Scientific paper/Znanstveni rad

EU GENERAL DATA PROTECTION REGULATION IMPLEMENTATION: PRELIMINARY ANALYSIS OF RECENT RESEARCH EFFORTS AND CHALLENGES

IMPLEMENTACIJA OPĆE UREDBE O ZAŠTITI PODATAKA PRI EU: PRELIMINARNA ANALIZA AKTUALNIH ISTRAŽIVAČKIH NAPORA I IZAZOVA

ANTUN BILOŠ
Faculty of Economics in Osijek
Josip Juraj Strossmayer University of Osijek
Gajev trg 7, 31000 Osijek, Croatia
abilos@efos.hr

DAVORIN TURKALJ
Faculty of Economics in Osijek
Josip Juraj Strossmayer University of Osijek
Gajev trg 7, 31000 Osijek, Croatia
davorin@efos.hr

IVAN KELIĆ
Faculty of Economics in Osijek
Josip Juraj Strossmayer University of Osijek
Gajev trg 7, 31000 Osijek, Croatia
ikelic@efos.hr

ABSTRACT

On May 25, 2018, the old European Data Protection Directive (Directive 95/46/EC) was replaced with the new General Data Protection Regulation (GDPR). The GDPR is one of the latest initiatives in the continuous global recognition of the value and importance of personal information and privacy. The new regulation applies to those responsible for controlling and processing personal data. Data controllers are expected to meet strict standards and procedures related to collecting, holding, distributing and processing personal data and will be held accountable for ensuring compliance with the new regulation. This paper provides an overview of recent academic and professional articles based on the influence of GDPR on various subjects, including scientific research, privacy issues, company policies and implications on end users. Considering the fact that the new regulation was only recently enforced, the true effects on all the stakeholders are still to come to full effect. The GDPR provides a delicate balance between the necessity of effectively protecting data subjects' rights

in a digitalized world while simultaneously allowing the processing of personal data for heterogeneous business oriented activities. This paper discusses several research challenges and suggests guidelines on future research approaches on the influence of GDPR on various target groups. Special focus is set on two target groups influenced heavily by GDPR: companies of various sectors dealing with personal data and users of various ICT platforms. As the topic is rather significant in terms of personal data handling and privacy, this paper aims to provide preliminary research analysis and suggest a foundation for comprehensive future research activities.

KEYWORDS: general data protection regulation, GDPR, research analysis, guidelines, privacy

SAŽETAK

Stara europska Direktiva o zaštiti podataka (Directive 95/46/EC) je 25. svibnja 2018. zamijenjena s novom Općom uredbom o zaštiti podataka (General data protection directive, GDPR). GDPR je jedna od recentnijih inicijativa u kontinuiranom globalnom prepoznavanju značaja osobnih informacija i privatnosti. Nova regulativa primjenjuje se na subjekte koji kontroliraju i procesuiraju osobne podatke. Od subjekata koji kontroliraju podatke se očekuje pridržavanje strogim standardima i procedurama pri prikupljanju, čuvanju, distribuiranju i obradi osobnih podataka i smatra ih se odgovornima za osiguranje pridržavanja novoj regulativi. Rad daje pregled recentnih znanstvenih i stručnih članaka vezanih uz utjecaj Uredbe na različitim poljima, od znanstvenih istraživanja, izazove privatnosti, politike poslovnih subjekata te implikacija na krajnje korisnike. Uvažavajući činjenicu da je nova regulativa tek razmjeno nedavno primijenjena, pravi učinci na sve dionike će tek naknadno biti vidljivi. Opća uredba pruža osjetljivu ravnotežu između nužne učinkovite zaštite prava podataka subjekta u digitaliziranom svijetu uz istovremeno omogućavanje obrade osobnih podataka za heterogene poslovno orijentirane potrebe. Rad se bavi s nekoliko istraživačkih izazova i predlaže smjernice za buduće istraživačke pristupe pri utjecaju Uredbe na različite ciljne skupine. Poseban fokus umjeren je na dvije skupine koje su pod snažnim utjecajem Uredbe: poslovni subjekti različitih djelatnosti koje koriste osobne podatke te krajnji korisnici različitih platformi informacijsko-komunikacijskih tehnologija. Uvažavajući činjenicu da je tema iznimno značajna zbog uporabe osobnih podataka i privatnosti, cilj rada je pružiti preliminarnu analizu istraživanja i oblikovati temelj za buduće robusnije istraživačke napore.

KLJUČNE RIJEČI: opća uredba o zaštiti podataka, GDPR, analiza istraživanja, smjernice, privatnost

1 UVOD

Internetska i/ili digitalna revolucija koja se odigrala devedesetih godina prošlog stoljeća puno je više od uspješne tehnološke inovacije. Globalni uspjeh koji je postigao TCP/IP protokol za sveopću popularizaciju i globalni prodor interneta, nedvojbeno je nepovratno izmijenio komunikaciju i razmjenu podataka u najširem mogućem smislu, snažno utječući na društvene

promjene. Jedna od glavnih razvojnih snaga koja je omogućila globalnu popularnost i prodor u gotovo svaki zakutak svijeta jest otvorenost arhitekture internetske mreže [Čizmić i Boban, 2018] u kojoj su njezini korisnici istovremeno i kreatori sadržaja, stvaratelji zajednica i osnaživači daljnjeg razvoja. Na tragu prethodnog, ova tehnološka inovacija osnažila je i proširila mogućnosti različitih organizacija i subjekata u prikupljanju, pohranjivanju i razmjeni digitaliziranih podataka s gotovo bilo koje točke na svijetu. Rastuća složenost obrade podataka dodatno je proširila informacijsku asimetriju između onih koji procesuiraju podatke i pojedinaca te stvorila posve nove oblike podataka nastale kroz interakciju pojedinaca i računala [ili digitalnih uređaja], ali i između računala međusobno [Lachaud, 2018].

Brojna područja modernih digitalnih tehnologija poput *Internet of Things* (IoT), robotike, umjetne i proširene stvarnosti se snažno razvijaju pomičući granice mogućega. Mnogi stručnjaci predviđaju nastavak progresivnog rasta i razvoja specijalizirane umjetne inteligencije koja će u brojnim novim poljima dosegnuti i prestići ljudske mogućnosti [Sokolovska i Kocarev, 2018]. Složeni algoritmi koji su počesto zamjena za trome birokratske procese koriste se za donošenje posljedičnih odluka o pojedincima što podiže brojna pitanja vezana uz privatnost građana te osiguravanje pravde, pravičnosti i odgovornosti korištenih algoritama.

Privatnost i informacijska prava su podjednako važni i proporcionalno zaštićeni pod pravom Europske Unije, a ravnoteža između ovih prava je nužna za osiguravanje osobnih sloboda i demokratske participacije [Keller, 2017]. U suvremenom informacijskom društvu, informacije su sastavni element slobode i prava na širenje informacija koji u velikoj mjeri ovisi o legitimnosti i mogućnosti upravljanja velikim bazama podataka [Čizmić i Boban, 2018]. Podaci odnosno informacije predstavljaju osnovnu vrijednost digitalnih tržišta [Martinez-Martinez, 2017]. S druge strane, privatnost u vremenu informacijskog društva zaista predstavlja brojne izazove na različitim razinama i osnovama [Post, 2017]. Osiguravanje ravnoteže između identifikacije i pristupu podacima s jedne strane i korisničkih prava na privatnost s druge, od neobično je velikog značaja. Ipak, osiguravanje spomenute ravnoteže predstavlja velik izazov zbog specifičnosti arhitekture internetskih tehnologija i tehnika anonimizacije [Wachter, 2018].

Za pretpostaviti je da prosječni internetski korisnik nije ni svjestan koliko digitaliziranih informacija svakodnevno proizvodi i kakav digitalni otisak ostavlja. Svaka pretraga na tražilici, svaka aktivnost na društvenim mrežama, svaka interakcija na mobilnim uređajima može se pohraniti i analizirati. Sveprisutne društvene mreže sadrže fascinantnu količinu najšireg spektra korisničkih podataka [Youyou i sur., 2015; Kosinski i sur., 2013]. Dok je svaki pojedinačni podatak preslabo uporište za oblikovanje pouzdanog predviđanja, s desecima, stotinama i tisućama podataka o pojedincu rezultati predviđanja postaju značajno pouzdaniji. Postoji veći broj recentnih istraživanja koja su ukazala kako se uz razmjerno lako dostupne podatke korisničkog ponašanja na društvenoj mreži (poput iskazivanja „sviđanja“ na Facebooku) može automatizirano i precizno predvidjeti psihološki profil pojedinca i druge atribute. Primjerice, na bazi određenog broja Facebook Likeova, autori su prilično precizno mogli predvidjeti dob i spol, spolnu orijentaciju, etičku pripadnost, religijske i političke stavove, značajke osobnosti, inteligenciju, sreću, uporabu ilegalnih supstanci, bračni status i drugo [Sokolovska i Kocarev, 2018; Youyou i sur., 2015; Kosinski i sur., 2013].

Dodatni veliki izazov šireg područja privatnosti leži u činjenici da je osobna privatnost pod snažim utjecajem konteksta [Watson & Rodrigues, 2017], a korisnička očekivanja o privatnosti i osjetljivost osobnih informacija su snažno obilježene kulturološkim specifičnostima. Također, stupanj privatnosti i povezane regulative zaštite osobnih podataka se značajno razlikuje među

različitim zemljama odnosno pravnim okvirima u kojima funkcioniraju. Lucente i Clark [2017] uočene raznolikosti među zemljama i njihovim pravim okvirima opisuju segmentacijom na 3 skupine: zemlje sa snažnim stavom i implementacijom regulative, zemlje sa umjerenim i zemlje s slabim stavom. Sve navedeno potvrđuje veliku heterogenost na više razina i jasnu potrebu za sustavnim rješenjem ovih izazova.

S približavanjem dana implementacije nove Opće uredbe o zaštiti podataka (General Data Protection Regulation (EU) 2016/679), stvoren je iznimno velik interes svih dionika koji izravno ili neizravno sudjeluju u provođenju nove regulative; poslovni subjekti usavršavali su svoje pristupe uporabe korisničkih podataka, pojedini subjekti specijalizirali su se za implementaciju nove regulative u drugim subjektima, a sami korisnici bili su izloženi strahovito velikom frekvencijom upita za davanje privole u okviru internetskog web-prostora te putem e-pošte [Garber, 2018; Vale, 2018]. Gotovo da nije bilo interakcije u digitalnom informacijskom prostoru koja od korisnika nije zahtijevala neki oblik potvrde privole, davanju suglasnosti ili drugog oblika iskazivanja potvrde za pristupu podacima [Haug, 2018; Starčević i sur., 2018]. Velik medijski interes koji je pratio uvođenje nove regulative potvrdio je značaj primjena koje Uredba treba donijeti.

2 OPĆA UREDBA O ZAŠTITI PODATAKA

Nova Opća uredba o zaštiti podataka (Uredba, GDPR) stupila je na snagu 25. svibnja 2018. godine. Uredba ažurira dotada važeću Direktivu o zaštiti podataka (Data Protection Directive, 95/46/EC) s ciljem ojačavanja građanskih temeljnih prava s posebnim naglaskom na pravo na privatnost i zaštitu osobnih podataka u okviru digitalnog informacijskog društva. Istovremeno, Uredba omogućava slobodno kolanje podatka u okviru jedinstvenog digitalnog tržišta pojednostavljivanjem pravila za poslovne subjekte [Macenaite, 2017].

Regulativa uspostavlja opća principe zaštite podataka i pravni okvir za obradu [procesuiranje] podataka te nameće različite obveze subjektima koji obrađuju ili odlučuju o obradi osobnih podataka (tzv. *data controllers*). S druge strane, Uredba pruža pojedincima o kojima su podaci obrađivani (tzv. *data subjects*) određena prava, poput prava pristupa osobnim podacima, prava na ispravke podataka i brisanje [Poullet, 2018; Macenaite, 2017]. Čizmić i Boban [2018] sugeriraju kako nova Uredba redefinira osobne podatke i zamjenjuje nedosljedne nacionalne zakone s ciljem povećanja razine zaštite osobnih podataka kao i povećanja pravne sigurnosti digitalnog okruženja.

Prvotna Direktiva o zaštiti podataka (95/49/EC) bila je snazi dvadeset godina te je određivala minimalni standard zakona o zaštiti podataka u članicama Europske Unije. Obzirom na korjenite promjene koja je donijela opća digitalizacija društva i društvenih procesa, mnoge su članice EU i druge zemlje samostalno ulagale napore i značajnije zakonski određivale mjere za zaštitu osobnih podataka odnosno podataka pomoću kojih je moguće identificirati pojedinca. Navedena heterogenost je značajno otežala stanovnicima EU shvaćanje kako se njihova prava štite, a organizacijama određivanje kojih zakona se trebaju pridržavati, posebice ukoliko posluju u više zemalja članica [IT Governance, 2017]. Istovremeno smanjivanje harmonizacije između članica te značajno povećavanje kolanja podataka dodatno je stvaralo kaotičnu situaciju te je postojala jasna želja rješavanja ovog pravnog i informacijskog izazova [Boban, 2016].

Slijedom navedenog, EU komisija je donijela odluku kako će jedan unificirani set zakona ili pravila na učinkovitiji način omogućiti ostvarivanje dva cilja [IT Governance, 2017]:

- Zaštita prava, privatnosti i sloboda fizičkih osoba u EU i
- Smanjiti ograničenja poslovnih subjektima kroz omogućavanje slobodnog prometa podataka diljem EU.

Temeljna načela privatnosti osobnih podataka još uvijek vrijede iz Direktive, ali su brojna područja doživjela značajne promjene. Usvajanje Opće uredbe o zaštiti podataka označava prekretnicu u pristupu zaštiti osobnih podataka i korak je prema stvaranju jedinstvenog digitalnog tržišta u EU [Boban, 2016]. Opća uredba o zaštiti podataka označava ujednačavanje pravnog statusa zaštite osobnih podataka u okviru jedinstvenog digitalnog tržišta te daje prvi pravni referentni okvir implementacije „istinske kulture privatnosti" [Martinez-Martinez, 2017]. Da Veiga i Martins [2015] definiraju kulturu privatnosti informacija kao „kulturu u kojoj su zaštita informacija i poštivanje privatnosti način na koji se stvari čine unutar organizacije. To je kultura u kojoj zaposlenici pokazuju stavove, pretpostavke, uvjerenja, vrijednosti i znanje koje pridonosi zaštiti i privatnosti informacija prilikom procesuiranja u bilo kojem trenutku životnog ciklusa informacije, rezultirajući s etičkim i podržavajućim ponašanjem." Uredba donosi značajne promjene u pravilima koja definiraju osobne podatke te uvodi nove termine: usklađenost, planiranje, implementacija, održavanje usklađenosti te procjena učinka [Čizmić i Boban, 2018]. Lachaud [2018] sugerira kako je nova regulativa pretvorila certifikaciju u novi regulatorni instrument zaštite podataka te ju naziva nadziranom samo-regulacijom koja treba premostiti jaz između samo-regulacije i tradicionalne regulacije s ciljem stvaranja „regulacijskog kontinuuma".

2.1 OSOBNI PODACI

Jedan od glavnih ciljeva kojeg Opća uredba o zaštiti podataka treba ispuniti je zaštita osobnih podataka bez obzira je li riječ o osobnim podacima korisnika, klijenata, zaposlenika ili drugih subjekata [GDPR2018, 2018a]. Subjekt koji prikuplja osobne podatke i prije samog prikupljanja ima obvezu pružanja informacija u koju svrhu se podaci prikupljaju, na temelju koje pravne osnove, komu se podaci otkrivaju te o pravu pojedinca da svojim podacima pristupi, da zahtijeva njihovu korekciju ili brisanje [Agencija za zaštitu osobnih podataka, 2018]. Prikupljeni podaci se mogu koristiti samo u svrhu za koju je dan pristanak i potrebno je omogućiti davanje pojedinačne privole za različite postupke obrade podataka [GDPR2018, 2018b].

Koncept osobnog podatka ima razmjerno široko područje tumačenja, a vezan je uz pojedinca čiji se identitet može utvrditi ili je utvrđen. Agencija za zaštitu osobnih podataka [2018] navodi kako je pojedinac čiji se identitet može utvrditi "osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca".

Osobni podatak može biti [Agencija za zaštitu osobnih podataka, 2018; GDPR2018, 2018a]: ime i prezime, identifikacijski broj, slika, glas, adresa, broj telefona, e-pošta, IP adresa, MAC adresa, video snimka pojedinca, biometrijski podaci (otisak prsta, snimka šarenice oka), genetski podaci, podaci o obrazovanju i stručnoj spremi, podaci o plaći, podaci o kreditnom

zaduženju, podaci o računima u banci, povijest bolesti, popis najdraže literature ili pjesama ako takvi podaci mogu dovesti do izravnog ili neizravnog identificiranja pojedinca i dr. Uredba određuje opća pravila primjenjiva za bilo koji oblik procesuiranja osobnih podataka, ali i specifična pravila za posebne kategorije osobnih podataka poput zdravstvenih podataka koji se prikupljaju za potrebe znanstvenog istraživanja [Limb, 2018; Chassang, 2017].

2.2 ZNAČAJ ZA POSLOVNE SUBJEKTE

Usprkos činjenici što je Uredba predviđena i kako bi koristila poslovnim subjektima pružajući konzistentnost pri aktivnostima zaštite podataka i odgovornosti diljem članica EU te povećanje integriranosti politika zaštite podataka, ipak donosi brojne složene izazove za ove dionike. Poslovni subjekti nisu nužno u potpunosti (ili uopće) spremni za promjene koje su se odigrale stupanjem nove regulative na snagu ili čak nisu svjesni mjera koje Odredba nužno nameće [Tikkinen-Piri i sur., 2017]. Implementacija odredbi Uredbe može zahtijevati značajne ljudske i financijske resurse te edukaciju zaposlenika što posljedično znači da poslovni subjekti trebaju pomoć u tranzicijskom procesu. Ipak, valja naglasiti da je formalno gledano taj prijelazni rok prošao sa stupanjem Odredbe na snagu u svibnju 2018.

Primjena Uredbe odnosi se na voditelje i izvršitelje obrade osobnih podataka u Europskoj uniji, bez obzira odvija li se unutar teritorija članice ili ne. Uredba se primjenjuje i na obradu osobnih podataka pojedinaca koji se nalaze u Europskoj uniji od strane voditelja i izvršitelja podataka koji se ne nalaze u EU [Bhaimia, 2018; GDPR2018, 2018b]. Dakle, iako je riječ o Uredbi na razini EU, svi poslovni subjekti koje obrađuju podatke građana EU također podliježu ovoj regulativi. Također, Uredba je utjecala na preustroj zaštite podataka mnogih giganata elektroničkih poslovnih modela poput Facebooka, Googlea, Microsofta i drugih [GDPR2018, 2018a].

Stupanjem Uredbe na snagu, mnogi poslovni subjekti dobili su obvezu imenovanja službenika za zaštitu osobnih podataka (Data Protection Officer, DPO). Službenik mora biti imenovan na temelju profesionalnih kvalifikacija, a osobito stručnih znanja o pravu i praksama u području zaštite podataka te sposobnosti za izvršavanje zadaća koje ima temeljem Uredbe [Agencija za zaštitu osobnih podataka, 2018c; Bhaimia, 2018]. Službenici za zaštitu osobnih podataka moraju biti imenovani u slučajevima [Agencija za zaštitu osobnih podataka, 2018b; GDPR2018, 2018b]:

- Obradu provodi tijelo javne vlasti ili javno tijelo;
- Organizacije koje se u velikoj mjeri bave sustavnim praćenjem velikih razmjera;
- Organizacije koje se bave opsežnom obradom osjetljivih osobnih podataka u širokom razmjeru i osobnih podataka o kaznenim predmetima;
- Država članica EU svojim pravnim aktima ili pravo Unije nalaže obvezu imenovanja službenika za zaštitu osobnih podataka.

Kazne za organizacije koje prekrše odredbe Opće uredbe o zaštiti podataka su uistinu drakonske: mogu iznositi do 4% godišnjeg prometa na svjetskoj razini ili 20 milijuna eura, ovisno koji je iznos veći [Agencija za zaštitu osobnih podataka, 2018; Doe, 2018]. Ovakva značajne kazne određene su za najozbiljnija kršenja nove regulative vezana uz načela obrade, prava ispitanika, prijenosi u treće države, obveze u skladu s nacionalnim pravom, nepoštovanja naredbe ili pravo pristupa nadzornog tijela.

2.3 IZAZOVI PRIMJENE UREDBE

Nekoliko autora adresiralo je i najznačajnije izazove u širem području istraživačkih aktivnosti koji su nastali primjenom Opće uredbe o zaštiti podataka. Rumbold [2017] drži da će usvajanje i primjena Uredbe utjecati na znanost o podacima (tzv. *data science*) u Europi. Poseban stupanj zabrinutosti iskazan je prema zahtjevima za suglasnost koji će značajno ograničiti medicinska istraživanja odnosno prikupljanje medicinskih podataka [Morrison i sur., 2017; Rumbold, 2017].

Kindt [2017] sugerira kako je rast uporabe biometrijskih podataka u različitim digitalnim korisničkim uređajima, ali i vladinim nadzornim sustavima izgledno nepovratan. Nova Uredba ne daje jasna pravila i potrebnu zaštitu poštivanja temeljnih prava i sloboda stvaranjem umjetne razlike između različitih kategorija biometrijskih podataka. Kategorizacija zanemaruje ljudska prava i služi interesima velikih (vladinih) baza podataka.

Odredbe Uredbe nenamjerno, ali ozbiljno narušavaju ravnotežu između privatnosti i informacijskih prava, favorizirajući prava privatnosti i pojedince koji ih nameću [Keller, 2017]. Ovo je postignuto kroz naizgled neškodljiva proceduralna pravila za subjekte koji obrađuju podatke, a kad se ista primjene na internetske pružatelje usluga postaje vidljivo da su sustavno skloni brisanju podataka.

Wachter [2018] pojašnjava da se standardi Opće uredbe o zaštiti podataka hitno zahtijevaju daljnje preciziranje i implementaciju u oblikovanju internetskih i digitalnih tehnologija s ciljem minimiziranja utjecaja privatnosti na sukob između načela zaštite podataka i sustava identifikacije u okviru digitalnih tehnologija.

Uz navedena prava koje Uredba štiti, posebnu pažnju imaju i djeca kao vrlo specifična ciljna skupina. Uredba ima za cilj prilagoditi prava djece na privatnosti u digitalnom okruženju. Uredba izričito prepoznaje da djeca zaslužuju posebnu zaštitu svojih osobnih podataka te uvodi dodatna prava i zaštitne mjere za djecu [Macenaite, 2017]. Obzirom da Uredba favorizira zaštitu nad osnaživanjem djece, ista riskira ograničavanje djece u njihovim internetskim mogućnostima i, oslanjajući se na kriterij prosječnog djeteta, ne razmatra razvijanje sposobnosti i najbolje interese djeteta.

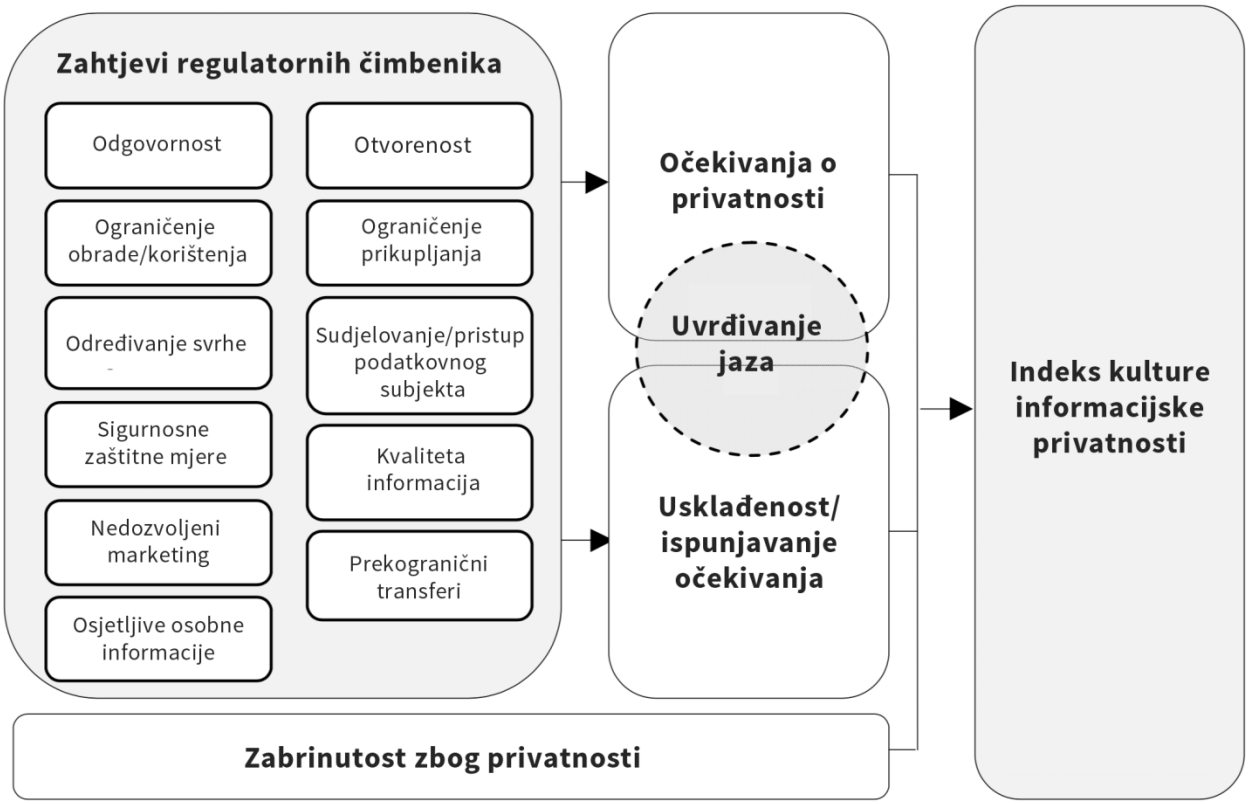
3 ANALIZA AKTUALNIH ISTRAŽIVAČKIH NAPORA

Opća uredba o zaštiti podatka održava ravnotežu između nužnosti učinkovite zaštite prava pojedinaca u digitalnom okruženju, omogućujući obradu osjetljivih osobnih podataka u okviru znanstvenih istraživanja [Chassang, 2017]. Kao značajna novost, Uredba adresira i poštivanje etičkih standarda kao dio zakonitosti istraživačkog procesa, što je velik iskorak za uvažavanje specifičnosti istraživačkog područja i istraživačke konzistentnosti.

U nastavku je dan pregled recentnih znanstvenih istraživanja vezanih uz utjecaj Uredbe na različitim poljima, od istraživačkog procesa, izazove privatnosti, politike poslovnih subjekata te implikacija na krajnje korisnike. Teme značaja nove regulative i povezane implementacije istraživački su analizirani u više znanstvenih područja: od društvenih, tehničkih, humanističkih te biomedicinskih znanosti [Sokolovska i Kocarev, 2018; Limb, 2018; Chassang, 2017; Da Veiga, 2017; Pagallo, 2013].

Od dostupnih analiziranih radova, a uzevši u obzir recentnost teme i očigledan manjak povezanih istraživanja, samo se u nekoliko radova govori o oblikovanom konceptu mjerenja informacijske privatnosti. Da Veiga [2018] predlaže okvir indeksa kulture informacijske privatnosti (*information privacy culture index framework*, IPCIF) s validiranim instrumentom - indeksom kulture informacijske privatnosti (*information privacy culture index instrument,* IPCII). Indeks se koristi za mjerenje kulture informacijske privatnosti institucije, organizacije ili zemlje te identificira što je potrebno usavršiti za premošćivanje jaza između korisničkog očekivanja o privatnosti i usklađenosti odnosno ispunjavanja tog očekivanja. Koncept se bazira na korisničkim očekivanjima vezanom uz privatnost, njihovim stvarnim iskustvima prilikom obrađivanja osobnih podataka od strane organizacija, kao i njihovim općenitim stavovima o privatnosti (Slika 1).

Slika 1. Okvir indeksa kulture informacijske privatnosti



Izvor: prilagođeno prema Da Veiga [2018:343]

Validirani indeks kulture informacijske privatnosti (IPCI) sastoji se od 4 elementa koji se mogu koristiti u različitim zemljama za određivanje potrošačkih očekivanja o privatnosti i razine povjerenja [Da Veiga, 2018]:

- Element A – Očekivanja o zaštiti informacija [10 čestica];
- Element B – Očekivanja o uporabi informacija [8 čestica];
- Element C – Očekivanja o prikupljanju informacija [4 čestice];
- Element D – Povjerenje u ispunjavanje očekivanja o privatnosti i zahtjevi usklađenosti [24 čestice].

Prvo istraživanje koristeći ovaj instrument provedeno je u Južnoj Africi. Testirani indeks kulture informacijske privatnosti pokazao je kako postoji jaz između onoga što potrošači očekuju u smislu privatnosti i načina na koji organizacije ispunjavaju [odnosno neispunjavanju] ta očekivanja što rezultira gubitkom povjerenja i narušavanjem društvenih odnosa. IPCII je ukazao da Južnoafrikanci imaju velika očekivanja o privatnosti te da iskazuju zabrinutost o dijeljenju osobnih, financijskih i zdravstvenih podataka, posebice u digitalnom okruženju [Da Veiga [2018].

Uvažavajući činjenicu da su različite zemlje različito formalno, zakonski i kulturološki nastrojene prema pitanju privatnosti osobnih podataka, Custers i sur. [2018] su u okviru istraživačkog projekta komparirali zaštitu i privatnost osobnih podataka u 8 zemalja članica EU: u Francuskoj, Njemačkoj, Ujedinjenom Kraljevstvu, Irskoj, Rumunjskoj, Italiji, Švedskoj i Nizozemskoj. Istraživači su uspoređivali pet glavnih cjelina: svijest i povjerenje, vladine politike za zaštitu osobnih podataka, primjenjivi zakoni i regulativa, implementacija zakona i regulative te nadzor i provođenje. Usporedba stanja privatnosti i zaštite podataka diljem EU ukazuje na specifične razlike otkrivajući koje su zemlje predvodnici, a koje zemlje zaostaju u testiranim elementima. Na bazi kompariranih osam zemalja članica EU, Njemačka se u većini aspekata pokazala predvodnikom, dok su Italija i Rumunjska na drugom kraju poretka [Custers i sur., 2018].

Tikkinen-Piri i sur. [2017] oblikovali su analitički rad s ciljem identifikacije i diskusije o promjenama koje uvodi Uredba, a koje će imati praktični značaj za poslovne subjekte odnosno utjecati na upravljanje podacima i njihovu uporabu. Rezultat rada je razvijeni okvir s glavnih 12 cjelina utjecaja i povezane smjernice o načinu pripremanja za prilagodbu na novu regulativu [Tikkinen-Piri i sur., 2017]:

1. Preciziranje potrebe za podacima i njihove uporabe;
2. Uvjeti obrade podataka u međunarodnom kontekstu;
3. Izgrađivanje privatnosti kroz zaštitu podataka pri oblikovanju i zadanim postavkama;
4. Demonstriranje pridržavanja odredbi Uredbe;
5. Razvijanje procesa za rješavanje kršenja podatkovnih prava;
6. Procjena sankcija zbog neusklađenosti;
7. Određivanje službenika za zaštitu osobnih podataka;
8. Pružanje informacija pojedincima o kojima su podaci obrađivani;
9. Dobivanje suglasnosti za uporabu osobnih podataka;
10. Osiguravanje prava biti zaboravljenim [prava na brisanje];
11. Osiguravanje prava na prenosivost podataka;
12. Održavanje dokumentacije.

Navedene cjeline opisuju poslovne strategije i praktične pristupe, ali i organizacijske i tehničke mjere. Na bazi razvijenog okvira, poslovni subjekti mogu planirati mjere usavršavanja zaštite osobnih podataka te implementaciju potrebnih politika, procedura i procesa. Uz navedeno, okvir donosi i smjernice za iskorištavanje primjene novih pravila u oblikovanju poslovnih procesa.

Bailey [2018] je u istraživačkom radu prije implementacije Uredbe dao ažurirani pregled opsega upravljanja zaštitom podataka u području britanskog knjižničarstva i informacijskih usluga. Rezultati istraživanja ukazuju kako je većina ispitanika bila svjesna postojeće regulative, znala je za nadolazeće promjene regulative te ključne elemente promjena.

Istraživanje implicira kako je povećana svijest o zaštiti podataka među knjižničnim osobljem; knjižničari su pokazali svijest o manjkavom znanju te izrazili entuzijazam za dodatno usavršavanje.

Zanimljivo recentno istraživanje donosi analizu zatečenog stanja i načina na koji se obrađuju i koriste svi prikupljeni osobni podaci svih sudionika u sustavu velikog poslovnog subjekta [grupe subjekata] iz Hrvatske [Starčević i sur., 2018]. U radu su opisuje usuglašeni projekt strukturiranog i metodološki ispravnog postupka prilagodbe, s ciljem najvišeg mogućeg stupnja uređenja obveza poslovnog subjekta s pravnom regulativom Uredbe. Prilikom definiranja projektnog pristupa, određeni su ciljevi koje se trebaju postići tijekom pojedinačnih faza prilagodbe [Starčević i sur., 2018]:

- Snimanje/mapiranje osobnih podatka i baza podataka;
- Identificiranje i definiranje pravne osnove za prikupljanje i obrađivanje podataka;
- Razvijanje organizacijskih pravila na razini grupe kao krovnog rješenja koji se može primijeniti u svim članicama grupe;
- Priprema preduvjeta za procjenu rizika i njegova implementacija;
- Definiranje organizacijskih i tehničkih mjera za osiguravanje adekvatnih mjera zaštite osobnih podataka;
- Određivanje službenika za zaštitu osobnih podataka;
- Određivanje odgovornih osoba za zaštitu osobnih podataka za svaki proces;
- Razvijanje kulture zaštite podataka na svim razinama;
- Edukacija djelatnika.

Papageorgiou i sur. [2018] dali su dubinsku analizu sigurnosti i privatnosti nekih od najpopularnijih besplatnih zdravstvenih aplikacija za mobilne uređaje. Mobilnim zdravstvenim aplikacijama značajno raste popularnost te su već raširene među korisnicima mobilnih uređaja. Iako su ih korisnici srdačno prigrlili, ove aplikacije aktualiziraju pitanje privatnosti zbog upravljanja osobnim informacijama. Smisao zdravstvenih aplikacija i jest upravljanje zdravstvenim podacima o korisnicima koji se tretiraju iznimno osjetljivima i koje su snažno zaštićene nacionalnim i međunarodnim propisima kao što je Opća uredba o zaštiti podataka. Na bazi provedene analize, Papageorgiou i sur. [2018] zaključili su da većina analiziranih aplikacija ne slijedi uobičajene postupke i smjernice, čak ni zakonska ograničenja nametnuta suvremenim propisima o zaštiti podataka, čime ugrožavaju privatnost milijuna korisnika.

Slične zaključke izveli su Stalla-Bourdillon i sur. [2018] prilikom interdisciplinarne analize implementacije Uredbe u kontekstu sustava elektroničke identifikacije. Analiza je obuhvaćala Gov.UK Verify, sustav britanske vlade za elektroničku identifikaciju te kompatibilnost sustava sa značajnim odredbama nove Uredbe. Istraživanje je pokazalo kako analizirani sustav nije u skladu sa nekoliko značajnih odredbi okvira Opće uredbe o zaštiti podataka.

4 SMJERNICE ZA BUDUĆA ISTRAŽIVANJA

Rad se bavi s nekoliko istraživačkih izazova i predlaže smjernice za buduće istraživačke pristupe pri utjecaju Uredbe na različite ciljne skupine. Poseban fokus umjeren je na dvije skupine koje su pod snažnim utjecajem Uredbe: poslovni subjekti različitih djelatnosti koje

koriste osobne podatke te krajnji korisnici različitih platformi informacijsko-komunikacijskih tehnologija.

S ciljem razumijevanja kako se poslovni subjekti prilagođavaju zakonskim promjenama, implementiranju novih zahtijeva i rješavanju povezanih izazova, buduća sveobuhvatna empirijska istraživanja su prijeko potrebna na poslovnim subjektima koji značajno koriste osobne podatke u svojim poslovnim procesima. Također, od neobično velikog značaja je istraživanje provedbe Opće uredbe o zaštiti podataka u poslovnim subjektima različitih veličina te uočavanje razlika u provedbi i rješavanju izazova u drugačijim poslovnim okruženjima [Tikkinen-Piri i sur., 2017]. Kroz empirijska istraživanja ove vrste, mogu se pratiti i analizirati sredstva za provedbu promjena i odgovarajuća praktična rješenja, zajedno s načinima uporabe podataka specifičnih djelatnosti i upravljačkim politikama analiziranih subjekata. Uz navedeno, budući istraživački napori ne bi trebali samo odrediti razinu do koje se promišlja o privatnosti već i dodatno omogućiti fokusiranje na najbolja rješenja iz prakse u shvaćanju, upravljanju i reagiranjuna rastuće izazove vezane uz privatnost i osobne podatke [Watson & Rodrigues, 2017].

Buduća istraživanja poslovnih subjekata kao značajnog dionika implementacije nove Uredbe mogu se fokusirati na sljedeće sastavnice:

- Status uporabe osobnih podataka;
- Zaštita privatnosti osobnih podataka prije stupanja Uredbe na snagu;
- Procjena informiranosti o odredbama Uredbe prije implementacije;
- Način implementacije Uredbe unutar subjekta;
- Tijek procesa prilagodbe;
- Ulaganja resursa tijekom procesa prilagodbe;
- Aktualni status implementacije Uredbe;
- Uloga službenika za zaštitu osobnih podataka;
- Status edukacije djelatnika;
- Aktualni izazovi.

Ciljna skupina od najvećeg značenja su pojedinci o kojima se prikupljaju osobni podaci. Zato je neobično važno istražiti stanje, stavove i percepciju ove skupine prema uvođenju Uredbe i promjenama koje je donijela. Jedan od istraživačkih pristupa je primjena okvira indeksa kulture informacijske privatnosti [De Veiga, 2018] kojim se mjeri razina informacijske privatnosti na razini zemlje [a što može biti jedan od prvih koraka daljnjih istraživačkih napora autora], ali i na razini pojedine institucije ili subjekta. Uz navedeni model, buduća istraživanja krajnjih korisnika odnosno pojedinaca mogu uključivati:

- Procjenu informiranosti o Uredbi prije uvođenja;
- Procjenu informiranosti o Uredbi nakon uvođenja;
- Razumijevanje osobnih prava i obveza koje Uredba osigurava odnosno nameće;
- Aktivnosti davanja privola neposredno prije uvođenja Uredbe;
- Aktivnosti davanja privola nakon uvođenja Uredbe;
- Aktualni izazovi.

Uz očekivani daljnji tehnološki razvoj, procjena utjecaja koje aktivnosti obrade osobnih podataka mogu imati na prava i slobode pojedinaca zahtijeva neprestano razmatranje i

preispitivanje, posebice zbog činjenice što se neki još potencijalno ne mogu percipirati ili procijeniti [Gumzej, 2017]. Recentnost regulative, značaj promjena koje donosi i turbulentne promjene digitalnog okruženja dodatno potenciraju kontinuiranu analizu aktualnog stanja. Na tragu prethodnog, otvorena pitanja zahtijevaju daljnja pojašnjenja u specifičnim područjima te je za očekivati da će budućnost donijeti nove izazove, ali i rješenja novih izazova.

5 ZAKLJUČAK

Stara europska Direktiva o zaštiti podataka (Directive 95/46/EC) je 25. svibnja 2018. zamijenjena s novom Općom uredbom o zaštiti podataka. Uredba je jedna od recentnijih inicijativa u kontinuiranom globalnom prepoznavanju značaja osobnih informacija i privatnosti. Uvažavajući činjenicu da je nova regulativa tek razmjeno nedavno primijenjena, pravi učinci na sve dionike će tek naknadno biti vidljivi. Opća uredba pruža osjetljivu ravnotežu između nužne učinkovite zaštite prava podataka subjekta u digitaliziranom svijetu uz istovremeno omogućavanje obrade osobnih podataka za heterogene poslovno orijentirane potrebe. Uvažavajući činjenicu da je tema iznimno značajna zbog uporabe osobnih podataka i privatnosti, cilj rada je pružiti preliminarnu analizu istraživanja i oblikovati temelj za buduće robusnije istraživačke napore.

Usprkos obećavajućoj zaštiti pojedinaca i njihovih prava privatnosti koja su fokus Opće uredbe o zaštiti podataka pri EU, u stvarnosti će samo njihova pravilna i učinkovita provedba pokazati u kojoj mjeri je nova regulativa plodonosna za ciljeve za koje je oblikovana. Paralelno s zaštitom privatnosti pojedinaca i njihovih osobnih podataka, učinkovitost Uredbe bit će oslikana kroz objektivno mjerenu prilagodbu subjekata koji osobne podatke prikupljanju i obrađuju. Kako bi se dugoročno ostvarila uspješna implementacija novih pravila, potrebno je pravovremeno adresirati brojne složene regulativne i praktične izazove u kojima najviše sudjeluju kreatori politika pri EU, nacionalni autoriteti za zaštitu podatka u članicama EU, ali i izvan nje te poslovni subjekti internetski pružatelji usluga i povezane institucije.

Na bazi analiziranih radova, može se zaključiti kako je jedan od najboljih pristupa uspješnog rješavanja izazova koje nameće pitanje privatnosti primjena koncepta implementacije privatnosti u fazama oblikovanja [dizajniranja] sustava koji će koristiti privatne podatke. Takav sustav treba uzeti u obzir različite oblike i razine privatnosti, uvažiti kompromise između privatnosti i korisnosti, uvažiti različite implikacije pravednosti, privatnosti i učinkovitost mehanizama koji osiguravaju zaštitu privatnosti.

Obzirom na složenost održavanja ravnoteže između zaštite privatnosti i osobnih podataka te slobodnog kolanja podataka u digitalnom okruženju, umjesto očekivanja da problema nema i da će privatnost biti savršeno zaštićena, ispavan put napretka jest transparentnost i iskrenost prema rizicima i izazovima privatnosti koji nas okružuju. Dodatna istraživanja različitih aspekata privatnosti i učinkovitosti uvođenja te primjene Opće uredbe za zaštitu podataka su od neobično velikog značaja.

LITERATURA

[1] Agencija za zaštitu osobnih podataka (2018) Vodič kroz opću uredbu o zaštiti podataka, https://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka. [07.09.2018.]

[2] Agencija za zaštitu osobnih podataka (2018b) Imenovanje službenika za zaštitu osobnih podataka, https://azop.hr/zbirke-osobnih-podataka/detaljnije/registar-sluzbenika-za-zastitu-osobnih-podataka. [08.09.2018.]

[3] Agencija za zaštitu osobnih podataka (2018c) Važne napomene za voditelje i izvršitelje obrade, https://azop.hr/aktualno/detaljnije/obavijest-za-voditelje-i-izvrsitelje-obrade-ukidanje-sredisnjeg-registra. [08.09.2018.]

[4] Bailey, J. (2018). Data Protection in UK Library and Information Services: Are We Ready for GDPR?. *Legal Information Management*, 18(1), 28-34.

[5] Bhaimia, S. (2018). The General Data Protection Regulation: the Next Generation of EU Data Protection. *Legal Information Management*, 18(1), 21-28.

[6] Boban, M. (2016). Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world. *Economic and social development: book of proceedings*, 191.

[7] Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *ecancermedicalscience*, 11.

[8] Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, 34(2), 234-243.

[9] Čizmić, J., & Boban, M. (2018). Učinak nove EU uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj. *Zbornik Pravnog Fakulteta Sveučilišta u Rijeci*, 39(1).

[10] Da Veiga, A. (2017). An Information Privacy Culture Index Framework and Instrument to Measure Privacy Perceptions across Nations: Results of an Empirical Study. In Furnell, S. and Clarke N. (eds.), Proceedings of the *Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, Australia, Adelaide, pp. 196-205, ISBN: 978-1-84102-428-8.

[11] Da Veiga, A. (2018). An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information & Computer Security*, 26(3), 338-364, https://doi.org/10.1108/ICS-03-2018-0036

[12] Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), 243-256.

[13] Doe, S. (2018). Practical Privacy: Report from the GDPR World. *Legal Information Management*, 18(2), 76-79.

[14] Garber, J. (2018). GDPR–compliance nightmare or business opportunity?. *Computer Fraud & Security*, 2018(6), 14-15.

[15] GDPR2018 (2018a). Što donosi GDPR? https://gdpr2018.eu/sto-donosi-gdpr/. [03.09.2018.]

[16] GDPR2018 (2018b). Ključne promjene i kazne, https://gdpr2018.eu/sto-donosi-gdpr/kljucne-promjene-i-kazne/. [03.09.2018.]

[17] Gumzej, N. (2017). Law and technology in data processing: Risk-based approach in EU data protection law and implementation challenges in Croatia. In *Information and*

Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on (pp. 1424-1430). IEEE.

[18] Haug, C. J. (2018). Turning the Tables—The New European General Data Protection Regulation. *New England Journal of Medicine*.

[19] IT Governance (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*, 2nd ed. Cambridgeshire: IT Governance Publishing.

[20] Keller, D. (2017). The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation.

[21] Kindt, E. J. (2017). Having yes, using no? About the new legal regime for biometric data. *Computer Law & Security Review*, 34(3), 523-538.

[22] Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 201218772.

[23] Lachaud, E. (2018). The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law & Security Review*, 34(2), 244-256.

[24] Limb, M. (2018). How data protection changes will affect your practice. *BMJ: British Medical Journal (Online)*, 361.

[25] Lucente, K., Clark, J. (2017) Data protetction laws of the world: Full handbook. DLA Piper, https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all. [03.09.2018.]

[26] Martínez-Martínez, D. F. (2018). Unification of personal data protection in the European Union: Challenges and implications. *El profesional de la información* (EPI), 27(1), 185-194.

[27] Morrison, M., Bell, J., George, C., Harmon, S., Munsie, M., & Kaye, J. (2017). The European General Data Protection Regulation: challenges and considerations for iPSC researchers and biobanks. *Regenerative medicine*, 12(6), 693-703.

[28] Pagallo, U. (2013). Online security and the protection of civil rights: A legal overview. *Philosophy & Technology*, 26(4), 381-395.

[29] Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, 6, 9390-9403.

[30] Post, R. C. (2017). Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere. *Duke LJ*, 67, 981.

[31] Poullet, Y. (2018). Is the general data protection regulation the solution?. *Computer Law & Security Review*, 34(4), 773-778.

[32] Rumbold, J. M. M., & Pierscionek, B. (2017). The effect of the general data protection regulation on medical research. *Journal of medical Internet research*, 19(2).

[33] Sokolovska, A., & Kocarev, L. (2018). Integrating Technical and Legal Concepts of Privacy. *IEEE Access*.

[34] Stalla-Bourdillon, S., Pearce, H., & Tsakalakis, N. (2018). The GDPR, A game changer for electronic identification schemes? The case study of Gov. UK Verify.

[35] Starčević, K., Crnković, B., & Glavaš, J. (2018). Implementation of the General Data Protection Regulation in companies in the Republic of Croatia. *Ekonomski*

vjesnik/Econviews-Review of Contemporary Business, Entrepreneurship and Economic Issues, 31(1), 163-176.

[36] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153.

[37] Uredba (EU) 2016/679 Europskog parlementa i vijeća, https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR. [03.09.2018.]

[38] Vale, A. (2018). A race for maintaining personal data-how to manage consumers´ data under the right to be forgotten and the right to data portability of the new EU GDPR (Doctoral dissertation).

[39] Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, 34(3), 436-449.

[40] Watson, H., & Rodrigues, R. (2018). Bringing privacy into the fold: Considerations for the use of social media in crisis management. *Journal of Contingencies and Crisis Management*, 26(1), 89-98.

[41] Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, *112*(4), 1036-1040.