MOTIVI I IMPLIKACIJE GDPR UREDBE

MOTIVES AND IMPLICATIONS OF THE GDPR REGULATION

Džemal Kulašin*

ABSTRAKT

Cilj ovog rada je da se predstave motivi donošenja sveobuhvatne regulative u oblasti zaštite ličnih podataka, kao i njene implikacije koje su uslijedile nakon formalnog stupanja na snagu. Naime, regulativa imenovana kao GDPR uredba obavezala je kompanije na adekvatnu zaštitu ličnih podataka svojih klijenata, sa krajnjim ciljem njihove zaštite od (komercijalne) zloupotrebe. U radu se predstavljaju i krajnje ozbiljne implikacije Uredbe u smislu izricanja visokih novčanih kazni kompanijama u kojima su odgovarajuća nacionalna tijela pokazala i dokazala kršenja pojedinih GDPR odredbi.

Ključne riječi: GDPR uredba, lični podaci, zaštita, sankcije

ABSTRACT

The aim of this paper is to present the motives for the adoption of comprehensive regulations in the field of personal data protection, as well as its implications that followed the formal entry into force. Namely, the regulation named as the GDPR regulation obliged companies to adequately protect the personal data of their clients, with the ultimate goal of protecting them from (commercial) misuse. The paper also presents the extremely serious implications of the regulation in terms of imposing high fines on companies in which the relevant national authorities have shown and proved violations of certain GDPR provisions.

Keywords: GDPR regulation, personal data, protection, penalties

UVOD

Privatnost i zaštita ličnih podataka nisu nikada u ljudskoj povijesti bili toliko eksponirani kao zadnjih desetak godina, naglim razvojem web-a, a posebno društvenih mreža. Dok, sa jedne strane, možemo govoriti o nepromišljenim ponašanjima korisnika, koji na taj način direktno ugrožavaju svoju privatnost, lične podatke i integritet, još je više zabrinjavajuće ponašanje kompanija koje se u osnovi bave (velikim) podacima, odnosno potencijalnim zloupotrebama različitih, pa i ličnih podataka svojih korisnika. Nije rijedak slučaj da ove kompanije, imaju i neku vrstu ugovora sa drugim kompanijama koje, na taj način, dobijaju profile potencijalnih kupaca, a što je u novoj ekonomiji postalo iznimno važno zbog personalizacije roba i usluga. Pritom, karakteristično je da se dio ličnih podataka, npr. korisničko ime i prezime, čak dobrovoljno „dijeli" sa aplikacijama i platformama, dok se dio ličnih podataka, npr. korisnička IP adresa i geolokacija, naprosto uzima bez direktnog pristanka i spoznaje o konačnom načinu i cilju podatkovne obrade. Osim toga, većina online aplikacija i platformi praktično i ne dozvoljava punu funkcionalnost bez tzv. registracije, koja podrazumijeva unos određenih dijelova ličnih podataka korisnika.

U ovom kontekstu, svakako treba posebno izdvojiti Google kao svojevrsni sinonim Interneta koji je već terećen za krivično raspolaganje ličnim podacima svojih korisnika zbog obrađivanja ličnih podataka korisnika u svrhu personalizacije oglasa[1]. Isto tako, i kompanija Zoom Video Communications[2] bila je pod ozbiljnom

1 Izdvojeno kao zaseban slučaj drastične sankcije zbog kršenja načela GDPR-a

2 Američka kompanija za komunikacijsku

* - Fakultet za menadžment i poslovnu ekonomiju Univerziteta u Travniku

lupom javnosti zbog krivičnog raspolaganja ličnim podacima korisnika i navodne prodaje podataka određenoj trećoj strani. U stvari, sve (američke) kompanije (Google, Facebook, Netflix, Amazon, Cloudflare, Microsoft, Oracle itd.) po važećem GDPR okviru prakično već u samom startu krše pravila kontrole i procesuiranja ličnih podataka korisnika iz EU, s obzirom da svoja poslovanja imaju registrirana u SAD-u. Pritom, situaciju ne mijenja ni činjenica da se data centri pojedinih kompanija nalaze na prostorima EU, što problematizira CLOUD Act (eng. Clarifying Lawful Overseas Use of Data) kao američki pandan evropskom GDPR-u. Naime, CLOUD Act omogućava vladi SAD-a zatražiti sve informacije koje određena kompanija obrađuje, uključujući i lične podatke korisnika EU, bez obzira nalaze li se serveri i data infrastruktura kompanije unutar ili izvan SAD-a[3].

Stoga se s pravom postavlja ozbiljno pitanje – postoji li garancija da korisnički podaci neće biti zloupotrijebljeni, i ko sve uopće može do njih doći? Praktična trgovina i neovlašteno korištenje ličnih podataka utiče čak i na političke procese u svijetu, gdje je markantna afera Cambridge Analytics-a, kada su se lični podaci korisnika Facebooka koristili za uticaj na birače u predizbornoj kampanji američkog predsjedničkog kandidata Donalda Trumpa, ali i u kampanji koja je u Velikoj Britaniji rezultirala Brexitom. Sve ove silne podatkovne eskalacije inicirale su i simboličnim uspostavljanjem tzv. Dana zaštite podataka (eng. Data Protection Day) - 28. januar, kao globalnog napora sa ciljem povećanja svijesti na individualnom nivou te poticanja kompanija u smjeru (nužnosti) poštivanja privatnosti i zaštite ličnih podataka kao dobrobiti njihovog uspješnog poslovanja. Takođe, inicirala je i najsveobuhvatnijom zakonskom regulativom u oblasti zaštite ličnih podataka, poznatom pod akronimom GDPR.

PROMJENE KOJE DONOSI GDPR-A

Opća uredba o zaštiti podataka, poznata pod akronimom GDPR (eng. GDPR – General Data Protection Regulation) upravo je i motivirana ekspanzijom ličnih podataka u javnom prostoru, sa krajnjim ciljem njihove zaštite od (komercijalne) zloupotrebe. Njen pravni temelj je Ugovor o funkcioniranju Evropske unije i Povelja Evropske unije o temeljnim pravima, koji u svom sadržaju eksplicitno navode da svako ima pravo na zaštitu svojih ličnih podataka. Kao Uredba, direktno nameće jedinstveni režim zakona sigurnosti podataka za sve članice EU uz obavezu usklađivanja nacionalnih zakona zaštiti podataka u svim zemljama članicama EU. Uredba stvara i jasnoću za organizacije uspostavljanjem jednog Zakona u cijeloj EU, pa bi trebala pojednostaviti zakonodavni okvir i olakšati usklađivanje firmama koje posluju u više država članica.

Slika 1. Logo GDPR-a

Izvor: https://gdpr-info.eu, pristup: 22.01.2021

Kako je posve neprihvatljivo da raznorazne kompanije nekontrolirano raspolažu nečijim ličnim novcem, nekretninama i slično, tako je i neprihvatljivo da kompanije imaju neometan pristup i slobodnu volju kad je riječ o ličnom imenu, matičnom broju, adresi i ostalim podacima koji obilježavaju određenu osobu[4]. Nažalost, činjenica je da

tehnologiju čija je popularnost naprosto „eksplodirala“ sa počecima pandemije koronavirusa

3 https://www.index.hr/clanak/ako-u-poslovanju-koristite-digitalne-alate-ogromna-je-sansa-da-vam-prijeti-kazna, pristup: 19.03.2022.

4 https://gdpr-info.eu, pristup: 20.01.2021

mnoge kompanije i organizacije često koriste lične podatke svojih klijenata kao besplatan resurs i koriste ih bez pitanja, prikupljaju bez ograničenja i bilo kakvih mjera zaštite. Osnovni razlog takvog ponašanja je konkurentska utrka, jer što više podataka kompanija ima na raspolaganju, utoliko ima i više informacija na osnovu kojih može predvidjeti tržište, donijeti strateške odluke i tako eventualno nadmašiti konkurenciju. Dakle, glavni "inicijator" ili motiv uspostave GDPR-a je digitalizacija i rastuće elektronsko tržište, uz svakodnevnu ogromnu razmjenu ličnih podataka. Uredbom se nastoje spriječiti moguće malverzacije, odnosno netransparentna obrada podataka, prodaja ili prosljeđivanje ličnih podataka trećim stranama bez znanja ispitanika.

Tako, prema GDPR uredbi (koja je i formalno stupila na snagu u maju 2018. godine), kompanije moraju adekvatno štititi podatke o svojim klijentima, što se posebno odnosi na kompanije koje prikupljaju velike količine podataka (tehnološke kompanije, maloprodajne firme, pružatelji zdravstvenih usluga, banke, osiguravajuća društva i sl.), zatim morati umanjiti količine podataka koje koriste te tačno odrediti koji im podaci doista i trebaju. U tom smislu, GDPR propisuje sljedeća načela koja se tiču prikupljanja i obrade ličnih podataka:[5]

- zakonitost, poštenost i transparentnost obrade,
- ograničavanje svrhe,
- smanjenje količine podataka,
- tačnost,
- ograničenje pohrane,
- cjelovitost i povjerljivost te
- pouzdanost.

Generalno, cilj GDPR-a je pružanje zajedničkih standarda za zaštitu podataka koji može biti primjenjiv na svjetskom nivou, rješavanje spornih pojmova, poput definiranje ličnih podataka, kreiranje novih prava kao što je pravo na zaborav, prenosivost ličnih podataka i provođenje sankcija, pravnih i novčanih, za kršenje ovih prava. Ovdje je posebno zanimljivo tumačiti (proširen) pojam lični podatak, jer se pod ličnim podacima mahom smatra(o) prilično uzak obim atributa. Naime, prema definiciji iz GDPR Uredbe, lični podaci su "...svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi; pojedinac čiji se identitet može utvrditi jeste lice koje se može identifikovati direktno ili indirektno, naročito uz pomoć identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca"[6]. Dakle, iznenađujuće je širok pojam što su sve lični podaci: ime i prezime, identifikacioni broj, adresa, slika, broj telefona ali i IP adresa, historija bolesti, popis najdraže literature i sl., tj. svi podaci koji mogu dovesti do direktnog ili indirektnog identificiranja pojedinca.

Doista, GDPR uredba donijela je cijeli niz novina u podatkovnom prosturu. To se posebno odnosi u pristupu obrade (ličnih) podataka, gdje je fokus na tzv. pseudonimizaciji koja podrazumijeva takvu obradu da se (obrađeni) lični podaci više ne mogu pripisati određenom ispitaniku bez upotrebe dodatnih informacija. Uz psedonimizaciju, tu je svakako i enkripcija, koja podatke čini šifiranim (nečitljivim) za sva neovlaštena lica bez pristupa odgovarajućeg ključu za dekripciju. Uz to, GDPR propisuje da se dodatni podaci, među njima i ključ za dekripciju, drže udaljeno od pseudonimiziranih podataka. Također, jedan od pristupa je i tzv. tokenizacija, kao savremeni nematematički pristup obradi. Tokeni nemaju važnost niti vrijednost kao podaci, ali se njima ne mijenja vrsta ili dužina podataka, zbog čega ih mogu obrađivati sistemi baze podataka koje su temeljene na podatkovnoj konzistentnosti.

Navest ćemo i nekoliko dodatnih primjera gdje je GDPR Uredba donijela značajne promjene. U prvom redu, radi se o tzv. kolačićima (eng. cookie), obrascima (eng.

5 http://azlp.ba/GDPR_Menu/Sta_je_GDPR, pristup: 21.01.2021

6 Ibid

forms) i biltenima (eng. newsletter), kao neizostavnim dijelovima savremenih web stranica.

- Kolačić (eng. cookie) je informacija spremljena na računar korisnika od strane web stranice koju posjeti. Kolačići obično spremaju postavke za web stranicu, kao što su preferirani jezik ili adresa. Kasnije, kada korisnik otvori istu web stranicu kolačići omogućavaju stranici da prikaže informacije prilagođene klijentovim potrebama. GDPR donosi bitnu promjenu kod kolačića, tako da više nije dozvoljen natpis "Ova stranica koristi kolačiće" odnosno za svaki kolačić koji se želi spremiti u internetski preglednik posjetitelja mora se dobiti korisnička dozvola. Pritom, obaveza se ne odnosi samo na kolačiće koji su neophodni za rad web stranice, već i za sve ostale vrste kolačića.

- Obrasci (eng. forms) služe za prikupljanje različitih podataka od strane korisnika na web stranicama. Prema GDPR-u, svaki podatak koji korisnik na taj način ostavi, može se koristiti samo u svrhu za koju je korisnik dao pristanak, odnosno dozvolu. Naprimjer, e-mail adresa koja je na ovaj način primljena od kupca putem web shopa, može se koristiti isključivo za realizaciju te narudžbe, ali ne i za slanje promotivnih ponuda. Ako se i to želi, ispod kontakt obrasca mora biti odgovarajući box (koji nije unaprijed, po default-u označen!), i pored koje treba stajati: "Slažem se da mi šaljete promotivne ponude".

- Bilteni (eng. newsletters) su, prije ozvaničenja GDPR-a, funkcionirali na doista različite načine. Tako, većina obrazaca na web stranicama kojima su se sakupljale e-mail adrese za biltene, kreirani su tako da imaju tekst koji traži da se ostavi e-mail adresa kako bi se preuzela besplatna elektronska knjiga ili ostvario popust na kupovinu; ta se adresa potom koristila za redovno slanje biltena. GDPR prekida ovu praksu te ako se korisniku bilten želi slati redovno, korisnik mora dati svoje jasno dopuštenje.

POZICIJA BOSNE I HERCEGOVINE

Naravno, u svemu ovome, posebno nam je bitna pozicima Bosne i Hercegovine, kao zemlje izvan Evropske unije? No, situacija je u ovom smislu potpuno jasna, i ova najsveobuhvatnija promjena u politici zaštite podataka u zadnjih nekoliko decenija, (ipak) se odnosi i na Bosnu i Hercegovinu.

Praktično, već i potpisivanjem Sporazuma o stabilizaciji i pridruživanju EU, Bosna i Hercegovina je preuzela obavezu usklađivanja domaćeg zakonodavstva sa pravnom osnovom Evropske unije. Osim toga, u skladu sa odredbama GDPR-a, Uredba se primjenjuje i na obradu ličnih podataka ukoliko kontrolor podataka sa sjedištem u EU ima poslovne ogranke u BiH ili na bilo koji način pruža usluge građanima u BiH. Također, subjekti iz BiH koja posluju na prostoru EU ili nude robe ili usluge građanima EU, dužni su primjenjivati GDPR[7]. Što se tiče kaznenih odredbi, primjenjivat će se odredbe iz (postojećeg, i inače nedostatnog) Zakona o zaštiti ličnih podataka u našoj zemlji, sve do stupanja na snagu novog zakona koji treba biti usklađen s GDPR Uredbom[8]. Konkretno, što se tiče naših poslovnih sistema i organizacija, u prvom redu dužni su da urade tzv. procjenu usklađenosti zaštite ličnih podataka sa važećim Zakonom o zaštiti ličnih podataka u BiH i GDPR Uredbom.

U ovom radu, izdvojit ćemo JP Autoceste Federacije FBiH, kao pozitivan primjer prilagođavanja novoj regulativi prikupljanja, obrade i zaštite ličnih podataka. Naime, u ovoj kompaniji uspostavili su odgovarajuću Politiku obrade i zaštite ličnih/osobnih podataka kao temeljni akt, uz imenovanje i tzv. DPO službenika[9] kao uposlenika zaduženog za zaštitu podataka kako bi se osiguralo djelovanje u skladu sa GDPR Uredbom. U Politici obrade i zaštite ličnih/

7 https://www.media.ba/bs/magazin-mreze-i-web, pristup: 13.03.2022

8 https://ed-vision.com/koje-promjene-donosi-gdpr-i-kako-ga-primjeniti-u-bih, pristup: 22.01.2021

9 DPO - Data protection Officer

osobnih podataka navode, pored ostalog, i sljedeće:[10]

"...Cilj Politike je uspostaviti odgovarajuće procese zaštite i upravljanja ličnim/osobnim podacima ispitanika, odnosno korisnika usluga, radnika i drugih osoba čiji se lični/osobni podaci obrađuju, u skladu sa GDPR uredbom (EU) 2016/679 Evropskog parlamenta i Vijeća od 27.04.2016. godine, Zakonom o zaštiti ličnih/osobnih podataka BiH o zaštiti pojedinaca u vezi s obradom ličnih/osobnih podataka i o slobodnom kretanju takvih podataka i internim aktima preduzeća. JP Autoceste FBiH su prepoznale važnost zaštite privatnosti, sigurnosti i zaštite podataka svih pojedinaca koji se pojavljuju kao učesnici u svim našim poslovnim procesima. JP Autoceste FBiH putem ove Politike izražava spremnost na poštivanje uredbe, zakona, internih akata preduzeća o zaštiti ličnih/osobnih podataka".

Drastični slučajevi GDPR sankcija

Kako današnja konkurencija "prisiljava" organizacije na maksimalnom približavanju kupcima i klijentima kroz personalizaciju roba i usluga, česta je pojava zloupotrebe prikupljenih podataka, posebno sa sveprisutnih platformi društvenih mreža (Facebook, Instagram itd.). No, sankcije zbog kršenja GDPR-a danas su jedna nova realnost, pri čemu se u praksi razlikuju dva nivoa novčanih kazni:[11]

– niži nivo novčane kazne (do 10 miliona eura ili 2% godišnjeg prometa), koji je rezerviran za prekršaje vezane uz osnovna načela Uredbe, pravne osnove obrade, uvjete dozvole, informiranje ispitanika, obradu posebnih kategorija osobnih podataka, odbijanje prava ispitanika te prijenos podataka u treće zemlje, odnosno van EU;
– viši nivo novčane kazne (do 20 miliona eura ili 4% godišnjeg prometa), koji je fokusiran na prekršaje povezane sa vođenjem evidencije aktivnosti obrade, sigurnošću ličnih podataka, provođenjem procjene učinka na zaštitu podataka, tehničkom i integriranom zaštitom podataka, ugovorima o obradi podataka, kao i imenovanjima službenika za zaštitu podataka.

U nastavku rada predstavit će se nekoliko drastičnih slučajeva izrečenih novčanih kazni kompanijama za nepoštivanje GDPR uredbe, u periodu 2019. – 2021. godina[12], uz kratak osvrt na način kako se pojedina sankcija mogla prevenirati.

- Slučaj „Amazon". Prvi i najdrastitičniji slučaj GDPR sankcija – iznos od 746 miliona €, juli 2021. godine, odnosi se kompaniju Amazon. Razlozi ovako visoke kazne nisu u javnosti potpunosti objašnjeni, ali je glavna pretpostavka da se radi o pristancima kompanije na tzv. kolačiće (eng. cookies). Zanimljivo je da ovo nije i prvi put da je kompanija Amazon kažnjena zbog načina na koji prikuplja i dijeli lične podatke putem kolačića. Naime, krajem 2020. godine Francuska je kaznila Amazon sa 35 miliona eura zbog gotovo identičnog razloga. Kako se ovako visoka kazna mogla izbjeći? Doista, kompanijama je primamljivo natjerati korisnike da "pristanu" na kolačiće (ili otežati isključivanje kolačića) kako bi prikupili što više ličnih podataka. No, da je Amazon dobijao "slobodnu volju", informiranu i nedvosmislenu saglasnost za uključivanje prije postavljanja kolačića na uređaje svojih korisnika, izbjegli bi kaznu GDPR-a.
- Slučaj „WhatsApp". Drugi drastični slučaj GDPR sankcija – 225 miliona €, septembar 2021. godina, odnosi se kompaniju WhatsApp. Naime, Irska koja je osudila WhatsApp ovom visokom kaznom ustanovila je da usluga WhatsApp-a za razmjenu poruka nije pravilno objasnila svoje postupke obrade podataka u svojoj obavijesti o privatnosti. Kako se kazna mogla izbjeći? Irski DPA rekao je da je krivica

10 https://jpautoceste.ba/zastita-podataka, pristup: 15.03.2022.

11 http://azlp.ba/GDPR_Menu/Sta_je_GDPR, pristup: 21.01.2021

12 https://www.tessian.com/biggest-gdpr-fines, pristup: 11.01.2022.

WhatsApp-a gotovo neprozirna obavijest o privatnosti te da je kompanija trebala dati informacije o privatnosti u lako dostupnom formatu, koristeći jezik koji njezini korisnici razumiju.

- Slučaj „Google“. Treći drastični slučaj GDPR sankcija – 50 miliona €, januar 2019, odnosi se kompaniju Google. Naime, ovom najpoznatijem svjetskom IT divu Francuska je izrekla kaznu za kršenje GDPR Uredbe, zbog toga što Google nije imao valjanu pravnu osnovu za različite obrade ličnih podataka korisnika svojih usluga, pogotovo u svrhu personalizacije oglasa. Nakon istrage zaključeno je da Google krši načelo transparentnosti te obavezu informiranja, jer nije lako pristupiti informacijama o obradi podataka koje kompanija pruža korisnicima s obzirom da su informacije razbacane kroz nekoliko različitih dokumenata, a važne informacije za određene obrade dostupne su tek nakon preduzimanja pet do šest radnji na uređaju. Osim toga, ustanovljeno je da informacije Google-a nerijetko nisu ni dovoljno jasne ili razumljive, dok u nekim slučajevima informacije o trajanju zadržavanja podataka naprosto i ne postoje. Kako se kazna mogla izbjeći? Kompanija Google trebala je pružiti više informacija korisnicima u pravilima o pristanku i dati im veću kontrolu nad načinom na koji se obrađuju njihovi lični podaci.

- Slučaj „H&M“. Četvrti slučaj GDPR sankcije – 35 miliona €, oktobar 2020. godina, odnosi se na kompaniju Hennes & Mauritz, poznatiji kao H&M. Naime, Njemačka je ovom švedskom lancu odjeće izrekla kazna za kršenja GDPR-a koja se tiču prekomjernog “nadzora” nekoliko stotina zaposlenika. Nakon što su zaposlenici uzimali godišnji odmor ili bolovanje, morali su dolaziti na sastanak za povratak na posao, pri čemu su neki od tih sastanaka snimljeni i bili dostupni za više desetina H&M menadžera. Tako je više osoblje kompanije steklo “široko znanje o privatnim životima svojih zaposlenika”, od prilično bezazlenih detalja do porodičnih problema i vjerskih uvjerenja.” Također, ovi “detaljni profili” korišteni su pri ocjenjivanju učinka zaposlenika i donošenju odluka o njihovom angažmanu. Kako se novčana kazna mogla izbjeći? H&M je prekršio GDPR-ovo načelo minimiziranja podataka, odnosno nije dozvoljeno obrađivati lične podatke, posebno osjetljive podatke o zdravlju i uvjerenjima ljudi, osim ako to nije nužno za posebnu svrhu. H&M je trebao postaviti strogu kontrolu pristupa podacima, i kompanija pogotovo nije smjela koristiti te podatke za donošenje odluka o zapošljavanju ljudi. Markantno je kako se kompanija izvinula svojim zaposlenicima i pristala povrijeđenim zaposlenicima isplatiti novčanu naknadu.

- Slučaj „TIM“. Peti slučaj GDPR sankcija – 28 miliona €, januar 2020, odnosi se na italijanski telekomunikacijski operater TIM, poznatiji kao Telecom Italia. Naime, Garantea kao odgovarajuće tijelo za zaštitu podataka, izrekla je TIM-u visoku kaznu zbog niza GDPR prekršaja i nezakonitih radnji, od kojih većina proizlazi iz pretjerano agresivne marketinške strategije. Tako su milioni pojedinaca bombardirani su promotivnim pozivima i neželjenom komunikacijom, od kojih su neki bili na popisima bez kontakta i mogućnosti isključenja. Istraga je otkrila i da TIM ne upravlja call centrima za marketinšku komunikaciju na primjeren način, ne osvježava listu pojedinaca koji su izrazili želju za isključivanjem iz marketinške komunikacije, zatim traži pristanak za marketinšku komunikaciju kao uslov da bi kupci dobili popuste, nudi netačne i netransparentne informacije o obradi podataka i sl. Kao dodatan primjer učestalosti nezakonitog ponašanja, ističe se situacija gdje je ista osoba bez prethodnog pristanka pozvana 155 puta u mjesec dana! Uz sve navedeno, kompanijin sistem za upravljanje povredama ličnih podataka pokazao se neefikasnim, a nije postojala ni adekvatna implementacija sistema upravljanja ličnim podacima, zbog čega je kompanija kršila i načela tehničke zaštite podataka te integrirane zaštite podataka (eng. privacy by design and default). Kako se kazna mogla izbjeći? TIM je morao pažljivije upravljati

popisima ličnih podataka korisnika (i potencijalnih korisnika) te kreirati posebne opcije za različite marketinške aktivnosti.

ZAKLJUČAK

GDPR, odnosno Opća uredba o zaštiti podataka motivirana je ekspanzijom ličnih podataka u javnom prostoru, sa krajnjim ciljem njihove zaštite, posebno od (komercijalne) zloupotrebe od strane (velikih) kompanija. Uredba je, precizno, nedvosmisleno, direktno nametnula jedinstveni režim zakona sigurnosti podataka, kako za sve članice EU, tako i zemlje koje na određeni način učestvuju u zajedničkom podatkovnom prostoru. Tako, prema GDPR-u, organizacije koje prikupljaju i upravljaju ličnim podacima korisnika dužne su zaštititi prikupljene podatke od zloupotrebe, što se u suprotnom sankcionira iznimno visokim novčanim kaznama.

Što se tiče naše zemlje, iako nije članica Evropske unije, postoje jasne obaveze u smislu GDPR-a kao najsveobuhvatnije promjene u politici zaštite podataka. U prvom redu, već samim potpisivanjem Sporazuma o stabilizaciji i pridruživanju EU, Bosna i Hercegovina je preuzela obavezu usklađivanja domaćeg zakonodavstva sa pravnom osnovom Evropske unije. Pored toga, odredbe GDPR-a primjenjuje se i na sve subjekte (naravno, ne samo iz BiH) koji posluju (ili nude robu i/ili usluge) na prostoru Evropske unije, što sve primorava (i) naše organizacije i poslovne sisteme na potrebne prilagodbe u pogledu politike prikupljanja, obrade i zaštite ličnih podataka. U tom kontekstu, izdvojili smo JP Autoceste Federacije BiH kao jedan (pozitivan) primjer prilagođavanja novoj podaktovnoj regulativi, gdje je uspostavljena odgovarajuća Politika obrade i zaštite ličnih/osobnih podataka kao temeljni akt koji opisuje svrhu i ciljeve prikupljanja, obrade i upravljanja ličnim/osobnim podacima shodno načelima GDPR-a.

LITERATURA

[1] http://azlp.ba/GDPR_Menu/Sta_je_GDPR, pristup: 21.01.2021
[2] https://www.tessian.com/biggest-gdpr-fines, pristup: 11.01.2022.
[3] https://www.media.ba/bs/magazin-mreze-i-web, pristup: 13.03.2022
[4] https://gdpr-info.eu, pristup: 22.01.2021
[5] https://www.index.hr/clanak/ako-u-poslovanju-koristite-digitalne-alate-ogromna-je-sansa-da-vam-prijeti-kazna, pristup: 19.03.2022.
[6] https://jpautoceste.ba/zastita-podataka, pristup: 15.03.2022.
[7] https://ed-vision.com/koje-promjene-donosi-gdpr-i-kako-ga-primjeniti-u-bih, pristup: 22.01.2021