UDK: 342.738(4-672EU)
Biblid: 1451-3188, 19 (2020)
God XIX, br. 73-74, str. 99–117
DOI: https://doi.org/10.18485/iipe_ez.2020.19.73_74.7

Pregledni naučni rad
Primljen 06.09.2020.
Odobren 05.10.2020.

OPŠTA UREDBA EVROPSKOG PARLAMENTA I SAVETA EVROPSKE UNIJE O ZAŠTITI PODATAKA (GDPR) – PREGLED I NOVINE

*Marija MAJSTOROVIĆ**

Apstrakt: Svakodnevno korišćenje interneta, što za poslovne potrebe, što u privatne svrhe (od čuvanja podataka na *cloud* sistemima, korišćenja aplikacija i mnogih drugih sadržaja koji pristupaju raznim biometrijskim i ličnim podacima), savremenog čoveka stavilo je u središte tehnološkog razvoja, digitalizacije i povezanosti putem različitih mreža. Značaj koji su nekada imale robna razmena, zlato, a zatim i promet roba i usluga na razvoj ekonomije i tehnološki napredak, danas imaju podaci. U digitalno doba kada su podaci pokretač i osnova za razvoj svake kompanije i osnovni derivat svakog društva, a građani, često i bez mnogo razmišljanja, svoje podatke olako ostavljaju na raspolaganje mnogim kompanijama koje prikupljaju podatke i na osnovu njihove obrade donose poslovne odluke, došlo je do potrebe za regulisanjem oblasti zaštite podataka. Sa povećanjem broja podataka o svima nama dolazi do potrebe za zaštitom privatnosti i povećanjem kontrole, te je iz te težnje i potrebe za poboljšanjem zakonskog okvira sa tekovinom modernog doba, doneta Opšta uredba o zaštiti podataka o ličnosti (GDPR) 2016. godine, a koja detaljno reguliše prava lica i obaveze kompanija. Cilj rada je predstavljanje bitnih karakteristika i novina u pogledu novih instituta i pojmova, kao i sagledavanje pozitivnih efekata koje je Uredba unela u oblast prava Evropske unije ali i na prava svih lica koja su predmet obrade, a sve na osnovu analize relevantnog zakonodavnog okvira Evropske unije i dokumenata koje su donela evropska regulatorna tela i relevantne institucije – od Evropskog parlamenta, Saveta Evropske unije, Evropskog odbora za zaštitu podataka, Evropske komisije itd.

Ključne reči: Opšta regulativa o zaštiti podataka, GDPR, pravo zaštite podataka, pravo Evropske unije.

* Direktor, GDPR Institut d.o.o., Beograd; doktorand, Fakultet za poslovne studije i pravo, Univerzitet „Union – Nikola Tesla", Beograd. E-mail: majstorovic.m@live.com.

1) UVOD

Potreba za uređenjem oblasti zaštite podataka potiče iz sedamdesetih godina prošlog veka kada su neke od evropskih zemalja, poput Švedske, Francuske, Nemačke, Austrije i dr. donele prve propise u sferi prava zaštite podataka o ličnosti.[1] Sa razvojem 4.0 industrije, inkorporiranju interneta i informacionih tehnologija u svakodnevni život građana i funkcionisanje kompanija, proizveo se i u opticaju je nemerljivo veliki broj podataka.[2] Kompanije, države i drugi privredni entiteti prikupljaju lične podatke, najrazličitijeg opsega i vrste, i na osnovu obrade predmetnih podataka donose odgovarajuće odluke. Prema analizi Evropske komisije u Izveštaju posvećenom tržištu podataka, procenjena vrednost ekonomije podataka u Evropi premašila je 2019. godine četiri stotine milijardi evra.[3]

Vrednost ekonomije podataka potvrđuje i činjenica da je nastavljen pozitivan trend rasta vrednosti u odnosu na prethodne godine, ali da se tek očekuje ekspanzija značaja podataka na razvoj savremene ekonomije po izlasku iz svetske ekonomske krize izazvane Covid-19 (korona) virusom.[4] Slobodno se može reći da na podacima počiva savremena ekonomija. Diskutabilni aspekt u vezi prikupljanja ličnih podataka je zapravo gde i kada je prekoračena tanka nit u smislu kada se podaci prikupljaju u naznačene svrhe, a kada su narušena prava privatnosti, porodičnog života, ličnih opredeljenja i preferencija, a koja su zagarantovana Poveljom o ljudskim pravima.[5] U navedenim slučajevima može doći do sukoba interesa lica čiji se podaci prikupljaju u težnji da sačuvaju svoju privatnost i opredele koje svoje podatke žele da „podele" sa rukovaocima i obrađivačima, odnosno onima

---

[1] Za više o zakonima koje su donele članice EU kao pioniri u oblasti zaštite podataka i pravnoj prirodi nezavisnih kontrolnih tela, videti: Stefan Andonović, doktorska disertacija, *Zaštita podataka u elektronskoj javnoj upravi u Republici Srbiji – pravni aspekti,* Univerzitet u Beogradu, Pravni fakultet, Beograd 2019, str. 254-265.

[2] Za više o 4.0 industriji, videti: Predrag Dašić, Raul Turmanidze, *„Industrija 4.0: stvarnost ili priviđanje (Pozivni referat)"*, XVI Međunarodna konferencija „Ekonomsko/pravno/komunikacijski aspekti zemalja Zapadnog Balkana sa posebnim osvrtom na Bosnu i Hercegovinu u procesu pristupa Evropskoj uniji", Ekonomski fakultet, Rijeka 2017, str. 80-89; Isak Karabegović, Edina Karabegović, „Implementacija „Industrije 4.0" primjenom robota i digitalne tehnologije u proizvodnim procesima u Kini", *Tehnika – Mašinstvo 67 (2018),* Tehnički fakultet, Bosna i Hercegovina, Bihać, 2018, str. 225-231.

[3] Evropska komisija, Ažurirana studija evropskog tržišta podataka, 6.7.2020, https://ec.europa.eu/digital-single-market/en/news/european-data-market-study-update, pristupljeno 17.9.2020.

[4] Ibid.

[5] Za više o Povelji o ljudskim pravima, videti: Klaus-Diter Borhart (Klaus-Dieter Borchardt), *Abeceda prava Evropske unije*, Kancelarija za publikacije Evropske unije, Luksemburg 2010, dostupno na: http://euinfo.rs/files/Publikacije-srp/10_Abeceda_prava_EU.pdf, pristupljeno 24.9.2020. god.

koji stupaju u posed predmetnih podataka, dok, s druge strane, postoji interes kompanija da svoje poslovanje baziraju baš na osnovu prikupljenih podataka kako bi ostvarile svoj osnovni cilj poslovanja – maksimizaciju profita.[6]

Mnoge institucije prepoznale su značaj prava zaštite podataka o ličnosti i donele razne propise, a neki od njih su: Konvencija Saveta Evrope o zaštiti pojedinaca od automatizovane obrade podataka, Povelja Evropske unije o osnovnim pravima, odnosno Evropska konvencija o ljudskim pravima, Direktive o privatnosti i elektronskim komunikacijama i dr., pa sve do Direktive o zaštiti građana u vezi sa obradom podataka o ličnosti i slobodnom kretanju takvih podataka iz 1995. godine[7] i Opšte uredbe o zaštiti podataka o ličnosti iz 2016. godine. Predmet ovog rada je isključivo Opšta uredba o zaštiti podataka ili skraćeno GDPR[8] (u daljem tekstu: Uredba), te prikaz osnovnih karakteristika i novina koje predmetna regulativa unosi u pravo Evropske unije, a pre svega u oblast prava zaštite podataka i privatnosti. U radu će biti prikazani novi instituti, pojmovi i činioci, kao i načela na kojima počiva Uredba, a sve sa krajnjim ciljem – obezbeđenjem prava licima čiji se podaci prikupljaju kako bi njihova privatnost i osnovna ljudska prava bila zaštićena.

2) OPŠTA UREDBA O ZAŠTITI PODATAKA O LIČNOSTI

Uredba Evropske unije 2016/679 o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i o slobodnom kretanju takvih podataka stavlja van snage Direktivu 95/46/EZ od 27.04.2016.[9] Iako je Uredba doneta 2016. godine, primena je odložena do 25.05.2018. godine usled nespremnosti kompanija ali i celokupnih zakonskih sistema kojima je bilo neophodno vreme da bi odgovorili na zahteve koje je postavila Opšta uredba o zaštiti podataka u pogledu obezbeđenja zaštite prava podataka o ličnosti licima čiji se podaci prikupljaju, kao i u vezi korišćenja, prenosa i slobodnog protoka predmetnih podataka. Smatralo se da se područje primene

[6] Sanja Prlja, „Pravo na zaštitu ličnih podataka u EU", *Strani pravni život* 2018/1, Beograd 2018, str. 89, UDK: 342.721 (4-672 EU).

[7] Za više o Direktivi, videti: Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, *Direktiva 95/46/EZ od 24.10.1995. o zaštiti građana u vezi sa obradom podataka o ličnosti*, b.d., https://www.poverenik.rs/sr-yu/међународни-документи6/699-direktiva-9546ez-od-24101995o-zatiti-graana-u-vezi-sa-obradom-podataka-o-linosti.html, pristupljeno 7.9.2020.

[8] U daljem tekstu će se koristiti skraćenica GDPR koja potiče od engl. *General Data Protection Regulation*, u prevodu na srpski jezik – Opšta regulativa o zaštiti podataka.

[9] Za više o tekstu Uredbe postoji dostupan prevod, videti: Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, *UREDBA 2016/679 (GDPR) – NEZVANIČAN PREVOD*, b.d., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, pristupljeno 7.9.2020.

Uredbe odnosi samo na Evropsku uniju, a kako je predmetna Uredba doneta od strane Evropskog parlamenta i Saveta Evropske unije, ipak to nije tačno. Primenu Opšte uredbe možemo posmatrati kroz aspekt teritorijalnog važenja Uredbe. Prvi slučaj kada se Uredba primenjuje na obradu podataka je kada rukovalac ili obrađivač imaju sedište u Evropskoj uniji, bez obzira na to da li vrše obradu podataka evropskih građana ili ne. Drugi slučaj kada se primenjuje Uredba je kada je sedište obrađivača ili rukovaoca van Evropske unije, ali se vrši obrada ličnih podataka građana sa teritorije Evropske unije. Bitan karakter Opšte uredbe o zaštiti podataka je i eksteritorijalno važenje, što znači da se Uredba primenjuje i u državama koje su van Evropske unije, ili gde se pravo članice primenjuje na osnovu međunarodnog javnog prava, ako obrađuju podatke građana Evropske unije ili vrše transfer podataka na teritoriju Evropske unije.

Za primenu Regulative ostavljena je i opcija implementacije predmetnog propisa u domaća zakonodavstva, kroz donošenje zakona o zaštiti podataka i drugih propisa u zakonodavni sistem država, kako bi implementirale predmetnu Uredbu ali i harmonizovale svoj dosadašnji pravni okvir sa sistemom zaštite podataka u Evropskoj uniji. Ovo je tipično za zemlje članice Evropske unije, kao i za one koje su na putu integracije evropskih vrednosti i primanja u članstvo Evropske unije. Takav primer je i Republika Srbija, koja je donela Zakon o zaštiti podataka o ličnosti.[10] Države članice postigle su dogovor da se osnuju nacionalna tela čija nadležnost bi bila ustanovljena u skladu sa članom 8, stav 3 Povelje Evropske unije o osnovnim pravima. Organ koji sprovodi sankcionisanje nad povredama prava zaštite podataka i vrši nadzor nad primenom Regulative je samostalan, nezavisni organ, kojeg odlikuje profesionalizam i iskustvo u pravnom delokrugu, koji se konstituiše na nivou države članice Evropske unije (ili države koja je van teritorija EU ali je sprovela Regulativu u domaće zakonodavstvo, ili podleže primeni međunarodnog javnog prava u ovom kontekstu). Kazne koje nezavisni nadzorni organ može da izrekne su izuzetno visoke i iznose čak do 20.000.000 evra ili 4% ukupnog godišnjeg prihoda u zavisnosti koji je iznos veći. Najčešći osnovi za izricanje sankcija su povrede načela obrade podataka, o kojima će više biti reči u daljem toku rada, kao i neadekvatni pravni osnovi za pristanak lica na obradu podataka, a u skladu sa članovima 5–9 Uredbe, ili u slučaju povrede nosioca prava ličnih podataka na osnovu članova 12–22 Uredbe.[11]

[10] Za više o tekstu Zakona o zaštiti podataka koji je donela Republika Srbija, videti: Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Zakon o zaštiti podataka o ličnosti „Sl. glasnik RS" br. 87/2018. od 13.11.2018, https://www.poverenik.rs/images/stories/dokumentacija-nova/zakoni/ZZPLnovembar2018/ZZPL, novembar 2018, pristupljeno 1.10.2020.

[11] Ivan Milošević, *GDPR Uputstvo za primenu*, Janković Popović Mitić advokatska kancelarija, str. 34, Beograd 2018. Dostupno na: https://www.jpm.rs/wp-content/uploads/2018/04/gdpr.pdf, pristupljeno 1.10.2020.

2.1. PREGLED SADRŽINE OPŠTE UREDBE O ZAŠTITI PODATAKA

Evropska uredba o zaštiti podataka o ličnosti koncipirana je u 11 poglavlja sa čak 99 članova, a koja ćemo poglavlja ukratko navesti kako bi se stekao uvid u obim predmetne regulative, ali i široki opseg delovanja na pravo zaštite podataka i privatnost građana. Samoj sadržini Regulative prethodi preambula koju čini preko 170 tačaka. Preambula predstavlja uvod u primenu materijalnih odredbi, te navodi razloge, načela, ideje i ciljeve Opšte uredbe o zaštiti podataka.[12] Preambula ukazuje i na značaj Povelje Evropske unije o osnovnim pravima i Ugovora o funkcionisanju Evropske unije, kao i na značaj institucija poput Suda pravde Evropske unije i Evropskog suda za ljudska prava, a proklamuju se i prava svakog lica na zaštitu podataka o ličnosti, kao i na druga ljudska prava i slobode, deklariše se težnja ka širenju slobode, sigurnosti i pravde na teritoriji Evropske unije, sigurnosti i bezbednosti razmene podataka, zaštiti privatnosti svakog lica.[13] Usled značajnih i sve bržih promena u oblasti interneta, digitalizacije i sajber prostora, kao i potrebe za zaštitom podataka, privatnosti i ljudskih prava korisnika interneta nastala je Opšta uredba o zaštiti podataka. U preambuli se detaljnije navode razlozi i težnje nastanka ove Regulative.

Tabela 1: Pregled Opšte uredbe o zaštiti podataka o ličnosti

Broj i naziv poglavlja	**Sadržina poglavlja**
Poglavlje I Opšte uredbe	U prvom poglavlju opisane su uvodne odredbe, predmet i ciljevi Uredbe, područje primene i definicije pojmova.
Poglavlje II Načela	Predmet druge glave su načela, uslovi za pristanak lica na obradu podataka i obrada podataka posebnih kategorija...
Poglavlje III Prava lica	Poglavlje tri posvećeno je pravima lica na koje se podaci odnose, informacijama i pristupu podacima, te ograničenjima u vezi sa obradom podataka i pravima lica…

[12] Za više o GDPR regulative, videti: Eur-Lex, *Protection of personal data (from 2018)*, b.d., https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_2&from=EN, pristupljeno 15.7.2020.

[13] Andrej Diligenski, Dragan Prlja, Dražen Cerović, *Pravo zaštite podataka – GDPR*, Institut za uporedno pravo, Beograd, 2018, str. 120-122.

Broj i naziv poglavlja	**Sadržina poglavlja**
Poglavlje IV Obrađivač i rukovalac	U četvrtom poglavlju definiše se odnos, funkcija i obaveze rukovaoca i obrađivača podataka, navode se obaveze u vezi evidencija aktivnosti obrade. Pažnja je posvećena i bezbednosti podataka i saradnji sa nadzornim organom, načinu obaveštenja lica i nadzornog organa u slučaju povrede podataka. Takođe, pažnja je posvećena i imenovanju ovlašćenog lica za zaštitu podataka, njegovom položaju i funkciji, kodeksima ponašanja i sertifikaciji i obaveznoj izradi procene uticaja u vezi sa zaštitom podataka.
Poglavlje V Transfer ličnih podataka	Glava pet je posvećena pravilima i merama zaštite, transferu i prenosu podataka u treće zemlje i međunarodne organizacije, a pominje se i značaj međunarodne saradnje radi efikasne zaštite podataka.
Poglavlje VI Nezavisna nadzorna tela	Uloga, funkcija, ovlašćenja i pravila funkcionisanja nezavisnog nadzornog tela navedena su u glavi VI.
Poglavlje VII Saradnja i konzistentnost	Glava sedam se oslanja na prethodno poglavlje i značaj daje saradnji nadzornih organa, uzajamnom rešavanju problema i sporova, razmeni iskustava. Takođe, uvodi se i institucija Evropskog odbora za zaštitu podataka, te objašnjava značaj, zadaci i procedure.
Poglavlje VIII Pravna sredstva, odgovornost i sankcije	Glava osam je posvećena pravnim lekovima, odgovornosti i sankcijama, to je pre svega pravo na delotvorno pravno sredstvo protiv nadležnog organa, rukovaoca ili obrađivača. Objašnjava se i zastupanje lica na koje se podaci odnose, postupak, uslovi za izricanje kazne, sankcije i naknada štete.
Poglavlje IX Odredbe koje se odnose na određene situacije obrade	U ovom poglavlju navode se posebne situacije obrade podataka, a neke od njih su: obrada i sloboda izražavanja i informisanja, obrada i pristup javnosti službenim dokumentima, obrada u svrhu naučnog istraživanja ili u statističke svrhe, obrada u vezi radnog prava i dr.

Broj i naziv poglavlja	Sadržina poglavlja
Poglavlje X Delegiranje i primena akata	Glava deset je posvećena delegiranju i primeni akata. Komisija delegirani akt istovremeno dostavlja Evropskom parlamentu i Savetu.
Poglavlje XI Završne odredbe	U završnim odredbama navodi se da je Direktiva 95/46/EZ stavljena van snage, te se bliže objašnjava odnos između Uredbe i Direktive kao i drugih sporazuma i akata Evropske unije o zaštiti podataka i naglašava se stupanje na snagu i primena Opšte uredbe o zaštiti podataka.

Izvor: Full text of EU GDPR, https://advisera.com/eugdpracademy/gdpr/, pristupljeno 22.09.2020.

2.2. POJMOVI

Potrebno je definisati pojam „podatak o ličnosti" kao polazište Opšte uredbe. Podaci o ličnosti su svi oni podaci koji se odnose na fizičko lice, te čine deo njegove ličnosti na osnovu kojih se to lice može identifikovati direktno ili indirektno. To mogu biti ime, prezime, jedinstveni matični broj, identifikacioni brojevi, podaci o lokaciji, IP adrese, e-mail adrese, podaci iz matičnih knjiga rođenih, lične karte, putne vize, vozačkih dokumenta, podaci iz zdravstvenih kartona, podaci koji upućuju na pripadnost verskim, političkim, socio-kulturološkim organizacijama i drugo.[14]

Kada smo definisali pojam podatka o ličnosti, potrebno je definisati ko je nosilac – vlasnik tih podataka. Nosilac ličnih podataka je fizičko lice na koje se lični podaci odnose. U literaturi se često naziva i subjekt prava zaštite podataka. Podaci o ličnosti se odnose samo na ljudska bića, dakle nosioci ličnih podataka ne mogu biti pravna lica ili životinje.[15]

Lice za zaštitu podataka o ličnosti ili službenik za zaštitu podataka je lice koje se imenuje ispred kompanije, a koje može biti zaposleno unutar nje ili eksterno angažovano. Osnovni zadaci lica za zaštitu podataka su: pomoć pri izradi opšteg akta o zaštiti podataka unutar kompanije, kontrolna i savetodavna funkcija, nadzor u domenu upravljanja ličnim podacima, promovisanje zaštite podataka o ličnosti i podizanje svesti zaposlenih o ovoj oblasti, potom tu su obaveze da prati izmene i praksu regulative i daje savete, obezbeđuje sprovođenje politika, ostvarivanja prava

[14] Andrej Diligenski, Dragan Prlja, Dražen Cerović, *Pravo zaštite podataka – GDPR*, op. cit., str. 23.

[15] Danilo Krivokapić, et al., *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – tumačenje novog pravnog okvira*, Danilo Krivokapić (ur.), Misija OEBS i SHARE fondacija, Beograd, 2019, str. 24.

zagarantovanih Opštom uredbom i aktima kompanije, da preduzima mere za obaveštavanje lica o obradi njegovih podataka, da usko sarađuje sa regulatornim telom prilikom inspekcija, nadzora, predlaže pokretanje disciplinskog postupka u slučaju povrede prava lica čiji se podaci obrađuju, kao i niz drugih radnji.[16]

Rukovalac i obrađivač podataka su centralne figure na kojima počiva obrada podataka. Rukovalac može biti fizičko ili pravno lice, ali i organ vlasti. Osnovna funkcija rukovaoca je da on određuje svrhu i način obrade podataka, vremenski period čuvanja podataka, kao i način na koji se postupa sa podacima. Obrađivač, s druge strane, takođe može biti fizičko lice, pravno lice i organ vlasti, kojem su na osnovu ugovornog odnosa sa rukovaocem ili zakonske obaveze povereni poslovi u vezi sa obradom podataka, u čije ime i za čiji račun obrađivač i obrađuje podatke.[17]

Regulatorno telo je nezavisni organ koji se konstituiše na nivou države sa ciljem regulisanja prava zaštite podataka i saradnje sa drugim inostranim nadzornim organima i međunarodnim institucijama, a neki od osnovnih zadataka ovog organa su: informisanje, edukacija, zaštita prava građana, regulisanje, inspekcija, sankcionisanje, sve sa ciljem da svojim savetima i izvršenim nadzorom obezbedi poštovanje principa definisanih u Opštoj uredbi.[18]

3) NAČELA OPŠTE UREDBE O ZAŠTITI PODATAKA

Načela predstavljaju postulate na kojima počiva zakonito rukovanje ličnim podacima. Ona su zvezde vodilje svakog rukovaoca i obrađivača jer svaka radnja koju preduzimaju mora u sebi imati inkorporirana načela. Postoji mandatorna obaveza poštovanja predmetnih načela, te kako su rukovaoci i obrađivači preduzeli sve radnje koje propisuje Uredba, oni mogu biti kažnjeni u slučaju da se utvrdi da je neko od načela povređeno sa kaznom u visini od 20 miliona evra ili 4% ukupnog godišnjeg prihoda kompanije, u zavisnosti od toga koja od navedene dve vrednosti je veća za izricanje kazne.[19]

Načela koja prepoznaje Opšta uredba o zaštiti podataka o ličnosti, u članovima 5–11 su:

– Zakonitost, poštenje i transparentnost;

---

[16] Danilo Krivokapić et al., *Vodič za organe vlasti – zaštita podataka o ličnosti*, Danilo Krivokapić, Đorđe Krivokapić (ur.), Share Fondacija, Novi Sad 2016, str. 34-35.

[17] Klemen Mišič, Maja Lubarda, *Zaštita podataka priručnik za rukovaoce*, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Beograd, 2012, str. 11-12.

[18] Stefan Andonović, doktorska disertacija, *Zaštita podataka u elektronskoj javnoj upravi u Republici Srbiji – pravni aspekti,* op. cit., str. 254-258.

[19] Danilo Krivokapić, et al., *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – tumačenje novog pravnog okvira*, op. cit., str. 33.

– Svrha obrade;
– Minimizacija;
– Tačnost;
– Ograničenje čuvanja;
– Integritet i poverljivost;
– Društvena odgovornost.

Težnja ovog rada je prikaz Opšte uredbe o zaštiti podataka o ličnosti (GDPR), te usled ograničenosti analize i prostora o predmetnim načelima autor će se samo ukratko osvrnuti i ukazati na osnovne karakteristike predmetnih načela. U prvo navedeno načelo zapravo su inkorporirana tri načela: zakonitost, poštenje i transparentnost. Sam naziv upućuje na to da se podaci mogu obrađivati, a i prikupljati, u skladu sa predmetnom Uredbom i na propisan način, odnosno kada postoji validan pravni osnov za prikupljanje i obradu podataka. Pri tome, razumljivo je da je neophodno da i drugi uslovi budu ispunjeni. Princip poštenja se može posmatrati kao nadogradnja principa zakonitosti, a predstavlja moralnu obavezu rukovaoca da postupa pošteno i sa pažnjom prema ličnim podacima. U smislu ovog načela kasnije će biti reči i o principu integriteta, a koje ne bi bilo moguće ispuniti bez preduslova poštovanja principa poštenja. Princip transparentnosti ima direktan uticaj na povećanje prava lica čiji se podaci prikupljaju, a odnosi se na to da lice ima pravo da zna koji se podaci prikupljaju, u koje svrhe, u kom obimu, koliko se dugo čuvaju, ko ima pristup podacima, a sva ta obaveštenja moraju biti razumljiva i nesumnjivo jasna svakom licu. Načelo transparentnosti omogućava licu da ima kontrolu nad svojim podacima, a ujedno utiče i na povećanje poverljivosti podataka i očuvanje bezbednosti podataka. Svrha obrade podataka mora biti ograničena, te se podaci mogu prikupljati samo u tačno određenu svrhu, koja mora biti jasno i nedvosmisleno definisana pre prikupljanja i obrade predmetnih podataka, a lice koje je subjekat obrade mora imati uvid u kom kontekstu se njegovi podaci prikupljaju i u koje svrhe. Princip minimizacije dopunjuje ograničenost svrhe obrade podataka, u smislu da mora postojati i ograničenost broja i obima prikupljanja podataka, odnosno da se smeju prikupljati samo oni podaci koji su neophodni da bi se ispunila svrha obrade podataka, dok, s druge strane, svi podaci koji nisu neophodni za naznačenu svrhu obrade predstavljaju prestup i kršenje prava lica prema Uredbi. Na ovo načelo direktno je oslonjen i član 42 GDPR-a u kojem se opisuju mere zaštite i uvode termini *privacy by design* i *privacy by default*, a koji se pre svega odnose na sisteme u kojima bi se prikupljeni podaci klasifikovali uz ugrađene sisteme bezbednosti informacija i privatnosti, tako da se ne prikupljaju a samim tim i ne obrađuju nepotrebni podaci.[20] Sa manjim brojem podataka u toku prikupljanja podataka, od obrade do analize, posredno se postiže i veća bezbednost

[20] Ibid., str. 34.

podataka ili se makar postiže manja izloženost povredama bezbednosti podataka usled manje količine podataka u opticaju. Ograničenost čuvanja podataka je u direktnoj korelaciji sa načelom ograničenosti svrhe obrade podataka, te se podaci mogu čuvati samo onaj vremenski period koji je neophodan ali i jasno i transparentno naznačen, da bi se svrha obrade ostvarila. Dalje, načelo tačnosti je samo po sebi jasno i podrazumeva da podaci budu tačni i pravovremeni. Osim tačnosti, obrada podataka mora da obezbedi sigurnost prava zaštite podataka i privatnosti licu čiji se podaci prikupljaju, uz primenu odgovarajućih pravnih, tehničkih i organizacionih mera, kako bi se smanjile šanse za povredu ličnih podataka, ali i obezbedila pravovremena i adekvatna reakcija u slučaju gubitaka, krađe ili curenja podataka. Princip poverljivosti i integriteta uključen je u svaki aspekt sistema zaštite podataka, a inkorporiran je u većini slučajeva u raznim politikama privatnosti, upozorenjima i obaveštenjima o politici zaštite podataka.

Ako načela posmatramo kao osnovu ili polazište na kojem počiva sistem zaštite podataka i Opšta uredba o zaštiti podataka, onda bi za cilj trebalo postaviti obezbeđenje i unapređenje prava lica čiji se lični podaci prikupljaju.

4) PRAVA LICA

Opšta uredba o zaštiti podataka propisuje brojna prava građanima u vezi sa podacima o ličnosti. Posao rukovaoca je da sprovede i stvori uslove za primenu propisa koji obezbeđuju prava licima, u saradnji sa obrađivačem na kojem je pretežno primena tehničkih, organizacionih i pravnih mera, a regulatorno telo ima kontrolnu i nadzornu funkciju nad radom rukovaoca, a može postupati i po žalbi fizičkog lica. Povećanje prava građana čiji se podaci prikupljaju, kao i povećanje kontrole nad tokom i obimom podataka, centralna su težnja GDPR-a. U tom smislu izdvajaju se:

– Pravo na pristup podacima, ispravku, dopunu i brisanje podataka;
– Pravo na obaveštenje o obradi i ograničenje obrade;
– Pravo na prenosivost podataka;
– Automatizovano donošenje odluka;
– Pravo na prigovor.

Članom 15 GDPR-a definisano je pravo lica da može da zatraži od rukovaoca informaciju da li se njegovi lični podaci obrađuju, u koju svrhu, u kom obimu, ko ima pristup njima, na koji vremenski period se čuvaju, te ima pravo da sazna sve relevantne informacije u vezi svojih ličnih podataka i da zatraži pristup podacima. Narednim članovima obezbeđuju se prava lica da može od rukovaoca da zatraži da se njegovi podaci isprave ili ažuriraju, a naročito i izbrišu ukoliko predmetni podaci nanose štetu ili krše neko drugo pravo propisano pozitivnim zakonima Evropske unije. U tom pogledu postoji ograničenje prava na brisanje ličnih podataka, ili prava

na zaborav, a to je da se brisanje ne može izvršiti ukoliko su prikupljeni kako bi se ispunila svrha ostvarivanja prava slobode informisanja ili izražavanja, ispunjenja neke druge zakonske obaveze ili radi poštovanja radnji učinjenih u javnom interesu. Lice – subjekt obrade ima pravo da bude jasno i transparentno obavešten o svrsi obrade podataka i u tom kontekstu lice ima pravo da ograniči obradu podataka kada su podaci o njemu netačni, kada je obrada nezakonita ili su podaci nepotrebni za predmetnu svrhu obrade, kada je podnet prigovor u vezi navedenih situacija i kada postoji sumnja da se radi o konfliktu interesa subjekta prava i rukovaoca.[21]

Pravo na prenosivost podataka je novostvoreno pravo definisano Uredbom članom 20, a odnosi se na transfer ličnih podataka jednog lica kojima rukuje rukovalac, a na zahtev lica se ti podaci mogu transponovati – „preneti" drugom rukovaocu, kada je to tehnički moguće i kada ne ugrožava druga prava lica. Prenosivost podataka je moguća i kada je obrada zasnovana na pristanku i kada se vrši automatski.[22] Prava koja se odnose na automatizovano donošenje odluka bi se zbog svoje široke primene u digitalnom svetu, na internetu, brojnim sajtovima i društvenim mrežama, mogla posmatrati kao zasebna celina. Automatska obrada se, pre svega, odnosi na obradu i prikupljanje podataka gde radnje vrši mašina, kompjuter, softver ili programski dodatak. Na ovaj način skupljaju se mnogi lični podaci u vidu ličnih preferencija, na primer koje sajtove najčešće posećujemo, koje knjige volimo da čitamo, koje lekove, medicinske usluge i bolesti pretražujemo i dr. i na osnovu prikupljenih podataka se vrši pravljenje ličnih profila o nama, tzv. profilisanje. Profilisanje ima za cilj nuđenje određenih proizvoda ili usluga, targetiranje putem ciljanog marketinga i pružanje sadržaja namenjenog našem profilu. U smislu automatske obrade mora se povesti računa da se osetljivim ličnim podacima rukuje na zakonit način, kao i da ne dođe do ugrožavanja radnog, ugovornog ili socijalnog prava, verskih, seksualnih, političkih sloboda i drugih ljudskih prava.

Pravo na prigovor daje licu pravo žalbe u vezi sa predmetnom obradom podataka, prema kojem rukovalac mora da prestane sa obradom podataka dok se ne utvrdi da li je žalba osnovana, a pravni osnov za obradu podataka valjan. Ograničenje prigovora lica se, pre svega, odnosi na legitimni interes, odnosno u određenim slučajevima interes društva preteže u odnosu na interese pojedinca.

Ovo su neka od prava koje ova obimna Regulativa prepoznaje i koja čoveka i kontrolu nad ličnim podacima stavlja u središte sistema zaštite podataka i postavlja za cilj povećanje privatnosti u digitalnom dobu kada je privatnost suočena sa mnogim izazovima.[23]

---

[21] Ibid., str. 75.

[22] Sanja Prlja, „Pravo na zaštitu ličnih podataka u EU", op. cit., str. 95.

[23] Za više o pravima lica u vezi sa podacima o ličnosti, videti: Stefan Andonović, Dragan Prlja, „Osnovi prava zaštite podataka o ličnosti", *Institut za uporedno pravo*, Beograd, 2020, str. 87-115.

5) MAPIRANJE OBAVEZE KOMPANIJA

Proces implementacije Opšte uredbe o zaštiti podataka o ličnosti u poslovanje kompanije je izuzetno kompleksan poduhvat koji kompanija mora da učini kako bi ispunila svoju zakonsku obavezu i uskladila svoje poslovanje sa konceptom zaštite podataka o ličnosti. Takođe, kompanije dobijaju i šansu za ostvarivanje boljih poslovnih saradnji i izlazaka na nova tržišta jer se u modernom digitalnom dobu očekuje da kompanije imaju implementiran sistem zaštite podataka i koncept privatnosti u svoje poslovanje. Svakako se kao razlog integracije ka ovim evropskim vrednostima nameće i izbegavanje visokih kazni o kojima je bilo reči u toku rada. Tu je i podsticaj za preduzeća van EU koji saglašavanjem sa ovom Uredbom stiču šansu za poslovanje na evropskom tržištu i mogućnost nuđenja svojih roba i usluga evropskim građanima. Dalje, korist inkorporiranja GDPR-a u poslovanje kompanije trebalo bi da dovede do očuvanja reputacije i ugleda kompanije usled adekvatnog prikupljanja, čuvanja i obrađivanja, ali i dalje distribucije podataka klijenata. Osim očuvanja reputacije u poslovnom svetu i među klijentima, integrisanje sistema prava zaštite podataka u poslovne procese kompanija za cilj bi moglo imati povećanje opšte društvene dobrobiti, a u kojem bi se ispoštovala osnovna prava svakog pojedinca u ovoj oblasti.[24]

Proces implementacije Regulative u poslovanje preduzeća trebalo bi da obuhvata tri ključne oblasti, a to su:

1) Organizacija zaduženja u okviru kompanije;

2) Mapiranje podataka;

3) Preduzimanje pravnih, tehničkih i organizacionih mera.

Kako regulativa pogađa poslovanje kompanije i najveći broj sektora i mora da uskladi svoje poslovanje sa predmetnom Regulativom, neophodno je pre svega upoznati zaposlene sa sadržinom i zahtevima koje postavlja Uredba, a potom ih obučiti za primenu ove legislative primenjeno na reon u kojem zaposleni radi. Potrebno je kontinuirano raditi na podizanju svesti zaposlenih o značaju zaštite ličnih podataka, kako podataka zaposlenih tako i klijenata. Preporučljivo je izraditi *gap* analizu s ciljem identifikovanja koji procesi nisu, ili u kojoj su meri usklađeni sa zahtevima GDPR-a, kao i koje korake je neophodno sprovesti da bi se uveli u standard.[25] Potom, kao i u svakom projektu, potrebno je dobro isplanirati korake, a zatim i podeliti zaduženja kako bi proces implementacije ovako kompleksne

[24] Marija Majstorović, „Usklađivanje poslovanja preduzeća sa GDPR", *6th International Conference Law, Economy and management in modern ambience,* LEMIMA 2019, Fakultet za poslovne studije i pravo Univerzitet „Union – Nikola Tesla", Beograd 2019, UDC 342.721 (497.11), str. 53-54.

[25] Za pojašnjenje pojma „Gap analiza", videti: Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/gap-analysis.

Regulative bio koordinisan i celishodan. U većini slučajeva neophodno je da pravna služba, kadrovska služba, marketing, IT sektor i po potrebi i drugi sektori raspodele zaduženja i sprovedu mere i procedure koje su definisane Regulativom. U zavisnosti od vrste kompanije i podataka koji se obrađuju, potrebno je imenovati Lice za zaštitu podataka, a koje može biti zaposleno lice iz kompanije ali može biti i eksterno angažovan. Jedan od prvih koraka je da se navedu aktivnosti obrade koje se odvijaju pošto su prikupljeni podaci, potom je neophodno pribaviti pristanak lica ili drugi pravni osnov za prikupljanje podataka i obavestiti lice o preduzetim radnjama. Sledeći korak je definisanje zaduženja rukovaoca, obrađivača i službenika za zaštitu podataka. Potrebno je da kompanija ustanovi svoju funkciju da li je u ulozi rukovaoca ili obrađivača, zavisno od kontakta i radnji koje poduzima sa predmetnim podacima. Rukovalac ima obavezu da na osnovu člana 30 Uredbe vodi evidenciju o aktivnostima obrade podataka, te o informativnim podacima o obrađivaču, rukovaocu i licu za zaštitu podataka, svrsi obrade, kategorijama i opisu ličnih podataka, kao i o primaocima podataka itd. Preporučuje se i vođenje evidencije o zakonskim osnovama za obradu podataka i ugovorima o obradama. Takođe, članom 15 rukovalac je u obavezi da na zahtev subjekta podataka dozvoli pravo pristupa ličnim podacima lica koje je zatražilo uvid. Obrađivač i rukovalac su dva posebna pravna entiteta ali su u međusobnom odnosu. Rukovalac na osnovu zakona ili na osnovu ugovornog odnosa poverava obrađivaču deo poslova vezanih za obradu podataka, odnosno obrađivač je izvršilac radnji u smislu obrade podataka, odnosno radnji koje mu je dodelio rukovalac.[26] Lice za zaštitu podataka o ličnosti (DPO) ili Službenik za zaštitu podataka predstavlja novo zanimanje od kada je u primeni Uredba.[27] Osnovna misija DPO-a je da obrada podataka ne krši ljudska prava i privatnost lica čiji se podaci prikupljaju. Lice savetuje koje mere i zaštite bi obrada morala da sadrži. Lice za zaštitu podataka ne mora nužno biti pravnik, ali se preporučuje da bude dobro pravno potkovan, kao i da poseduje određeno razumevanje IT bezbednosti, iz razloga što DPO mora biti obavešten o politikama i pravnim kontrolama kako bi bio u mogućnosti da proceni rizik od povrede podataka. Važna funkcija ovog lica je i podizanje svesti o zaštiti i sigurnosti podataka u kompaniji, prema članu 39 Uredbe. Značaj ovog novog zanimanja ogleda se i u broju i obimu članova koji su posvećeni Službeniku za zaštitu podataka u Uredbi, a neki od njih su: članovi 37–39, iz glave četvrte, koji su posvećeni imenovanju, funkcijom i zaduženjima ovog lica, potom članom 30 navodi se uloga ovog lica u registru i proceni uticaja (član 39). Takođe, spominje se i u drugim članovima, a član 97 naglašava karakter nezavisnosti. Osim

[26] Danilo Krivokapić et al., *Vodič za organe vlasti – zaštita podataka o ličnosti*, op. cit., str. 17.

[27] U daljem tekstu će se koristiti skraćenica DPO koja potiče od engl. *Data Protection Officer*, u prevodu na srpski jezik: Službenik za zaštitu podataka. Za više o licu za zaštitu podataka o ličnosti u Evropskoj uniji, videti: Paul Lambert, *Understanding the New European Protection Rules*, Taylor & Francis Group 2018, str. 457-467.

savetodavne funkcije ima i obavezu da sarađuje sa nezavisnim regulatornim telom prilikom inspekcija ili žalbenih postupaka.[28]

Drugu bitnu celinu u procesu implementacije Regulative u poslovanje preduzeća čini mapiranje podataka. Potrebno je ustanoviti tok podataka, koji se podaci prikupljaju, u kom obimu, broju, kako se prikupljaju, gde i koliko dugo se čuvaju, da li se brišu i kada, koji put prolaze od prikupljanja, obrade do distribucije, ko ima pristup podacima i dr. Odnosno, potrebno je ustanoviti sve relevantne informacije koje se tiču podataka koji se prikupljaju i proceniti rizik i način za upravljanje takvim podacima. Neophodno je definisati razne procedure u skladu sa klasom podataka u odnosu na vrstu, osetljivost i rizik koji takvi podaci nose. Poenta mapiranja podataka je razumevanje koji se podaci prikupljaju i iz kog razloga, te da li su prikupljeni podaci korisni za naznačenu svrhu obrade podataka, te bi u skladu sa konceptom minimizacije trebalo prikupljati samo onoliko podataka koliko je stvarno neophodno da bi se ispunila svrha obrade. Članom 30 Uredbe kompanijama se na teret stavlja obaveza vođenja evidencije o aktivnostima obrade koja bi trebalo da sadrži informacije o rukovaocu i službeniku za zaštitu podataka, svrsi obrade, kategorijama lica čiji se podaci prikupljaju i vrsti ličnih podataka, primaocima ličnih podataka, predviđenim rokovima za brisanje podataka i drugo. Preporučljivo je uključiti i načelni opis tehničkih i organizacionih mera iz člana 32. U ovom procesu bi trebalo da učestvuju svi relevantni činioci od kadrovske, marketinške, pravne i informatičke službe, odnosno svi oni koji imaju saznanja o tome gde se i koji podaci čuvaju, u papirnom, digitalnom, audio i drugim formatima, a lice za zaštitu podataka bi trebalo da od tih informacija sačini celinu i izvrši mapiranje podataka.[29]

U pogledu obima pravnih, tehničkih i organizacionih mera koje bi kompanija trebala da preduzme kako bi uskladila svoje poslovanje sa GDPR-om moglo bi se napisati više naučnih radova i sprovesti brojne analize. U pogledu ovih mera autor će navesti svega nekoliko značajnih koraka. Procena rizika je neizostavna na putu saglašavanja sa Uredbom. Sa urađenom procenom rizika trebalo bi da se dobije odgovor na pitanje sa kojim pretnjama se suočava kompanija u pogledu zaštite podataka i na osnovu analize bi dalje trebalo da se sprovedu odgovarajuće tehničke i organizacione mere kako bi se obezbedila sigurnost podataka. Pod procenom rizika važno je uraditi i DPIA, a što predstavlja izveštaj o usklađenosti obrade podataka, rizicima i problemima koji mogu nastati kao rezultat obrade.[30]

---

[28] European Data Protection Supervisor, Data Protection Officer (DPO), b.d., https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en, pristupljeno 20.9.2020.

[29] GDPR Data Flow Mapping, b.d., https://www.itgovernance.eu/en-ie/gdpr-data-mapping-ie, pristupljeno 22.9.2020.

[30] DPIA skraćenica od engl. *Data protection impact assessments*, u prevodu na srpski jezik: Procena uticaja na zaštitu podataka. Za više o proceni uticaja na zaštitu podataka, videti: Ben

Sprovođenje procene rizika preporučljivo je izraditi preko procene uticaja na privatnost (PIA), kako je navedeno u članu 35 GDPR-a.

U pogledu tehničkih i bezbednosnih mera potrebno je sprovesti mere kojima se smanjuje rizik od zloupotrebe podataka, a to se uglavnom postiže pseudonimizacijom i/ili anonimizacijom podataka. Pseudonimizacijom se postiže obrada podataka tako da se oni ne mogu više pripisati i dovesti u vezu sa licem koje je nosilac tih podataka. U pojednostavljenom obliku podaci o nečijem imenu i prezimenu se u određenoj bazi ne skladište u formatu Petar Petrović, već dobijaju neki šifrovani oblik, na primer p1A HDK. Anonimizacija prestavlja korak dalje u zaštiti podataka. Osnovna razlika je što se u slučaju pseudonimizacije nosilac podataka može identifikovati uz pomoć dešifrovanja jer postoji baza koja povezuje podatak sa njegovim pseudonimom, a dok je u slučaju anonimizacije taj proces izuzetno komplikovan i u najvećem broju slučajeva se identitet podatka ne može vratiti.[31]

Potom je potrebno osnovati efikasan sistem koji bi obezbedio održavanje stalne poverljivosti, integriteta i otpornosti sistema na udare i izazove koje postavlja obrada novih podataka i potrebno je konstantno unapređivati bezbednosne mere u skladu sa potrebama kompanije i tehnološkim napretkom. U skladu sa tim zaštita podataka bi trebalo da bude inkorporirana u poslovne procese i infrastrukturu kompanije, te bi i podešavanja privatnosti kao i životni ciklus podataka trebali da budu postavljeni u skladu sa zahtevima GDPR-a.[32] Pravne mere prožimaju svaki proces i korak ka ispunjenju zahteva iz Uredbe. Potrebno je dokumentovati sve preduzete radnje, konstantno vršiti proveru i unapređenje pravničkih procedura i akata i vršiti edukaciju svih aktera ali i zaposlenih u kompaniji. Osnovni zadatak pravne službe je da pribavi adekvatne pravne osnove za prikupljanje i obradu podataka i tako smanji rizik od prijave nadležnom organu i sankcionisanje kompanije. Obrada je moguća kada postoji saglasnost lica čiji se podaci prikupljaju ili je zaključen ugovorni odnos između kompanije i klijenta, odnosno lica čiji se podaci prikupljaju. Potom, obrada je moguća kada je neophodno ispunjenje pravne obaveze ili javnog interesa prema domaćem ili zakonodavstvu Evropske unije. Pravni osnov za obradu može da bude i zaštita vitalnih interesa pojedinca ili pak zaštita legitimnih interesa kompanije. U ovom slučaju se mora obratiti značajna pažnja da ne postoji konflikt interesa ljudskih prava i sloboda lica čiji se podaci prikupljaju i kompanije.[33]

Wolford, *Data Protection Impact Assessment (DPIA),* b.d., https://gdpr.eu/data-protection-impact-assessment-template/, pristupljeno 10.9.2020.

[31] Andrej Diligenski, Dragan Prlja, Dražen Cerović, *Pravo zaštite podataka – GDPR*, op. cit., str. 41.

[32] O primeni koncepta *Privacy by design* i *Privacy by default,* videti: „Anonimizacija i pseudonimizacija podataka", *CERT*, 2018, dostupno na: https://www.cert.hr/wp-content/uploads/2018/08/anonimizacija_i_pseudonimizacija_podataka.pdf, pristupljeno 20.9.2020.

[33] Ivan Milošević, *GDPR Uputstvo za primenu*, op. cit., dostupno na: https://www.jpm.rs/wp-content/uploads/2018/04/gdpr.pdf, pristupljeno 5. avgust 2020.

Mora se napomenuti da je proces implementacije Opšte regulative o zaštiti podataka u poslovanje kompanija relativno nov zahtev, te da su brojne kompanije još uvek u procesu upoznavanja sa brojnim odredbama Uredbe. Multinacionalne kompanije prednjače u broju mera i procedura i stepenu implementacije ovog propisa u svoje poslovanje, dok manje kompanije imaju gotovo identične obaveze prema GDPR-u kao i gigantske kompanije, stoga se postavlja pitanje profitabilnosti i povećanog administrativnog ali i novčanog nameta, iz razloga neophodnosti angažovanja eksternih stručnjaka za zaštitu podataka. Ovaj proces se mora obavljati kontinuirano i sinhronizovano sa svim departmanima u okviru kompanije.

6) ZAKLJUČAK

Opšta Uredba o zaštiti podataka u primeni je od 25. maja 2018. godine. Kompanije su preduzele brojne korake kako bi implementirale ovu kompleksnu regulativu u svoje poslovanje i tako sebi obezbedile mesto u tržišnoj igri u kojoj podaci predstavljaju novi kapital, ali i spasile svoje poslovanje i reputaciju od curenja podataka i visokih kazni. Ipak, težnja ove Uredbe je obezbeđenje prava na zaštitu podataka i prava na privatnost u internet eri, kada je svakodnevno u opticaju bezbroj ličnih podataka i kada pojedinci svakodnevno svoje podatke ostavljaju brojnim kompanijama na obradu i korišćenje, često bez mnogo znanja.

Opšta regulativa o zaštiti podataka je jedan od najznačajnijih pravnih akata donetih u poslednje vreme i ima značajan uticaj na globalnom nivou u oblasti zaštite podataka i privatnosti, kako u Evropi tako i šire. Najveći broj zemalja u svetu je usaglasio svoje zakonodavstvo sa GDPR regulativom, a pomenute multinacionalne kompanije, a potom i nacionalne kompanije su pod uticajem GDPR-a promenile svoj način poslovanja i odnos prema prikupljanju, obradi i čuvanju podataka. Primena ove Uredbe ogleda se i u naplaćivanju mnogobrojnih visokih kazni, od čega je samo u 2020. godini napisano više od 150 novčanih kazni u ukupnom iznosu od preko 60 miliona evra, prema finansijskom istraživanju kompanije *Finbold*.[34] Neke od najviših izrečenih kazni su kazne prema *British Airways*, britanskoj avio kompaniju, u iznosu od preko 204 miliona evra, potom je lanac hotela *Mariott International* platio preko 110 miliona evra za gubitak podataka svojih gostiju. Prošle godine je Guglu (*Google*) francusko regulatorno telo izreklo kaznu od preko 50 miliona evra, a italijanski telekomunikacioni operater TIM je platio kaznu od preko 28 miliona evra[35]. Primera milionskih kazni u praksi ima još, a one utiču na

[34] Finbold, GDPR fines 2020, b.d., dostupno na: https://finbold.com/gdpr-fines-2020/, pristupljeno 25.09.2020.

[35] Data Privacy Manager, 5 biggest GDPR fines so far, 2020, dostupno na: https://data privacymanager.net/5-biggest-gdpr-fines-so-far-2020/, pristupljeno 25.09.2020.

još dosledniju i širu primenu Opšte uredbe o zaštiti podataka, kako u nacionalnim zakonodavstvima tako i u poslovanju kompanija.

U duhu ovog rada, cilj Opšte uredbe o zaštiti podataka o ličnosti je podizanje svesti o zaštiti podataka, savesnijem pristupu kompanija prema prikupljanju i obradi ličnih podataka, ali i odgovornijem pristupu korisnika interneta prema svojoj privatnosti i ostavljanju ličnih podataka na raspolaganje brojnim sajtovima, a u tom kontekstu se obeležava i Dan zaštite podataka u Evropi svakog 28. januara, simbolično na dan Konvencije 108 Saveta Evrope o ličnim podacima.

7) LITERATURA

Andonović, Stefan, „Zaštita podataka u elektronskoj javnoj upravi u Republici Srbiji – pravni aspekti", doktorska disertacija, *Pravni fakultet Univerziteta u Beogradu*, Beograd 2019.

Borhart, Klaus-Diter, *Abeceda prava Evropske unije*, Kancelarija za publikacije Evropske unije, Luksemburg, 2010.

Brajušković, Sandra, Blagojević, Goran, „Novo poglavlje u oblasti zaštite podataka o ličnosti: opšta regulativa EU o zaštiti podataka o ličnosti", *Istraživački centar Skupštine Crne Gore*, Podgorica 2018.

Čizmić, Jovan, Boban, Marija „Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj", *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, vol. 39, br. 1, 377-410 (2018), UDK 342.738::061.1EU, https://doi.org/10.30925/zpfsr.39.1.13.

Dašić, Predrag, Turmanidze, Raul, „Industrija 4.0: stvarnost ili priviđanje (Pozivni referat)", XVI međunarodna konferencija ekonomsko/pravno/komunikacijski aspekti zemalja Zapadnog Balkana sa posebnim osvrtom na Bosnu i Hercegovinu u procesu pristupa Evropskoj uniji, Ekonomski fakultet, Rijeka 2017, str. 80-89.

Diligenski, Andrej, Prlja, Dragan, Cerović, Dražen, *Pravo zaštite podataka – GDPR*, Institut za uporedno pravo, Beograd, 2018.

Đukić, Dejan, „Zaštita podataka o ličnosti sa osvrtom na novo zakonodavstvo Evropske unije u ovoj oblasti", *Pravni zapisi br. 1/2017*, Pravni fakultet Univerziteta Union, Beograd 2017.

Karabegović, Isak, Karabegović, Edina, „Implementacija "Industrije 4.0" primjenom robota i digitalne tehnologije u proizvodnim procesima u Kini", *Tehnika – Mašinstvo 67 (2018)*, Tehnički fakultet, Bosna i Hercegovina, Bihać 2018, str. 225-231.

Krivokapić, Đ., Adamović, J., Tasić, A., Petrovski, A., Kalezić, P., Krivokapić, *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – tumačenje novog pravnog okvira*, Misija OEBS i SHARE fondacija, Beograd, 2019.

Krivokapić D., Krivokapić Đ., Todorović I., Komazec S., Petrovski, A., Ercegović K., *Vodič za organe vlasti – zaštita podataka o ličnosti*, Share Fondacija, Novi Sad, 2016.

Lađevac, Ivona, „Povelja Evropske unije o osnovnim pravima", Blagoje Babić (ur.), *Vodič kroz pravo Evropske unije*, Institut za međunarodnu politiku i privredu, Beograd 2005.

Lambert, Paul, *Understanding the New European Protection Rules,* Taylor & Francis Group, New York 2018.

Lilić, Stevan, „Pravo privatnosti i informatička tehnologija", *Kompjuteri i pravo br. 1-2/1999*.

Majstorović, Marija, „Usklađivanje poslovanja preduzeća sa GDPR", *6th International Conference Law, Economy and management in modern ambience LEMIMA 2019*, Fakultet za poslovne studije i pravo Univerzitet „Union – Nikola Tesla", Beograd 2019, UDC 342.721 (497.11).

Milenković, Dejan, „Značaj nezavisnih institucija u zaštiti ljudskih prava", *Jubilarna monografija 15 godina rada Poverenika*, Poverenik za informacije od javnog značaja i zaštitu podataka, Beograd 2019.

Prlja, Sanja, „Pravo na zaštitu ličnih podataka u EU", *Strani pravni život 2018/1*, Beograd 2018, str. 89, UDK: 342.721 (4-672 EU).

Šabić, Rodoljub, *15 godina rada Poverenika za informacije od javnog značaja i zaštitu podataka: Jubilarna monografija*, Poverenik za informacije od javnog značaja i zaštitu podataka, Beograd 2019.

GENERAL REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF THE EUROPEAN UNION ON DATA PROTECTION (GDPR) – OVERVIEW AND NEWS

Summary: Everyday use of the Internet, both for business needs and for private purposes (from storing data on cloud systems, using applications and many other contents that access various biometric and personal data), has put a modern man at the center of technological development, digitalization, and connectivity via different networks. The significance that the exchange of goods, gold, and then the trade of goods and services once had on the economic development and technological progress is today transferred on data. In the digital age when data are the driver and the basis for the development of every company and the basic derivative of every society, citizens often and without much thought easily leave their data available to many companies that collect data and make business decisions based on their processing. This led to the need to regulate the field of data protection. With the increase in the number of data about all of us comes the need to protect privacy and increase control of our personal data. In line with this aspiration and the need to improve the legal framework with the legacy of modern times, the General Regulation on Personal Data Protection (GDPR) was adopted in 2016. It regulates in detail the rights of persons and the obligations of companies. The aim of this paper is to present important characteristics and innovations in terms of new institutes and concepts, as well as to consider the positive effects that the Regulation has introduced in the field of European Union law, but also on the rights of all persons whose data are processed. The analysis was performed on the basis of a review of the relevant legislative framework of the European Union and documents adopted by the European regulatory bodies and relevant institutions, from the European Parliament, the Council of the European Union, the European Data Protection Board, the European Commission, etc.

Keywords: General data protection regulations, GDPR, data protection law, European Union law.