljnjem tekstu služiti terminologijom koja je općeprihvaćena u BiH.
[5] § 30 Preambule Uredbe (bilj. 2) navodi sljedeće: „Pojedinci mogu biti pridruženi mrežnim identifikatorima koje pružaju njihovi uređaji, aplikacije, alati i protokoli, kao što su adrese internetskog protokola, identifikatori kolačića

Obrada osobnih podataka[7] predstavlja svaku moguću radnju povezanu sa osobnim podacima, koja se može vršiti automatiziranim (digitalna obrada) ili neautomatiziranim putem (ručno)[8].

Kontrolor obrade je osoba koja vrši aktivnosti obrade, a ona može biti fizička ili pravna osobaili tijelo javne vlasti.

Obrađivač je fizička ili pravna osoba ili tijelo javne vlasti koje obrađuje osobne podatke u ime i po uputama kontrolora, najčešće na osnovu ugovora.

Nositelj osobnih podataka je živi pojedinac – fizičko lice čije je identitet utvrđen ili se može utvrditi na osnovu tih podataka.

3. Glavna načela obrade

Obrada osobnih podataka može se vršiti uz poštivanje osnovnih načela obrade, a to su načela zakonitosti, transparentnosti i proporcionalnosti[9]. Načelo zakonitosti zahtijeva da se osobni podaci mogu prikupljati i obrađivati samo u skladu sa zakonom. Posebno se to odnosi na svrhu obrade, način i vrijeme obrade osobnih podataka. Transparentnost obrade podrazumijeva da su pojedincu dostupne informacije o tome kako se obrađuju osobni podaci koji se na njega odnose. Dodatno, pojedinci bi trebali biti upoznati s rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom osobnih podataka.

Konačno obrada osobnih podataka bi trebala biti primjerena, bitna i ograničena na ono što je nužno za svrhe u koje se podaci obrađuju (*načelo proporcionalnosti*). Zbog toga je osobito potrebno osigurati da je razdoblje u kojem se osobni podaci pohranjuju ograničeno na strogi minimum. Osobni podaci trebali bi se obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima.

4. Pravo zaštite osobnih podataka u Europskoj uniji

Opća deklaracija o ljudskim pravima Ujedinjenih nacija iz 1948. je prvi međunarodni pravni dokument koji je propisao zabranu miješanja u privatni život pojedinca, obitelj, dom ili

---

ili drugim identifikatorima poput oznaka za radiofrekvencijsku identifikaciju. Tako mogu ostati tragovi koji se, posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrijebiti za izradu profila pojedinaca i njihovu identifikaciju."

[6] Posebne kategorije osobnih podataka podrazumijevaju otkrivanje rasnog ili etničkog podrijetla, političkog mišljenja, vjerskih ili filozofskih uvjerenja ili članstva u sindikatu te obradu genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

[7] Iako § 4 preambule Uredbe (bilj. 2) navodi da bi obrada osobnih podataka *trebala bi biti osmišljena tako da bude u službi čovječanstva*, svjedoci smo da se obrada osobnih podataka vrlo često provodi (nekada i zloupotrebljava) radi zadovoljenja ekonomskih, političkih ili vojnih interesa, a ne interesa čovječanstva promatrano iz kuta ljudskih prava i sloboda.

[8] Više o mogućim vidovima obrade osobnih podataka v. čl. 4 st. 1 toč. 1 Uredbe (bilj. 2).

[9] V. Poglavlje II Uredbe.

dopisivanje[10]. Pravo zaštite privatnog života je potom ugrađeno i u Europsku konvenciju o ljudskim pravima i temeljnim slobodama (Europska konvencija).

Zaštita osobnih podataka je integralni dio *prava na poštovanje privatnog i obiteljskog života* propisanog člankom 8 Europske konvencije. Kao i kod drugih kvalificiranih prava zaštićenih Europskom konvencijom, zadiranje u ovo pravo je dozvoljeno kada je to utemeljeno na zakonu i kada je to u demokratskom društvu potrebno u situacijama propisanim stavkom 2 članka 8[11], što znači da to pravo nije apsolutno. Dakle, u pravo zaštite osobnih podataka može se zadirati davanjem prvenstva nekim drugim legitimnim interesima (npr. ekonomski interes ili nacionalna sigurnost) pod uvjetima koji su propisani zakonom i u skladu sa načelom proporcionalnosti[12].

U zemljama članicama Europske unije, *zaštita osobnih podataka* se kao zasebno i jasno određeno ljudsko pravo prvi put spominje u vezi sa Konvencijom Vijeća Europe iz 1981. godine za zaštitu pojedinaca u vezi sa automatskom obradom osobnih podataka. Prvi akt Europske unije u ovoj oblasti bila je Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (Direktiva). Upravo je ova Direktiva, zajedno sa pratećim nacionalnim pravnim propisima, izgradila pravni partikularizam u oblasti zaštite osobnih podataka. Kao pravni akt, Direktiva je obvezujuća u smislu cilja koji se njome želi ostvariti, dok je državama članicama prepušteno da same odlučuju na koji način doći do tog cilja. Direktiva je stvorila pravni partikularizam na razini EU, unutar kojeg egzistiraju zasebni pravni okviri zaštite podataka, interpretacije i praktična primjena propisa o zaštiti osobnih podataka, mehanizmi nadzora nad primjenom zakona, te prekršajne odnosno kaznene odredbe za kršenje zakona[13]. Posljedica toga je bilo to da su se gospodarski subjekti koji posluju u više država EU (na jedinstvenom bescarinskom tržištu), suočeni sa pravnom nesigurnošću različitih regulativa i postupanja nadležnih tijela u dijelu zaštite osobnih podataka, morali prilagođavati posebnostima svake od država u kojoj su prisutni, što je nespojivo sa proklamiranom jedinstvenošću tržišta Unije[14]. Želja Europske komisije i zakonodavca je bila da se pravo zaštite osobnih podataka uredi jedinstveno na nivou EU, donošenjem uredbe koja po svom karakteru ne zahtijeva donošenje primjenjujućih propisa (iako sama Uredba dopušta državama članicama da neka pitanja sama uređuju[15]), već se izravno primjenjuje u pravnom sustavu svake od država članica.

[10] Kronološki prikaz uspostavljanja okvira zaštite prava na privatnost i prava zaštite osobnih podataka dostupno na: https://rm.coe.int/16806ae653, očitanje: 07. 12. 2017.
[11] Sud pravde Europske Unije je u niz svojih odluka potcrtao da zaštita osobnih podataka potpada pod čl. 8 EKLJP, što znači da zaštita osobnih podataka spade u domenu zaštite privatnog i obiteljskog života, doma i dopisivanja. Up. C-465/00 AND C-138/01, Rechnungshof v. Österreichisch-steierischer Rundfunk, 20. 05. 2003 („Rechnungshof“).
[12] U uredbi se “sukobljavaju” sljedeća prava i načela: poštovanje privatnog i obiteljskog života, doma i komuniciranja, zaštita osobnih podataka, sloboda mišljenja, savjesti i vjeroispovijedi, sloboda izražavanja i informiranja, sloboda poduzetništva, pravo na učinkoviti pravni lijek i pošteno suđenje te pravo na kulturnu, vjersku i jezičnu raznolikost.
[13] Razlike u pravnim okvirima, mehanizmima nadzora, prekršajnim i kaznenim odredbama, kao i druge razlike između država članica moguće pronaći na: https://www.dlapiperdataprotection.com/index.html, očitanje: 07. 12. 2017.
[14] Više o koristima novog okvira dostupno na: http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf.
[15] Iako se Uredba izravno primijenjuje u državama članicama EU, države članice će same morati urediti pitanja poput ovlaštenja nacionalnog regulatornog tijela zaštite osobnih podataka, odnosno pitanja u kojima je Uredba ovlastila države članice da ih mogu pobliže kao npr. suglasnost na obradu podataka djeteta.

Ako su Lisabonski ugovori zapravo Ustav Europske unije, onda zaštita osobnih podataka u Europskoj uniji predstavlja ustavnu kategoriju, pošto članak 16 Ugovora o funkcioniranju Europske unije propisuje da *svatko ima pravo na zaštitu svojih osobnih podataka.* Iz istog članka proizilazi i zajednička nadležnost Europskog parlamenta i Vijeća da urede pitanje zaštite osobnih podataka u EU i na razini država članica (temelj za donošenje Uredbe kao akta sa neposrednom primjenom).

U odnosu na prethodno važeći pravni okvir, važno je istaknuti da se od njegovog usvajanja mnogo toga promijenilo - osobni podaci su postali najvažnije pogonsko gorivo svjetske ekonomije. Osim ekonomskog aspekta, obrada i razmjena osobnih podataka su, danas više nego ikad, postale važne radi obrane interesa sigurnosti država članica EU, ali i same EU. Građani EU vrlo rado i jednostavno dijele svoje osobne podatke (to se prvenstveno odnosi na internet), ponekad i ne shvaćajući negativne posljedice koje za njih iz toga mogu proizaći. Kako bi omogućila konkurentnost i rast svoga gospodarstva, te zaštitu interesa nacionalne sigurnosti i obrane, Europska unija je trebala pravni okvir koji će sve to omogućiti, uz najvišu moguću razinu zaštite osobnih podataka na svijetu. Uredba je stoga pravovremeni i sveobuhvatni odgovor Europske unije na novi način života, vladanja i privređivanja.

5. Uredba i njena primjena

5.1. Razlozi za donošenje Uredbe

Još od 1995. godine, zaštitu osobnih podataka u Europskoj uniji uređivala je Direktiva 95/46/EZ[16], te prateća nacionalna zakonodavstva država članica. Takav pravni okvir bio je problematičan iz dva praktična razloga. *Prvi* razlog je da su se s protjecanjem vremena uspostavili partikularni pravni okviri zaštite osobnih podataka, a potom i zasebne prakse postupajućih regulatornih i sudbenih tijela, na razini svake države članice. *Druga* manjkavost ranijeg okvira bila je njegova neprimjenjivost u današnjem svijetu. Od 1995. na ovamo, tehnološki razvoj svijeta napredovao je eksponencijalnom brzinom. U vrijeme donošenja Direktive, postavljalo se pitanje koliko kućanstava ima računalo, dok je pristup internetu još bio rijetkost, čak i u EU. Danas građani pristupaju internetu sa svojih računala, laptopa, tableta, pametnih telefona, satova, televizora, automobila, pa čak i kućanskih aparata[17]. Tom prilikom, svjesno ili ne, građani masovno dijele svoje osobne podatke koje kontrolori koriste za izradu profila potrošača kako bi svoj proizvod maksimalno prilagodili potrebama tržišta. Nacionalne vlade, pod izgovorom nacionalne sigurnosti (što se vrlo često zloupotrebljava), također izrađuju profile svojih građana kako bi kontrolirali neželjene pojave poput terorizma. U nedemokratskim režimima poput Irana ili Sjeverne Koreje vlade prate društvene mreže kako bi sankcionirale antirežimska ponašanja.

U svijetu u kojem je osobni podatak postao najvažniji gospodarski i/ili vojni resurs, gospodarskim subjektima je bila potrebna regulativa koja će pratiti tehnološki razvoj i potrebe tržišta. Zbog zaštite pojedinca u svijetu masovne obrade podataka, generiranja gospodarskog

[16] Puni naziv: Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. 10. 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka.
[17] Prema podacima EUROSTAT-a za 2016. čak 85% kućanstava je imalo pristup internetu. Taj se udio postupno povećavao od 2007. kada je pristup internetu imalo 55% kućanstava. Pomalo preambiciozno zvuči najava predsjednika Europske komisije J. C. Junckera da će 2020. svako selo i grad u EU imati besplatni bežični internet.

rasta i konkurentnosti tržišta EU, Europska unija je morala brzo djelovati donošenjem novog pravnog okvira koji će biti primjenjiv u ovom trenutku, ali i u budućnosti.

5.2. Primjena Uredbe

Uredba predstavlja pravni okvir zaštite osobnih podataka u EU koji se odnosi na *fizičke osobe*, i to isključivo na žive pojedince, s tim što se državama članicama daje diskrecijsko pravo da vlastitim propisima urede pitanje zaštite osobnih podataka preminulih osoba. Uredba se, dakle, odnosi na svaku vrstu kontrolora ili obrađivača, bez obzira da li su oni fizičke ili pravne osobe, ukoliko provode obradu osobnih podataka građana EU. Uredba prvenstveno pruža zaštitu u odnosu na obradu osobnih podataka od strane kontrolora ili obrađivača ukoliko je njihov poslovni nastan u EU, bez obzira da li sam nositelj osobnih podataka živi u EU ili izvan EU[18].

Nadalje, Uredba se odnosi i na obradu osobnih podataka nositelja osobnih podataka – građana EU koju obavljaju kontrolori ili obrađivači bez poslovnog nastana - sjedišta u Uniji[19], ukoliko se obrada odnosi na nuđenje robe ili usluga nositeljima osobnih podataka u Uniji[20] ili se odnosi na praćenje ponašanja nositelja osobnih podataka dokle god se njihovo ponašanje odvija unutar Unije[21].

Razumljivo je da se Uredba odnosi na obradu osobnih podataka građana EU koju vrše subjekti sa sjedištem u EU. Također, u skladu je sa intencijom stvaranja prostora visoke razine zaštite osobnih podataka, da se Uredba odnosi općenito na postupanje kontrolora ili obrađivača nastanjenih u EU, bez obzira da li su fizička lica čiji se podaci obrađuju nastanjeni u EU ili izvan EU. Međutim, vrlo je kontroverzno pitanje primjene Uredbe na kontrolore ili obrađivače nastanjene izvan EU. Uzmimo za primjer kontrolora koji posluje i ima sjedište u Bosni i Hercegovini, te obrađuje osobne podatke građana EU. Njegova obveza je da se ponaša u skladu sa propisima Bosne i Hercegovine. Jasno je, pritom, da takav subjekt nije dužan voditi računa o propisima drugih država, niti je osnovano od njega očekivati da prati proces usvajanja, objavljivanja i stupanja na snagu propisa druge države ili pravnih tvorevina kao što je Europska unija. Prema Uredbi, takav će pravni subjekt biti u obvezi u cijelosti postupati u skladu sa odredbama Uredbe u odnosu na obradu osobnih podataka građana EU. Praktično, takav subjekt će prije 25. svibnja 2018. godine[22] morati provesti detaljnu analizu o tome da li se i u kojem obimu ova Uredba odnosi na njega. U slučaju potvrdnog odgovora, bit će u obvezi provesti sve

[18] Više o pitanju proširene teritorijalne jurisdikcije EU u odnosu na zaštitu osobnih podataka njenih građana na: http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf, očitanje: 07. 12. 2017.

[19] Radi komunikacije sa nadzornim tijelima u EU, kontrolori ili obrađivači sa sjedištem izvan EU koji obrađuju osobne podatke građana EU, u obvezi su imenovati *predstavnika* koji mora imati sjedište u jednoj od država članica EU.

[20] O tome više u § 23 Preambule Uredbe (bilj. 2).

[21] *Ibid*, § 24 Preambule Uredbe: "Na obradu osobnih podataka nositelja osobnih podataka koji se nalaze u Uniji, a koju obavlja kontrolor ili obrađivač bez poslovnog nastana u Uniji, također bi se trebala primjenjivati ova Uredba kada se odnosi na praćenje ponašanja takvih nositelja osobnih podataka ako se njihovo ponašanje odvija unutar Unije. Kako bi se odredilo može li se aktivnost obrade smatrati praćenjem ponašanja nositelja osobnih podataka, trebalo bi utvrditi prati li se pojedince na internetu među ostalim mogućom naknadnom upotrebom tehnika obrade osobnih podataka koje se sastoje od izrade profila pojedinca, osobito radi donošenja odluka koje se odnose na njega ili radi analize ili predviđanja njegovih osobnih sklonosti, ponašanja i stavova."

[22] Datum početka primjene Uredbe.

propisane mjere zaštite osobnih podataka u skladu sa Uredbom. U ovom dijelu se postavlja nekoliko pitanja na koje će se odgovor pronaći tek praktičnom primjenom Uredbe:

- Da li će subjekti nastanjeni izvan EU u praksi postupati u skladu sa Uredbom?
- Kako će sporni subjekti provoditi duple propise o zaštiti osobnih podataka s obzirom da primjena Uredbe ne isključuje obvezu da se poštuju lokalni propisi zaštite osobnih podataka?
- Kakav stav će zauzeti države u kojima se nalaze sporni subjekti s obzirom da se na subjekte osnovane u skladu sa njihovim propisima širi primjena propisa drugih država (u ovom slučaju EU) bez potpisivanja bilo kakvih bilateralnih ili multilateralnih sporazuma?
- Kako će se Uredba provoditi na teritoriji država u kojima se nalaze sporni subjekti (Kako naplatiti izrečenu kaznu?)?

5.3. Izuzeci od primjene

Osim vrlo široko definirane primjene Uredbe (prekogranična primjena), Uredba propisuje i nekoliko važnih izuzetaka. Tako se Uredba ne odnosi na: obradu osobnih podataka pravnih osoba, preminulih osoba, pitanja zaštite osobnih podataka u vezi sa djelatnostima poput onih povezanih sa nacionalnom sigurnošću, obradu osobnih podataka od strane država članica pri obavljanju djelatnosti povezanih sa zajedničkom vanjskom i sigurnosnom politikom Unije, te obradu osobnih podataka koju fizičke osobe obavljaju u okviru isključivo osobnih ili kućnih aktivnosti.

Uredba se ne primijenjuje niti na aktivnosti koje obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprječavanja.

6. Prava nositelja podataka

6.1. Prošireni spektar prava nositelja podataka

Osnovni motiv Europske komisije (barem prema preambuli Uredbe i riječima njenih glavnih dužnosnika), bilo je donijeti novi okvir zaštite osobnih podataka koji će pojačati prava građana EU u ovoj oblasti i dati im konkretnu moć kako bi umjesto objekata, postali subjekti i zaista počeli odlučivati o sudbini svojih osobnih podataka. Jedna od temeljnih odrednica Uredbe je proširenje prava nositelja podataka i njihovo poprilično detaljno propisivanje. Aktivnosti koje poduzimaju kontrolori i obrađivači u vezi sa ostvarivanjem prava nositelja podataka se obavljaju bez zaračunavanja naknade prema nositelju podataka. Svjedoci smo da čak i minimalne administrativne pristojbe utječu vrlo negativno na podnošenje zahtjeva za zaštitu prava potrošača. Ukidanje naknada moglo bi, stoga, djelovati vrlo pozitivno na povećanje broja zahtjeva za zaštitu prava nositelja podataka. Ali, istovremeno to bi djelovalo i vrlo negativno prema kontrolorima i obrađivačima koji bi morali podnijeti administrativni (dakako i financijski) teret obrade i rješavanja takvih zahtjeva[23]. Često se misli (i piše)[24] da je svrha donošenja Uredbe

[23] Izuzetak predstavlja čl. 12 st. 5 Uredbe (bilj. 2) koji propisuje da se razumna naknada može naplatiti u slučaju očigledno neutemeljenih i pretjeranih zahtjeva nositelja podataka.

bilo disciplniranje multinacionalnih kompanija poput Facebook-a, Uber-a ili Airbnb-a, ali prava svrha Uredbe[25] je promoviranje i učvršćivanje prava građana Europske unije u kontekstu zaštite njihovih osobnih podataka u vremenu digitalizacije u kojem informacije postaju najvažniji ekonomski resurs.

Niti jedno od propisanih prava nije apsolutno, što znači da se može konzumirati uz ispunjenje određenih propisanih uvjeta. U ovom dijelu ću predstaviti neka od najvažnijih prava koje donosi Uredba.

6.2. Pravo na pristup informacijama o obradi osobnih podataka

Radi se o pravu čije uživanje predstavlja temeljnu odrednicu težnje da se kontrolora i obrađivača ograniči u upotrebi takvih podataka mimo svrhe u koju su uzeti ili, recimo, izvan rokova unutar kojih je postojala potreba da se ovi podaci obrađuju. S druge strane, ovo pravo je u samoj srži prava na zaštitu osobnih podataka kao vrlo bitnog aspekta prava na privatnost. Danas je za građane važnije nego ikad da znaju tko obrađuje njihove podatke, koja je svrha obrade, do kada će se podaci obrađivati i da li će biti nekome proslijeđeni, arhivirani ili uništeni.

6.3. Pravo na zaborav (prije Uredbe)

Jedna od najpoznatijih i najspominjanijih novina koju nam donosi Uredba se odnosi na tzv. pravo na zaborav. Ovo pravo je aktualizirano puno prije donošenja Uredbe, no njegovu konačnu sudbinu je odredio Sud pravde EU donošenjem pravnog presedana u poznatom slučaju "GOOGLE"[26]. Mario Costeja Gonzalez, španjolski odvjetnik tužio je Google Inc., Google Španjolska i medijsku kuću La Vanguardia zbog činjenice da je ukucavanjem njegovog imena u Google-ovu tražilicu svaki korisnik te tražilice mogao klikom na dvije poveznice (linkove) na stranice La Vanguardia-e, doći do informacija koje ga kompromitiraju (informacije su se odnosile na 16 godina staru aukciju povezanu sa odvjetnikovim dugovanjima za koja je on tvrdio da su odavno riješena i da mu postojanje ovih poveznica veoma šteti). On je zatražio da se ovi podaci izbrišu ili prikriju od strane Google Inc ili Google Španjolska.

Prije donošenja odluke, pred Sudom pravde EU se pojavilo nekoliko pitanja o dopustivosti zahtjeva kao i primjenjivosti pravnog okvira EU za zaštitu podataka na konkretni slučaj, koja je trebalo raspraviti da bi se uopće moglo pristupiti meritornom odlučivanju.

Prije svega, bilo je potrebno utvrditi primijenjivost Direktive 95/46 s obzirom da se ona odnosila samo na subjekte sa sjedištem u EU, a u svjetlu činjenice da usluge tražilice pruža Google Inc. sa sjedištem u Sjedinjenim Američkim Državama, dok je Google Španjolska registran za obavljanje

[24] Članak o novom pristupu EU prema multinacionalnim kompanijama iz SAD-a, uključujući pitanje zaštite osobnih podataka: http://fortune.com/2017/07/20/google-facebook-apple-europe-regulations/, očitanje: 07. 12. 2017.
[25] Europska komisija u svom priopćenju navodi da je cilj novog pravnog okvira povratiti građanima kontrolu nad njihovim osobnim podacima. Priopćenje Europske komisije dostupno na: http://ec.europa.eu/justice/data-protection/, očitanje: 07. 12. 2017. Isto se navodi u priopćenju Europskog parlamenta dostupnom na: http://www.europarl.europa.eu/news/hr/press-room/20160407IPR21776/reforma-zastite-podataka-ep-odobrio-nova-pravila, očitanje: 07. 12. 2017.
[26] Presuda Suda pravde Europske unije br. C-131/12, Google Spain SL & Google Inc. V. AEPD (Agencija za zaštitu osobnih podataka Španjolske) & Mario Costeja Gonzalez, 13. 05. 2014. ("GOOGLE").

poslova oglašavanja u vezi sa rezultatima pretrage na Google-ovoj tražilici. Zatim, bilo je dvojbeno da li aktivnosti Google tražilice predstavljaju obradu osobnih podataka s obzirom da ova internetska platforma ne prikuplja osobne podatke na izravan način, već da ih prikuplja od drugih subjekata i uvrštava ih u rezultate pretrage za svoje korisnike.

Sud je odlučio da aktivnosti Google tražilice poput prikupljanja podataka, koji se potom spašavaju, arhiviraju, čuvaju na serverima i organiziraju u skladu sa potrebama i pravilima tražilice te otkrivaju u formi rezultata pretrage svojim korisnicima, predstavlja obradu osobnih podataka, unatoč činjenici da su ovi podaci već ranije objavljeni od strane npr. nekog medijskog portala i da nisu izmijenjeni od strane Google tražilice prije njenog uvrštavanja u tražilicu. Sud je zauzeo stav da uvrštavanje u tražilicu predstavlja odvojenu radnju obrade osobnih podataka u odnosu na obradu koju je proveo prvobitni kontrolor ili obrađivač tako što je nečije osobne podatke objavio na svojoj web platformi. Također, odbijanje prvobitnog kontrolora ili obrađivača da ukloni osobne podatke sa svoje platforme, ne oslobađa tražilicu od odgovornosti za obradu osobnih podataka preuzetih od prvobitnog kontrolora ili obrađivača.

Još je jedan vrlo važan aspekt koji je donijela ova presuda. Naime, ona je zajedno sa još nekim slučajevima kršenja zakonite obrade osobnih podataka, ukazala na problem obrade osobnih podataka građana EU izvan EU i od strane subjekata koji nemaju sjedište, a ni glavninu poslovnih aktivnosti na teritoriji EU. Ovaj problem je riješen tako što se novo zakonodavstvo zaštite osobnih podataka odnosi i na subjekte koji nemaju poslovni nastan u EU, ali nude proizvode ili usluge nositeljima osobnih podataka u EUili prate ponašanje nositelja osobnih podataka koje se odvija unutar EU. Konkretno, u Google presudi, Sud je odlučio da bez obzira što se obrada osobnih podataka obavlja u sjedištu Google Inc. (SAD), aktivnosti koje obavlja Google Španjolska (aktivnosti oglašavanja) su u neodvojivoj povezanosti sa aktivnostima tražilice, iz kojeg razloga se ranije EU zakonodavstvo može primijeniti i na ovaj slučaj.

Konačno, ova presuda je ogledni primjer suprotstavljenih interesa više strana gdje kontrolor, obrađivač, regulator, a po potrebi i sud, moraju voditi računa čiji će interes prevagnuti i o čemu, na koncu, ovisi zakonitost obrade osobnih podataka. Za Sud pravde, izraz pravedne ravnoteže između navedenih interesa je iskazan u njegovoj odluci kojom je Google obavezan da izbriše s popisa rezultata tražilice podatke odvjetnika, kao i poveznice prema mrežnim stranicama koje su objavile treće stranke. Sud pravde je smatrao da pravo na zaborav preteže u odnosu na ekonomski interes Google-a, ali i u odnosu na javnost čiji je interes da se informacije objavljuju i budu dostupne. Sud pravde je posebno naglasio (iako se to može jasno tumačiti i iz propisa) da bi zbog uloge neke osobe u javnom životu i naročito zbog interesa javnosti za informacije o toj osobi, miješanje u njezina temeljna prava (obrada njenih osobnih podataka) moglo biti opravdano javnim interesom. Tako bi na primjer interes javnosti u vezi sa informacijama o životu nekog od političara vrlo vjerojatno prevagnuo nad njegovim pravom na zaborav i takvu informaciju ne bi trebalo brisati u demokratskom društvu. Pravo na zaborav se kao posljedica ove presude našlo u nacrtu Uredbe Europske komisije, a potom je i usvojeno kao jedno od najvažnijih prava koje donosi Uredba.

6.4. Pravo na zaborav u Uredbi

Sama Uredba uređuje ovo pitanje u skladu sa stavovima Suda pravde EU izraženim u presudi Google. Naime, nositelj podataka ima pravo od kontrolora tražiti brisanje osobnih podataka koji se na njega odnose, a za koje obrada više nije potrebna ili je utvrđena nezakonitost obrade, dok je kontrolor u obvezi obrisati takve osobne podatke.

Također, kontrolor će morati obrisati osobne podatke nositelja ukoliko se obrada provodi na temelju pristanka nositelja podataka. Brisanje osobnih podataka se može izvršiti na dva načina. Prvi način je da kontrolor sam jednostavno obriše sporne osobne podatke, dok drugi način podrazumijeva postojanje drugih kontrolora (npr. medijske kuće koje su objavile vijest koja se nalazi na platformi kontrolora) koji obrađuju te iste podatke. U tom slučaju kontrolor je dužan druge kontrolore obavijestiti o postojanju zahtjeva za brisanje osobnih podataka te ih pozvati da obrišu sve poveznice do tih podataka.

Kao što je Sud pravde EU u presudi Google naglasio da pravo na zaborav nije apsolutno i da u svakom konkretnom slučaju mora proći test proporcionalnosti, tako i Uredba predviđa izuzetke od prava na zaborav, *u mjeri u kojoj je obrada nužna*. Primjerice, to mogu biti ostvarivanje prava na slobodu izražavanja i informiranja, javni interesi u području javnog zdravlja[27], arhiviranje u javnom interesu, i drugi.

Bit će zanimljivo vidjeti, sa tehničke i troškovne strane, praktičnu implementaciju prava na zaborav. Sigurno je da će pravo na zaborav zauzeti središnje mjesto u politikama obrade osobnih podataka kod kontrolora koji su velike svjetske platforme (ali ne samo kod njih) na kojima se prikupljaju i dijele osobni podaci. Svaki od korisnika takvih platformi će, vrlo vjerojatno, u nekom trenutku poželjeti da određeni njegov osobni podatak, opravdano ili ne, bude izbrisan sa takve platforme. Posebno treba imati u vidu da Uredba propisuje da ostvarivanje prava na zaštitu osobnih podataka mora biti besplatno. Kada se ima na umu broj korisnika npr. društvenih mreža ili nekih drugih platformi poput Uber-a ili Airbnb-a, vrlo je vjerojatno da će odjeli za zaštitu osobnih podataka ovih kompanija biti izuzetno operativno opterećeni, dok će same kompanije, vrlo vjerojatno, trošiti značajna novčana sredstva na obradu takvih zahtjeva, kao i upravne i sudske sporove koji mogu proizaći iz takvih zahtjeva. Osim obveze da brišu osobne podatke na zahtjev svojih korisnika, kontrolori su u obvezi informirati ostale kontrolore (npr. medijske portale) da je nositelj osobnih podataka zatražio brisanje takvih podataka. Ova obveza informiranja je ipak uvjetovana dostupnom tehnologijom na strani kontrolora kao i troškovima njene provedbe kao i formulacijom iz Uredbe koja propisuje “poduzimanje razumnih mjera” od strane kontrolora.

6.5. Pravo na prenosivost (tzv. data portability)

Obrada osobnih podataka se mora zasnivati na: a) pristanku nositelja osobnih podataka, zatim u svrhe izvršavanja ugovore u kojem je nositelj podataka stranka ili radi zaštite prava kontrolora obrade ili nositelja podataka u području radnog prava i socijalne sigurnosti, b) provođenju obrade automatiziranim putem. Ako su ovi uvjeti ispunjeni, nositelj osobnih podataka će imati pravo da zaprimi osobne podatke koji se odnose na njega i koje je pružio kontroloru i ima ih pravo prenijeti drugom kontroloru obrade, a prvobitni kontrolor takav prijenos ne može ometati.

[27] Više o tome u čl. 9 st. 1 toč. h) i i) Uredbe (bilj. 2).

Uredba je vrlo praktična u dijelu izravnog prijenosa jer daje pravo nositelju podataka da se prijenos izvrši izravno sa jednog na drugog kontrolora pod uvjetom da je takav prijenos tehnički izvodljiv.

Pravo na prenosivost trpi određena ograničenja i iznimke pošto se ne može ostvarivati u odnosu na obradu osobnih podataka koju kontrolori provode u okviru svoje javne dužnosti ili prilikom izvršavanja javnih ovlasti. Pravo na prenosivost podataka je regulatorni izraz težnje da se nositelju podataka omogući manipulacija vlastitim osobnim podacima. Tako će nositelj podataka bez ometanja dotadašnjeg kontrolora i bez ulaganja novčanih sredstava moći tražiti da se njegovi osobni podaci dostave drugom kontroloru radi bolje usluge ili zbog nekog drugog razloga.

6.6. Pravo na prigovor

Nakon ulaganja prigovora, kontrolor više ne smije obrađivati osobne podatke nositelja osobnih podataka, osim ako kontrolor dokaže da postoje *uvjerljivi legitimni razlozi za obradu koji nadilaze interese* nositelja osobnih podataka. Pritom se kao uvjerljivi legitimni razlog na strani kontrolora ne može uzeti njegov ekonomski interes kao preovladavajući faktor u odnosu na interes nositelja osobnih podataka[28]. Zbog svoje neprecizne formulacije, imajući u vidu 28 regulatornih tijela i pravosudnih sustava unutar EU (bez obzira na krovne uloge Europskog odbora za zaštitu osobnih podataka kao regulatornog i Suda pravde EU kao sudskog organa), za očekivati je nastajanje različite prakse u konkretnim slučajevima, prouzrokovane različitim tumačenjem.

Kod izravnog marketinga i izrade profila na temelju ovih aktivnosti, nositelj podataka može, također, u svakom trenutku, uložiti prigovor na takvu obradu osobnih podataka, uz obvezu prestanka obrade ako se nositelj podataka eksplicitno protivi obradi. Bez obzira na velike obveze kontrolora po izjavljivanju prigovora, pravo na prigovor nositelja osobnih podataka je iznenađujuće restriktivno postavljeno u Uredbi, dok općeniti prigovor na obradu nije dopušten.

7. Pristanak na obradu

Na prvi pogled, Uredba ima stroge odredbe u odnosu na kontrolore i obrađivače osobnih podataka u slučaju kada se obrada provodi na temelju pristanka nositelja podataka. Međutim, pristanak na obradu osobnih podataka predstavlja samo jednu od propisanih osnova za obradu osobnih podataka građana EU[29]. Temeljna karakteristika obrade osobnih podataka na temelju pristanka nositelja podataka je to da se pristanak može dati samo jasnom radnjom kojom se

[28] Presuda Suda pravde Europske unije br. C-131/12, Google Spain SL & Google Inc. V. AEPD (Agencija za zaštitu osobnih podataka Španjolske) & Mario Costeja Gonzalez, 13. 05. 2014. ("GOOGLE"), § 80: „Imajući u vidu moguću težinu takvog miješanja, nužno je ustvrditi da ono ne može biti opravdano samo ekonomskim interesom operatera takvog pretraživača u toj obradi."

[29] Kao ostale moguće osnove za obradu osobnih podataka pojavljuju se: obrada u vezi sa izvršavanjem ugovora u kojem je nositelj podataka stranka; obrada koja je nužna radi poštovanja pravnih obveza kontrolora; obrada koja je nužna kako bi se zaštitili ključni interesi nositelja podataka ili druge fizičke osobe; obrada koja je nužna za izvršavanje zadaće od javnog interesa od strane kontrolora; obrada koja je nužna za potrebe legitimnih interesa kontrolora ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode nositelja podataka koji zahtijevaju zaštitu osobnih podataka, osobito ako je nositelj podataka dijete.

izražava dobrovoljan, poseban, informiran[30] i nedvosmislen pristanak nositelja podataka na obradu osobnih podataka koji se odnose na njega (npr. pisana izjava)[31]. Nadalje, kontrolor bi trebao moći dokazati da je nositelj podataka dao pristanak za postupak obrade. S druge strane, nositelj podataka u svakom trenutku može povući svoju suglasnost za obradu podataka. S obzirom na vrlo rigorozno postavljene uvjete za obradu osobnih podataka koji se prikupljaju i obrađuju na temelju pristanka nositelja podataka, za očekivati je da će kontrolori radije koristiti druge osnove za obradu osobnih podataka (primjerice *obradu koja je nužna za ostvarenje legitimnih interesa kontrolora*).

8. Dužnosti kontrolora

Prema Uredbi, neke od najvažnijih dužnosti kontrolora i/ili obrađivača su: vođenje evidencija o aktivnostima obrade, suradnja sa nadzornim tijelima, osiguravanje sigurnosti osobnih podataka, izvještavanje nadzornih tijela i nositelja osobnih podataka o načinjenim povredama, izrada procjene učinaka na zaštitu podataka, imenovanje službenika za zaštitu osobnih podataka. U ovom dijelu ću pažnju pokloniti nekima od ovih dužnosti kontrolora kako bih pojasnio o kakvom obimu obveza u vezi sa postupanjem u skladu sa odredbama Uredbe se radi. Podsjećam da je jedan od osnovih motiva donošenja Uredbe kontroliranje postupanja velikih korporacija u vezi sa automatiziranom obradom osobnih podataka.

8.1. Obveza izrade procjene učinka obrade na zaštitu osobnih podataka

Kontrolor je u obvezi izraditi *procjenu učinka obrade osobnih podataka na zaštitu osobnih podataka* ako bi određena vrsta obrade osobnih podataka[32] mogla prouzrokovati *visok* rizik za prava i slobode nositelja osobnih podataka, uz savjetovanje sa službenikom za obradu podataka ukoliko je isti imenovan[33]. Osim visokorizične obrade (termin podložan različitom tumačenju), Uredba propisuje obveznu procjenu učinka obrade u slučaju sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila.

Za razliku od uopćenog propisivanja tehničkih i organizacijskih mjera koje su kontrolori dužni poduzeti u svrhu sigurnosti osobnih podataka, za obvezu izrade procjene učinka su propisani vrlo

[30] Zanimljivo je pitanje ”informiranosti” pristanka na obradu osobnih podataka u kontekstu brojnih kvadratića na internetu (iznad ili ispod kojih se nalazi poduži tekst sa sitnim slovima o pravima, obvezama, odgovornostima i ostalim uvjetima obrade podataka) koje označavamo i tako dajemo svoj pristanak na obradu naših podataka. S pravom se možemo zapitati da li su takve suglasnosti zaista “informirane” u smislu odredaba o pristanku na obradu osobnih podataka. Realnost je takva da će samo poneki strastveni pravnik ili stručnjak za obradu osobnih podataka pročitati cijeli tekst sitnih slova i zapravo analizirati koja su njegova prava, a koje su posljedice označavanja takvog kvadratića. Zbog osjetljivosti i vjerojatno restriktivnog tumačenja davanja pristanka od strane regulatora, većina kontrolora će pokušavati na drugim osnovama doći do osobnih podataka i njihove obrade. Pristanak na obradu osobnih podataka dijete može dati sa navršenih 16 godina (državama članicama se daje mogućnost da propisuju nižu dobnu granicu, ali ne nižu od 13 godina), a mlađe dijete jedino uz dodatno odobrenje roditelja.

[31] Preambula Uredbe navodi da se pismeni pristanak može dati označivanjem polja kvačicom pri posjetu internetskim stranicama ili biranjem tehničkih postavaka usluga informacijskog društva.

[32] Uredba na više mjesta posebno naglašava obradu koja se obavlja putem novih tehnologija.

[33] Osim savjetovanja sa službenikom za obradu osobnih podataka, potrebno je konzultirati nositelja osobnih podataka prije obrade te posavjetovati se sa nadzornim tijelom ako bi obrada mogla dovesti do visokog rizika.

konkretni parametri unatoč činjenici da obrada osobnih podataka može imati najrazličitije pojavne oblike i da je vrlo teško unaprijed odrediti kakve posljedice može izazvati neka vrsta obrade[34].

8.2. Vođenje evidencija

Dužnost je kontrolora da vodi evidenciju o aktivnostima obrade osobnih podataka. Primjerice, kontrolor obrađuje osobne podatke svojih zaposlenicima o kojoj obradi je dužan voditi odgovarajuću evidenciju[35]. S obzirom da je vođenje, a posebno ažuriranje evidencija o obradi osobnih podataka, iznimno zahtjevan posao koji predstavlja administrativni teret za kontrolore, Uredba zauzima vrlo fleksibilan stav u odnosu na ranije zakonodavstvo (ali recimo i važeće BiH propise) te obvezu vođenja evidencija nalaže samo subjektima koji imaju više od 250 zaposlenih[36].

8.3. Sigurnost obrade

Da bi se ostvarila željena sigurnost obrade osobnih podataka, morale bi se poduzeti određene tehničke i organizacijske mjere poput: pseudonimizacije i enkripcije osobnih podataka, sposobnosti pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta, i druge.

Provođenje tehničkih i organizacijskih mjera obrade osobnih podataka u svrhu očuvanja ili ostvarivanja sigurnosti osobnih podataka je postavljeno pretjerano fleksibilno bez odgovarajućih parametara kojima bi se kontrolori mogli voditi prilikom odluke o provođenju određene mjere[37]. Potencijalni rizik predstavljaju i mogući troškovi provedbe pojedine mjere, pa bi se u praksi moglo dogoditi da se pojedina mjera (npr. enkripcija) ne provede zbog pretjeranih troškova.

Kako bi se postigla sigurnost obrade osobnih podataka preporučuje se pribjegavanje metodi pseudonimizacije. Pseudonimizacija je obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom nositelju podataka bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi.

8.4. Izvještavanje nadzornog tijela i nositelja osobnih podataka o povredi osobnih podataka

Jedna od novih stvari koju donosi Uredba, za koju možemo reći da predstavlja veliki administrativni teret za kontrolore, jeste potreba izvještavanja nadzornog tijela, ali i nositelja osobnih podataka, u slučaju da se dogodi kršenja propisa o obradi. U oba slučaja je propisana

[34] Više o tome u čl. 35 Uredbe (bilj. 2).
[35] Više o obveznom sadržaju evidencija u čl. 30 Uredbe (bilj. 2).
[36] Iznimka je ako će obrada vjerojatno prouzročiti visok rizik za prava i slobode nositelja osobnih podataka, ako obrada nije povremena ili uključuje posebne kategorije osobnih podataka ili je riječ o osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima.
[37] Iz čl. 32 Uredbe (bilj. 2) proizilazi da će kontrolor odlučiti koju će mjeru poduzeti i da kontrolorova odluka ovisi o njegovoj autonomnoj procjeni koliki rizik određene aktivnosti obrade predstavljaju za osobne podatke.

obveza obavještavanja u slučaju povrede u roku od 72 sata od trenutka saznanja da se povreda dogodila.

Različito je propisana potreba obavještavanja nadzornog tijela u odnosu obavještavanje nositelja osobnih podataka o nastaloj povredi. Naime, nadzorno tijelo je potrebno obavijesti u slučaju da će povreda prouzrokovati *rizik* za prava i slobode pojedinaca, dok je nositelja osobnih podataka potrebno obavijesti u slučaju da će povreda prouzrokovati *visok rizik* za prava i slobode pojedinaca.

8.5. Posebna pravila koja se odnose na profiliranje

Profiliranje ukratko podrazumijeva automatiziranu obradu osobnih podataka koja se koristi za procjenu određenih karakteristika pojedinca. Svrha takve obrade može biti različita; od ekonomski motiviranih radnji profiliranja (poput internet oglašivača), onih koje se provode u svrhe efikasnog upravljanja ljudskim resursima u velikim kompanijama, pa do onih motiviranih razlozima javnog zdravstva ili sprječavanja terorističkih napada. Iako profiliranje općenito ima negativnu konotaciju, ono može biti vrlo korisno. Naime, uz pomoć profiliranja mogu se odrediti rizične skupine osoba od kojih prijeti opasnost da će izvršiti, pripremiti ili možda financirati teroristički napad. Takva vrsta profiliranja u demokratskom društvu nikome zapravo i ne smeta. Sa druge strane, svatko od nas na osobnom primjeru može potvrditi da je "meta" oglašivača koji su vrlo dobro upućeni u afinitete i interese povezane sa našim IP adresama, a sve na osnovu povijesti pretraga provedenih na internetu. Takvi oglašivači obrađuju masu podataka, uključujući i osobne podatake, koje svjesno ili nesvjesno ostavljamo prilikom pretraživanja interneta[38].

Da bi se uvela kontrola u ovu oblast, Uredba propisuje pravo nositelja podataka da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, uz izuzetke ako je odluka npr. potrebna za izvršavanje ugovora između nositelja podataka i kontrolora ili se temelji na izričitom pristanku nositelja podataka[39].

Zanimljiva je formulacija za koju su se odlučili kreatori uredbe jer se njome "daje pravo" nositelju podataka da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi. Veoma je jasno da se ne radi o kogentnoj pravnoj normi kojom se (s druge strane) kontrolorima brani da donose odluke na osnovu automatizirane obrade. Dakle, kontrolorovo je pravo da izrađuje profile nositelja podataka sve do trenutka dok nositelj podataka u smislu članka 21 Uredbe ne uloži prigovor na takvu obradu.

8.6. Imenovanje službenika za zaštitu osobnih podataka

Uredba propisuje obvezno imenovanje službenika za zaštitu osobnih podataka u slučaju kada obradu provodi tijelo javne vlasti, osnovne djelatnosti kontrolora ili obrađivača se sastoje od postupaka obrade koji znače sustavno redovno praćenje nositelja osobnih podataka, te kada se

[38] Online bankarstvo počiva na profiliranju – na osnovu profila se donosi automatizirana odluka o kreditnoj sposobnosti, pa će kreditno sposobni profil moći dobiti kredit, dok onaj kreditno nesposobni to neće moći.
[39] U navedenim izuzetnim situacijama, moraju se provesti odgovarajuće zaštitne mjere za prava i slobode nositelja osobnih podataka poput prava na ljudsku intervenciju ili prava na izražavanje vlastitog stajališta.

osnovne djelatnosti kontrolora ili obrađivača sastoje od opsežne obrade posebnih kategorija osobnih podataka.

9. Dužnosti obrađivača

Kao što sam već naveo, ranije europsko zakonodavstvo (kao uostalom i važeće bosanskohercegovačko) nije propisivalo odgovornost za nezakonitu obradu osobnih podataka u mjeri u kojoj je za takvu obradu bio odgovoran kontrolor. Regulator bi u slučaju kršenja prava zaštite osobnih podataka od strane obrađivača na odgovornost pozvao isključivo kontrolora koji je obradu ustupio obrađivaču. Takav pristup zakonodavca nije bio izbalansiran i predstavljao je nesrazmjeran teret na leđima kontrolora kojemu su usluge obrađivača bile potrebne, ali on osim potpisanog ugovora sa obrađivačem nije imao adekvatan mehanizam utjecaja na ponašanje obrađivača.

Novo europsko zakonodavstvo donosi dobro rješenje tako što jasno razdvaja odgovornost kontrolora i obrađivača na način da obrađivač postaje objekt nadzora od strane regulatornih tijela u punom smislu tih riječi. Ne smije se dopustiti obrađivačima da se kriju iza kontrolora i na taj načina budu amnestirani za nesavjesno ponašanje i kršenje propisa o zaštiti osobnih podataka, a da kontrolori istovremeno plaćaju cijenu takvog ponašanja obrađivača. Osim što je odgovoran za pravilnu obradu osobnih podataka, obrađivač je prema Uredbi dužan provesti sve mjere zaštite osobnih podataka, uključujući tehničke i organizacijske mjere u svrhu sigurnosti obrade podataka.

10. Transfer osobnih podataka u treće zemlje

Transfer osobnih podataka građana EU u treće zemlje je prvorazredno pitanje zaštite osobnih podataka s obzirom na rizike povezane sa nemogućnošću kontroliranja zakonodavnih, upravnih i sudskih procesa povezanih sa zaštitom osobnih podataka u trećim zemljama u koje se prenose osobni podaci. Transfer osobnih podataka u treće zemlje predstavlja poseban izazov, jer je u isto vrijeme važno osigurati slobodan, brz i efikasan prijenos osobnih podataka ali i visoku razinu zaštite osobnih podataka. Sam naziv Uredbe sadrži "slobodni protok osobnih podataka" što svjedoči da je prijenos osobnih podataka jedan od njenih temeljnih ciljeva.

U periodu prije donošenja Uredbe može se reći da je vladala pravna nesigurnost (za standard EU i anarhija) kada je u pitanju transfer podataka građana EU u treće zemlje. Ilustrativni primjer takvoga stanja pruža *Sporazum o legalnom transferu o ličnosti između EU i SAD-a* pod nazivom *"Sigurna luka"* o kojem je Europska komisija donijela odluku broj 2000/520 kojom je potvrdila da SAD pruža odgovarajući nivo zaštite osobnih podataka[40]. Ovaj i slični slučajevi (prvenstveno

[40] Poznata je odluka Suda pravde EU C-362/14, SCHREMS V. DATA PROTECTION COMMISSIONER, 06. 10. 2015 ("SCHREMS") koja je bila jedan od pokretača za Europsku komisiju i ostale aktere donošenja Uredbe da precizno i sveobuhvatno urede pitanje transfera osobnih podataka svojih građana izvan EU. U odluci se radilo o zahtjevu austrijskog državljanina koji je 2008. godine sklopio ugovor sa Facebook Irska koji je podružnica Facebook Inc. sa sjedištem u SAD-u. Podnositelj zahtjeva je tražio da Facebook Irska prestane sa prijenosom njegovih osobnih podataka u Facebook Inc. zbog činjenice da Facebook Inc. ne provodi dovoljne mjere zaštite od nadzornih aktivnosti nad ovim osobnim podacima koje vrši Nacionalna sigurnosna agencija (NSA). Irski komesar za zaštitu osobnih podataka se nije smatrao nadležnim za ovo pitanje s obzirom da je Europska komisija ocijenila da SAD provode adekvatne mjere zaštite u okviru programa "Sigurna luka". Sud pravde EU je u ovom slučaju poništio

slučaj Google), pokazali su svu nemoć, neefikasnost i dotrajalost sustava zaštite osobnih podataka EU koji je uspostavljen Direktivom i nacionalnim propisima još 1995. godine, te su potaknuli žustru raspravu o potrebi uvođenja jasnih (i strožih) pravila o transferima osobnih podataka u treće zemlje. Poglavlje V – prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama na vrlo precizan i sveobuhvatan način propisuje pitanje prijenosa osobnih podataka izvan EU.

Transfer osobnih podataka građana EU u treću zemlju ili međunarodnu organizaciju se može izvršiti ako postoji odobrenje Europske komisije koje predviđa da određena zemlja osigurava primjerenu razinu zaštite osobnih podataka ili ako kontrolor provodi odgovarajuće zaštitne mjere u obradi osobnih podataka. U nedostatku odobrenja ili odgovarajućih zaštitnih mjera, transfer će se moći izvršiti u izuzetnim, strogo propisanim situacijama.

Prijenos osobnih podataka na temelju odobrenja Europske komisije podrazumijeva njenu odluku da određena zemlja, pojedini sektori unutar te zemlje ili međunarodna organizacija osigurava primjerenu razinu zaštite osobnih podataka[41]. Osim prijenosa na temelju odluke Europske komisije, transfer osobnih podataka će biti moguće izvršiti i pod uvjetom da su kontrolor ili obrađivač predvidjeli odgovarajuće zaštitne mjere poput obvezujućih korporativnih pravila, standardnih klauzula o zaštiti podataka koje donosi Komisija, odobrenog kodeksa ponašanja ili odobrenog mehanizma certificiranja, te da je nositeljima osobnih podataka omogućena sudska zaštita.

U slučaju da Europska komisija nije donijela odluku o primjerenosti treće države ili međunarodne organizacije ili ako nisu provedene odgovarajuće zaštitne mjere od strane kontrolora (npr. obvezujuća korporativna pravila), transfer osobnih podataka u treću zemlju će se ipak moći provesti u izuzetnim, strogo ograničenim situacijama[42].

11. Utjecaj Uredbe na poslovanje gospodarskih subjekata

Pravno okruženje koje diktira nova Uredba karakterizira visok stupanj uređenosti (određeni dijelovi Uredbe u potpunosti slijede logiku provedbenih akata), predvidivosti i pravne sigurnosti za sve aktere uz propisivanje ekstremno visokih kazni za nepoštivanje Uredbe. U takvom okruženju posebno se nameće pitanje položaja gospodarskih subjekata u odnosu na obveze koje za njih proizilaze iz teksta Uredbe, te učinak koji će novi okvir imati na njihovo poslovanje.

---

odluku Europske komisije 2000/520 jer se tom odlukom dopustilo subjektima u SAD-u da u slučaju "sukoba" između programa "Sigurne luke" i nacionalnih propisa, mogu odabrati da postupaju u skladu sa nacionalnim propisima, dok sama sporna odluka ne sadrži objašnjenja o nacionalnim propisima SAD-a, odnosno da li ti propisi, s obzirom da pod određenim uvjetima mogu biti izravno primijenjivi na obradu osobnih podataka građana EU, osiguravaju adekvatan nivo zaštite njihovih osobnih podataka. U istoj odluci Sud pravde EU nalazi da vlasti SAD-a mogu pristupiti transferiranim osobnim podacima i obrađivati ih mimo svrhe zbog koje su transferirani, odnosno mimo potreba nacionalne sigurnosti pri čemu nositelji osobnih podataka nemaju adekvatna prava na zaštitu, poput prava na prigovor ili brisanje. Sud zaključuje da generalni pristup sadržajima elektroničke komunikacije koji sadrže osobne podatke, od strane vlasti, narušava srž poštivanja osnovnog prava na poštivanje privatnog života.

[41] Više o kriterijima na osnovu kojih Europska komisija donosi odluku o tome koja zemlja ili međunarodna organizacija osigurava primjerenu razinu zaštite osobnih podataka u čl. 45 Uredbe (bilj. 2).

[42] Detaljnije o tome u čl. 49 Uredbe (bilj. 2).

Od samog usvajanja Uredbe, određeni EU-centrični ekonomski analitičari brane stav da će primjena Uredbe donijeti značajne ekonomske blagodati za gospodarske subjekte, s obzirom da će gospodarski subjekti koji posluju na teritoriji više država članica EU sada biti u stanju unificirati svoje poslovanje u dijelu obrade osobnih podataka. Također, opravdano se ističe da su u prostor obrade osobnih podataka sada unesena jasna pravila prilagođena novom digitaliziranom vremenu[43], te da će Uredba doprinijeti bržem i efikasnijem protoku osobnih podataka što će poduprijeti konkurentnost gospodarskih subjekata iz EU na globalnom tržištu.

Unatoč znatnim administrativnim opterećenjima za njihovo poslovanje, Uredba bi trebala djelovati vrlo povoljno na poslovanje velikih igrača na tržištu EU koji imaju svoja sjedišta u više država članica, ali i izvan EU. Puna primjena Uredbe za njih ne bi trebala predstavljati pretjerani administrativni teret u odnosu na koristi koje im Uredba donosi[44]. Valja naglasiti i da Uredba nije uvijek kategorična, a njene odredbe kogentne i apsolutne. To je i razumljivo jer se ne može očekivati da kontrolor ili obrađivač ulažu pretjerane napore u provođenje zaštite obrade osobnih podataka, posebno ako je očigledno da takva obrada neće dovesti do kršenja prava i sloboda nositelja podataka[45]. Međutim, opravdana je bojazan da bi poslovanje malih i srednjih poduzeća moglo biti izloženo negativnom utjecaju birokratskih opterećenja[46]. Mali i srednji subjekti (čak ni fizička lica) nisu izuzeti od potpunog provođenja Uredba pa će oni, bez obzira na trenutnu poslovnu situaciju, biti u obvezi voditi evidencije o obradi podataka, udovoljavati zahtjevima nositelja podataka (npr. pravo na zaborav, ispravku, ili prenosivost podataka), obavještavati nadzorna tijela i nositelje podataka o rizičnim aktivnostima obrade, izrađivati i ažurirati procjene učinka obrade na zaštitu osobnih podataka, pa čak i zaposliti službenika za obradu osobnih podataka.

[43] U priopćenju Europskog parlamenta od 14. 04. 2016. navodi se da je jedan od ciljeva Uredbe stvaranje visoke i jedinstvene razine zaštite podataka u EU, spremne da odgovori zahtjevima digitalnog vremena. Priopćenje dostupno na: http://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era, očitanje: 07. 12. 2017.

[44] U informaciji KPMG-a Danske objavljenom 02. 10. 2017. psotavlja se pitanje koristi koje multinacionalne korporacije imaju od Uredbe. Zaključak je da će novi okvir doprinijeti efikasnosti sustava zaštite podataka na razini ovih korporacija, kao i da će jedinstveni okvir značiti velike uštede. Tekst je dostupan na: https://home.kpmg.com/dk/en/home/insights/2017/09/the-general-data-protection-regulation-brings-good-news-for-mult.html, očitanje 07. 12. 2017. Dodatna pogodnost za multinacionalne korporacije su tzv. *obvezujuća korporativna pravila* koja predstavljaju odgovarajuću zaštitnu mjeru u funkciji valjanog transfera osobnih podataka u treću zemlju koja ne ispunjava uvjet primjerenosti zaštite osobnih podataka. Ova mjera podrazumijeva mogućnost da gospodarski subjekt iz države članice EU prenosi osobne podatke povezanom licu u trećoj zemlji koja ne provodi adekvatne mjere zaštite osobnih podataka, pod uvjetom da su na razini grupacije poduzeća usvojena obvezujuća korporativna pravila koja predstavljaju nadomjestak za nedostajuća pravila i standard zaštite osobnih podataka u toj trećoj zemlji.

[45] Tako se na nekoliko mjesta u Uredbi propisuju izuzeci od obveze provođenja nekih odredaba ako bi to za kontrolora prouzrokovalo pretjerani napor kao npr. u slučaju pružanja informacija o obradi ako podaci nisu prikupljeni od nositelja podataka, zatim kod obveze obavještavanja primatelja podataka o svakoj ispravci, brisanju ili ograničavanju obrade te u slučaju obavještavanja nositelja podataka o povredi njegovih osobnih podataka.

[46] Članak u Financial Timesu objavljen pod nazivom: *„Data protection: Brussels' heavy hand on Europe's digital economy“*, problematizira pitanje opterećenja poslovnih subjekata Uredbom. Dostupno na: https://www.ft.com/content/777a1d34-ceb4-11e7-b781-794ce08b24dc, očitanje: 07. 12. 2017.

12. Usporedba Uredbe i trenutnog okvira zaštite osobnih podataka u BiH

Postojeći pravni okvir zaštite osobnih podataka u Bosni i Hercegovini je kompatibilan sa trenutno važećim pravnim okvirom Europske Unije, tako da odnos pravnog okvira zaštite podataka u BiH i Uredbe možemo promatrati jednako kao odnos ranijeg i novog pravnog okvira unutar same EU. Važeći Zakon o zaštiti osobnih podataka BiH[47] sadrži pojmove i institute inherentne standardnim pravnim okvirima zaštite osobnih podataka, poput obrade običnih i posebnih kategorija osobnih podataka, obrade uz i bez suglasnosti nositelja osobnih podataka, prijenosa osobnih podataka u treće zemlje, prava nositelja osobnih podataka, donošenja odluke na osnovu automatske obrade osobnih podataka i dr.

Međutim, donošenjem Uredbe, EU pravi značajan iskorak na ovom planu u odnosu na veliki dio ostatka svijeta, pa tako i BiH. Primjenom Uredbe, postaje vrlo upitno da li će Europska komisija odobriti BiH kao zemlju koja primijenjuje adekvatne mjere zaštite osobnih podataka, a koje su uvjet da bi pravni subjekti iz EU transferirali osobne podatke u BiH. Uredba ne donosi nešto sasvim novo (pravo zaštite osobnih podataka vuče korijene još od kraja drugog svjetskog rata), ali ona predstavlja sveobuhvatnu nadogradnju postojećih praktičnih i teorijskih rješenja u oblasti obrade i zaštite osobnih podataka i njihove zaštite i može dati odgovore na izazove digitalnog vremena. Razumije se da bi adekvatna zaštita osobnih podataka građana EU značila osiguravanje razine zaštite poput one u EU (ili barem približne), bez obzira gdje se ti osobni podaci transferiraju.

Općenito gledajući, stanje zaštite osobnih podataka u Bosni i Hercegovini ne ide dalje od relativno kvalitetnog pravnog okvira koji će se morati dodatno nadograditi zbog približavanja Bosne i Hercegovine Europskoj uniji u skladu sa *Sporazumom o stabilizaciji i pridruživanju*[48], ali i zbog omogućavanja primjerene razine zaštite osobnih podataka u odnosu na EU. Naime, kao što je to slučaj i sa drugim vrstama ljudskih prava u post-dejtonskoj BiH, građani BiH i njene institucije imaju malu ili nikakvu svijest o tome što je to zapravo zaštita osobnih podataka, koja su prava nositelja podataka, a koje su obveze onih koji te osobne podatke obrađuju i zbog čega i od koga se osobni podaci štite. Kakav god pravni okvir zaštite osobnih podataka bio, on će biti mrtvo slovo na papiru sve dok kao društvo ne budemo u stanju formirati, razviti i njegovati *kulturu zaštite osobnih podataka*. Pukom internetskom pretragom odluka Agencije za zaštitu osobnih podataka BiH, može se doći do najrazličitijih informacija o kršenjima osobnih podataka i to prvenstveno od strane državnih institucija koje bi trebale davati primjer ponašanja u skladu sa zakonima ove države. Pritom se ne radi o sofisticiranim kršenjima obrade osobnih podataka uzrokovanim manjkavostima softvera ili pogrešnim tumačenjima nejasnih pravnih normi, već se radi o kršenjima karakterističnim za društva niske razine kulture zaštite osobnih podataka. Tako se, vrlo često, događa da institucije objavljuju osobne podatke koji se očigledno ne bi smjeli objaviti, traže dokumentaciju koja nije potrebna u natječajnom postupku ili obrađuju osobne podatke mimo svrhe u koju su prikupljeni.

Na ovom mjestu se ipak neću detaljnije baviti faktičkim stanjem zaštite osobnih podataka u Bosni i Hercegovini, već ću pokušati izložiti najvažnije normativne razlike između Uredbe i BiH pravnog okvira.

[47] *Sl. gl. BiH* 49/06, 76/11 i 89/11.
[48] Puni naziv: Sporazum o stabilizaciji i pridruživanju između Evropskih zajednica i njihovih država članica, sa jedne strane i Bosne i Hercegovine, sa druge strane, *Sl. gl. BiH – Međunarodni ugovori* 10/08.

Za razliku od Uredbe koja, kako je već rečeno, proširuje spektar prava nositelja osobnih podataka i uz to nositelju osobnih podataka dodjeljuje ulogu subjekta koji se svojim pravima može koristiti aktivno, brzo i efikasno, u postojećem pravnom okviru BiH, nositelj osobnih podataka ima klasična prava poput prava na prigovor, održavanje autentičnosti podataka, pristupa osobnim podacima te obavještavanja o prikupljanju osobnih podataka. U tom kontekstu nositelj osobnih podataka u BiH je više objekt zaštite koji samo do neke mjere može utjecati na stanje svojih osobnih podataka (npr. može provjeravati njihovu autentičnost), ali je ograničen u pogledu poduzimanja konkretnih mjera koje se mogu provesti u odnosu na njegove podatke. Prava nositelja podataka u pravnom okviru Bosne i Hercegovine su apstraktna i podložna (pre)širokoj interpretaciji. Osim toga, ona nisu prilagođena novoj društvenoj realnosti. Uspoređujući prava nositelja osobnih podataka u BiH sa pravima iz Uredbe, opravdano se nameće pitanje da li sadašnji pravni okvir u BiH ispunjava kriterij kvalitete zakona u smislu njegove usklađenosti sa Ustavom BiH i Europskom konvencijom u dijelu prava na privatnost, ako pojedinac ne može aktivno, brzo i efikasno (kao što je to slučaj u EU) utjecati na obradu svojih osobnih podataka. Realna je mogućnost da će i Europski sud za ljudska prava kao minimalni standard zaštite prava osobnih podataka usvojiti standarde zaštite osobnih podataka iz Uredbe. Za Bosnu i Hercegovinu bi to moglo značiti potrebu usklađivanja Zakona o zaštiti osobnih podataka sa Ustavom BiH s obzirom na položaj Europske konvencije u ustavnom sustavu BiH.

Kada su u pitanju dužnosti kontrolora i obrađivača, u Bosni i Hercegovini se one svode na poduzimanje tehničkih i organizacijskih mjera, bez dovoljno konkretnog propisivanja o kakvim bi se mjerama za zaštitu radilo. Uredba povećava dužnosti kontrolora i obrađivača radi bolje zaštite osobnih podataka. Tako su kontrolori i obrađivači dužni izraditi procjenu učinka obrade na zaštitu osobnih podataka, voditi evidencije o aktivnostima obrade, izvještavati nadzorna tijela i nositelje osobnih podataka o povredi osobnih podataka, te imenovati službenika za zaštitu osobnih podataka. Kontrolori i obrađivači imaju i velike obveze kod procesuiranja prigovora nositelja osobnih podataka, a za kršenje Uredbe su izloženi veoma visokim novčanim kaznama. U Bosni i Hercegovini kontrolori nemaju dužnost izraditi procjenu učinka obrade na zaštitu osobnih podataka, izvještavati nadzorni organ i nositelja podataka u slučaju povrede osobnih podataka, niti imenovati službenika za zaštitu osobnih podataka.

Dojam je da su kontrolori dužni usvojiti samo tehničke i organizacijske mjere za zaštitu osobnih podataka, ali nije jasno koje su to mjere dovoljne da bi se postigla zadovoljavajuća razina zaštite podataka. Kako bi se postigla zadovoljavajuća razina zaštite osobnih podataka, od presudne je važnosti da su obveze kontrolora šire i konkretnije određene. Fleksibilan pristup Uredbe određenju dužnosti kontrolora i obrađivača bi bilo dobro slijediti i prilikom reforme ove oblasti u BiH. Za razliku od EU, u BiH su obveze kontrolora propisane uglavnom općenito bez obzira na kontekst, svrhu, vrstu ili obim obrade. Primjerice, kontrolor je dužan voditi evidenciju o svakoj vrsti obrade osobnih podataka, bez obzira da li se takvom obradom prouzrokuje rizik za prava i slobode pojedinaca ili se radi o potpuno bezazlenoj obradi osobnih podataka. Uredba, pak, pojednostavljuje procedure, smanjuje birokraciju i olakšava kontrolorima njihove obveze u vezi sa zaštitom podataka. Tako će kontrolor biti u obvezi imenovati službenika za obradu osobnih podataka *ako je kontrolor tijelo javne vlasti, ili obrađuje osobne podatke na način da sustavno i redovno prati ponašanje nositelja podataka*. Kontrolor će, nadalje, biti dužan izvijestiti nadzorno tijelo i nositelja osobnih podataka o nastaloj povredi *ako je njome nastao rizik za prava i slobode pojedinaca*. Također, kontrolor će biti dužan izraditi procjenu učinka obrade na zaštitu osobnih

podataka *pod uvjetom da bi određena obrada osobnih podataka mogla prouzrokovati veliki rizik za prava i slobode nositelja osobnih podataka*. Konačno, kontrolor će biti u obvezi voditi evidencije o aktivnostima obrade *pod uvjetom da zapošljava više od 250 osoba, odnosno da je obrada osobnih podataka rizična*. Da bismo imali konkurentno gospodarstvo na tržištu u kojem je osnovni podatak glavna sirovina, zaštita podataka ne smije biti apsolutna, jer će kao takva biti smetnja razvoju gospodarstva. Zaštita podataka bi trebala biti srazmjerna cilju koji se njome želi postići, uz posebno uvažavanje interesa gospodarstva i nacionalne sigurnosti.

Odgovornost za kršenje obrade osobnih podataka od strane obrađivača u BiH snosi isključivo kontrolor koji od obrađivača može eventualno potraživati naknadu štete po općim pravilima obveznog prava.

U Bosni i Hercegovini obrađivač nije subjekt nadzora u punom smislu riječi, jer nema nikakve obveze prema nadzornom tijelu i nositeljima osobnih podataka. Uredba potpuno opravdano uvodi odgovornost obrađivača koji za povrede odgovara identično kao i kontrolor. Osim odgovornosti, Uredba gotovo u potpunosti prenosi sve dužnosti koje su ranije važile samo za obrađivača. Pitanje odgovornosti obrađivača (a potom i posredne odgovornosti kontrolora za aktivnosti obrađivača) u BiH je „siva zona“ sustava zaštite osobnih podataka. Ugovorom između kontrolora i obrađivača se definiraju najvažniji elementi zakonite obrade podataka. Problem predstavlja utvrđivanje odgovornosti u slučaju povrede osobnih podataka od strane obrađivača. U tom slučaju se ne može govoriti o namjeri ili nepažnji kontrolora, pa se postavlja pitanje opravdanosti prenošenja odgovornosti na kontrolora za povrede koje je počinio obrađivač. Ovakav pristup obično rezultira eskiviranjem odgovornosti od strane aktera, pri čemu se kontrolor poziva na ugovorne obveze obrađivača, a obrađivač se poziva na zakonom utvrđenu odgovornost kontrolora za nastale povrede.

Jedna od glavnih razlika između Uredbe i BiH zakonodavstva je da Uredba prepoznaje realne rizike digitalnog vremena poput automatizirane obrade podataka koja uključuje profiliranje[49], obrade osobnih podataka djece, zaštitne mjere poput pseudonimizacije te prava nositelja podataka poput prava na prenosivost podataka. Nositelj osobnih podataka u BiH trenutno nema mogućnost prigovor podnijeti automatiziranim putem, koristiti se pravom na zaborav, niti od kontrolora zatražiti da njegove osobne podatake automatskim putem dostavi drugom kontroloru radi ostvarenja određenih interesa nositelja podataka. Pitanje obrade osobnih podataka djece u odnosu na usluge informacijskog društva (čest primjer su profili djece na društvenim mrežama) pravni okvir u BiH uopće ne dotiče. Sve to je rezultat činjenice da naš pravni okvir zaštite osobnih podataka datira još iz 2006. godine, uz izmjene koje su se dogodile posljednji put 2011. godine. Propis prilagođen digitalnom dobu bi bio od koristi za sve sudionike procesa obrade podataka u BiH. Nositelji osobnih podataka bi bili dodatno zaštićeni mjerama poput pseudonimizacije ili enkripcije te mjerama vezanim za profiliranje. Poslovni subjekti ili državni organi bi dobili okvir koji bi omogućio brži i efikasniji promet osobnih podataka, a nadzorni organi bi konačno dobili alate pomoću kojih bi se mogli suprotstaviti povredama osobnih podataka karakterističnim za digitalni svijet, a što sada nisu u mogućnosti. Iako spada među slabije razvijene europske države, BiH je uvelike dio digitalne revolucije. Raste udio informatički pismenog stanovništa, kao i broj digitalnih uređaja pomoću kojih građani dijele

[49] Čl. 29 Zakona o zaštiti osobnih podataka BiH (bilj. 47) zabranjuje donošenje odluke zasnovane na automatskoj obradi osobnih podataka. Uredba to ne zabranjuje, već nositelju podataka daje pravo da se usprotivi tzv. profiliranju.

svoje osobne podatke[50]. Državne institucije, javna i privatna poduzeća već odavno provode informatizaciju svojih sustava sa posebnim naglaskom na efikasnu obradu podataka. Vlast bi morala prepoznati ova društvena kretanja i brzo reagirati sa usvajanjem pravnog okvira primjerenog za digitalno vrijeme.

Za razliku od Uredbe koja transfer osobnih podataka propisuje veoma precizno i sveobuhvatno, BiH zakonodavstvo u samo jednom članku (i to vrlo uopćeno) propisuje ovo prvorazredno pravno pitanje ostavljajući ovo područje pravno neuređenim i podložnim (pre)širokim tumačenjima upravne i sudske vlasti (slično kao što je bilo u EU prije Uredbe). Pitanje transfera osobnih podataka iz BiH nije riješeno propisivanjem obveze nadzornom tijelu (ili resornom ministarstvu) da utvrdi koja zemlja ili međunarodna organizacija osigurava primjerenu razinu zaštite osobnim podataka, odnosno da periodično provjerava stanje zaštite u tim zemljama ili međunarodnim organizacijama. Umjesto toga, ostavljeno je kontroloru da sam procijeni da li neka zemlja osigurava primjerenu razinu zaštite osobnih podataka. Ova materija je vrlo rizična za osobne podatke jer izvozom osobnih podataka u zemlju koja nema odgovarajuće standarde zaštite osobnih podataka, ti osobni podaci postaju izloženi proizvoljnosti kontrolora ili obrađivača, a BiH regulatorni organ nema ingerencije za obradu izvan granica BiH. Ne može se govoriti o adekvatnoj zaštiti osobnih podataka građana BiH ako su ti podaci zaštićeni samo u granicama BiH i prepušteni proizvoljnosti kada napuste BiH. Praćenje osobnih podataka i izvan granica prvobitno nadležne jurisdikcije je standard koji usvaja Uredba i koji se čini opravdanim. Da bi se moglo govoriti o odgovarajućim standardima zaštite osobnih podataka u BiH, morao bi se regulirati transfer osobnih podataka tako da se nakon izvršenog transfera može osigurati njihova zakonita obrada.

S druge strane, od donošenja Uredbe je postalo upitno da li će BiH biti zemlja u koju će EU subjekti moći izvoziti osobne podatke[51]. Od svog osnivanja, Europska unija postavlja standarde ponašanja. Tako je i sa zaštitom osobnih podataka. Od trenutka primjene Uredbe, surađivati sa subjektima EU moći će samo oni koji prate standarde postavljene u Uredbi, što nedvojbeno proizlazi iz odredaba o prijenosu podataka u treće zemlje. Zakonodavac u Bosni i Hercegovini u ovom trenutku ne pokazuje zainteresiranost da prati ove standarde čime dovodi u pitanje mogućnost da se u nju izvoze osobni podaci građana EU. To može imati dalekosežne posljedice za tzv. „europski put“ Bosne i Hercegovine, ali i njen ekonomski položaj. Bez slobodnog prijenosa osobnih podataka u današnje vrijeme nema ekonomske razmjene većeg obima. Osim opasnosti koja proizilazi iz neusklađenosti sa Uredbom, važno je istaknuti da će razina zaštite osobnih podataka građana BiH od trenutka primjene Uredbe postati neadekvatna. Prilikom donošenja odluke o tome da li BiH osigurava primjerenu zaštitu osobnih podataka, Europska komisija će u obzir uzeti zakonodavstvo i primjenu zakonodavstva u praksi. Zbog svega navedenog, važno je da Vijeće Ministara BiH prepozna važnost reforme u ovom sektoru i da inicira proceduru izrade nacrta zakonskog rješenja koje će omogućiti barem primjerenu razinu zaštite osobnih podataka, ali i veća prava za građane čiji su podaci predmet obrade.

[50] Prema Godišnjem izvještaju Regulatorne agencije za telekomunikacije Bosne i Hercegovine za 2016. broj korisnika interneta se povećao sa 2.113.100 u 2011. godini, na 2.909.236 u 2016. godini. Godišnji izvještaji RAK-a dostupni na: http://www.rak.ba/bos/index.php?uid=1272548129, očitanje: 07. 12. 2017.

[51] U Izvještaju Europske komisije o napretku BiH za 2016. godinu se navodi da je zaštita osobnih podataka u BiH djelimično usklađena sa europskim standardima. S obzirom da primjena Uredbe počinje 2018. godine, postavlja se pitanje kakav će stav Europska komisija zauzeti u budućim izvještajima u odnosu na zaštitu osobnih podataka u BiH, a u svjetlu novog okvira u EU.

13. Zaključak

Nova Uredba usvaja visoke standarde zaštite osobnih podataka u Europskoj uniji. Novi europski okvir zaštite podataka otvara mogućnost razvoja ekonomije Unije, uz inzistiranje na zaštiti podataka pojedinaca. Stoga, Unijin zakonodavac nije zainteresiran samo za zaštitu osobnih podataka na teritoriji Unije, već i za njihovu zaštitu u slučaju daljnjeg prijenosa izvan granica Unije. To znači da će Unija tolerirati izvoz osobnih podataka u treće zemlje samo pod uvjetom da ove zemlje osiguravaju odgovarajuću razinu zaštite osobnih podataka. Ova analiza pokazuje da će Bosna i Hercegovina morati djelovati vrlo brzo i reformirati svoj pravni okvir zaštite osobnih podataka ukoliko želi ostati politički i ekonomski povezana sa Unijom. U tom smislu, Bosna i Hercegovina bi posredstvom novog zakonodavnog okvira trebala težiti da postane „sigurna država“ za osobne podatke koji dolaze iz zemalja EU. Osim što nije u dovoljnoj mjeri kompatibilan sa novom Uredbom, naš zakonodavni okvir zaštite osobnih podataka nije prilagođen novom digitalnom vremenu jer ne može jamčiti zaštitu privatnosti u okolnostima masovne obrade osobnih podataka. Reforma zaštite osobnih podataka u Bosni i Hercegovini bi se trebala provoditi na novim društvenim osnovama koje pretpostavlja digitalno doba. Građani bi trebali dobiti veću moć i kontrolu u odnosu na njihove osobne podatke, dok bi dužnosti i obveze kontrolora i obrađivača trebale biti strožije propisane. Osim postizanja kompatibilnosti sa Uredbom, Bosna i Hercegovina bi trebala, slijedeći Unijin model, usvojiti novi okvir zaštite podataka koji bi omogućio ekonomski rast i višu razinu nacionalne sigurnosti, ali istovremeno i visok stupanj zaštite privatnosti pojedinca.

Summary

The EU General Data Protection Regulation with a view to the compatibility of the BiH personal data protection system with the new European framework

The new Regulation on data protection in EU sets up high standards of protection of its citizens private data. The new European framework pushes for growth of the EU's economy, while persisting with high level of personal data respecting. Therefore, EU regulators are not interested just for protecting of data inside of the EU, but they also wanted these data to be secured in case of transfer. It means that EU will tolerate data export outside the EU only to third countries witih an adequate level of data protection. This analysis shows that Bosnia and Herzegovina should act very quickly with reforming its data protection framework, especially if it wants to stay politically and economically tied with EU. Therefore, Bosnia and Herzegovina should aim to become "safe country" for European data by adopting new adequate framework. Besides, current Bosnia and Herzegovina framework is not customized for new digital age because it cannot guarantee privacy and data protection in new circumstances. Data protection reform in Bosnia and Herzegovina should be grounded on new social environment. Citizens should be provided with more power and control of their data, while duties of controllers and processors should be strictly prescribed. Besides harmonising with EU framework for mentioned reasons, Bosnia and Herzegovina should, by following European model, adopt new data protection framework, which could generate an economic growth, anchoring of nacional security while setting up high level of respecting personal data.