Preliminary communication / Prethodno priopćenje

ZAŠTITA PODATAKA NA VISOKIM UČILIŠTIMA U REPUBLICI HRVATSKOJ: PRELIMINARNO ISTRAŽIVANJE

DATA PROTECTION AT HIGHER EDUCATION INSTITUTIONS IN THE REPUBLIC OF CROATIA: PRELIMINARY RESEARCH

ALEN PODBOJEC
Fakultet organizacije i informatike Sveučilište u Zagrebu
Pavlinska 2, 42000 Varaždin, Hrvatska
apodbojec@foi.unizg.hr

RENATA MEKOVEC
Fakultet organizacije i informatike Sveučilište u Zagrebu
Pavlinska 2, 42000 Varaždin, Hrvatska
renata.mekovec@foi.unizg.hr

SAŽETAK

Praćenjem i objedinjavanjem podataka o studentima, njihovom ponašanju u različitim informacijskim sustavima i platformama, sveučilišta prikupljaju puno informacija o studentima. Međutim, korištenje osjetljivih i osobnih podataka o studentima mora za sobom povlačiti i povećanje mjera kojima se osigurava privatnosti studenata, ali i svih ostalih dionika u edukacijskom procesu. Prošle su dvije godine od stupanja na snagu novih pravila o privatnosti koja su definirana Općom uredbom o zaštiti podataka. U ovom članku prikazana je analiza usklađenosti visokih učilišta u Republici Hrvatskoj s načelima zaštite podataka.

KLJUČNE RIJEČI: privatnost, osobni podaci, visoka učilišta.

ABSTRACT

By monitoring and aggregating data about students, their behavior in different information systems and platforms, the university collects a lot of information about students. However, the use of sensitive and personal data about students must lead to the increase of measures to ensure the privacy of students, but also of all other stakeholders in the educational process. Two years have passed since the entry into force of the new privacy rules defined by the General Data Protection Regulation. This article presents an analysis of the compliance of higher education institutions in the Republic of Croatia with the principles of data protection.

KEYWORDS: privacy, personal data, higher education institutions.

1. UVOD

Korištenje povezanih uređaja i pametnih tehnologija, kod kuće i na poslu, mijenja očekivanja kupaca. Tempo tehnoloških inovacija se ubrzava i kvaliteta korisničkog iskustva koju poduzeće može pružiti postaje vodeći pokazatelj budućeg uspjeha. Saleforce [2019] ističe kako 67% kupaca očekuje da će poduzeća pružati nove proizvode i usluge češće nego prije, pri čemu 75% kupaca očekuje da će poduzeća upotrijebiti nove tehnologije za poboljšanje njihovih iskustava.

Kako bi pružili povezana i personalizirana iskustva koja kupci očekuju, poduzeća moraju znati puno o individualnim potrebama, očekivanjima i navikama kupaca. Prema anketi kupaca digitalnih proizvoda u Sjevernoj Americi koju je proveo Vision Critical, 80,1% ispitanika reklo je da bi dijeliti osobne podatke izravno s određenim brandom u svrhu personalizacije marketinških poruka. No samo je 16,7% reklo da bi se složili s dijeljenjem ove vrste informacija putem trećih strana [eMarketer, n.d.] .

Uvjerenje da je njihova privatnost zaštićena jedan je od bitnih razloga koji utječe na odluku pojedinaca da kupe/koriste određeni proizvod ili uslugu. Korisnici su sve više svjesni svojih prava vezano uz zaštitu privatnosti pa sukladno tome biraju poduzeća koja prate i osiguravaju visoke standarde zaštite privatnosti [“Data Privacy Trends 2020: What You Need to Know,” 2020]. Prema Cisco istraživanju [2019] 84% ispitanika ističe da brinu za svoju privatnost, svoje podatke te brinu za podatke ostalih članova njihovih zajednica, također ističu kako žele imati više kontrole nad upotrebom njihovih podataka. S druge strane, poduzeća uviđaju kako su posljedice povrede privatnosti ili neusklađenosti s regulativom privatnosti sve rigoroznije te stoga ulažu sve više u educiranje svojih zaposlenika.

Gartner [2020] predviđa da će do 2023. godine 65% svjetske populacije imati zaštićene svoje osobne podatke sukladno nekom zakonu ili regulativi o privatnosti. Međutim, smatra kako će ubuduće proaktivni pristup privatnosti, kao i zaštiti osobnih podatka više pomoći poduzećima da povećaju povjerenje svojih korisnika, nego li pasivne reakcije na promjene u zakonodavstvu.

Otkako je u svibnju 2018. godine stupila na snagu Opća uredba o zaštiti podataka (GDPR), svijet privatnosti podataka pomaknuo je svoj fokus sa smjernica na postupno provođenje. U društvu koje se sve više temelji na obradi podataka GDPR predstavlja instrument kojim se osigurava da pojedinci imaju bolji nadzor nad svojim osobnim podacima. GDPR prepoznaje privatnost kao temeljno ljudsko pravo i zabranjuje organizacijama prikupljanje i obradu osobnih podataka bez zakonskog utemeljenja, u opravdane svrhe na zakonit, pravedan i transparentan način [COM (2020) 264, 2020].

Obrazovne institucije pohranjuju mnoštvo podataka o učenicima/studentima i roditeljima - uključujući stvari poput osobnih podataka, podataka o plaćanju i povijesti bolesti. Napadi na visoko obrazovanje množe se i učestalošću i težinom. Učilišta često objavljuju prednosti koje alati poput glasovnih asistenata, aplikacija za praćenje posjećenosti i sustava prepoznavanja lica mogu ponuditi studentima. No kako se ove tehnologije sve više usvajaju, a prikupljanje podataka postaje institucionalni prioritet, mnogi skreću pozornost na mogućnost zlouporabe i štete za studente. Svaki sustav upravljanja učenjem ili virtualno okruženje za učenje (LMS) upravlja i osobnim podacima o svakom učeniku/studentu [Amo et al. 2020]. Takav sustav obuhvaća podatke kao što su njihovo ime, prezime, adresa e-pošte i druge osobne podatke. LMS također pohranjuje i osjetljive podatke, poput ocjena učenika/studenta, mrežne aktivnosti, te povratne informacije nastavnika. Posljednje, ali ne najmanje važno, LMS zapisuje svaku interakciju učenika/studenta sa LMS-om: svaki put kad se prijavi, svaki klik, svaki dokument,

svaku napisanu riječ, svaki chat. Svi podaci i metapodaci se bilježe.

Visokoškolske ustanove u posljednje vrijeme fokusiraju se na analitiku učenja (LA) obrazovnih podataka gdje se primjenjuju metode rudarenja i analitičke prakse kako bi utjecale na poboljšanje njihovog studiranja i rezultata studiranja. Jones et al. [2020] izvještava o provedenom istraživanju sa studentima preddiplomskih studija u osam visokoškolskih ustanova u SAD-u. Rezultati pokazuju da studenti potencijal vide u LA, ali iznijeli su argumente o tome kada i s kime treba dijeliti podatke; također su izrazili zašto je informirani pristanak vrijedan i potreban. Institucije moraju uravnotežiti svoju želju za provedbom LA-a sa svojom obvezom te educirati studente o njihovim analitičkim praksama i tretirati ih kao partnere u dizajniranju analitičkih strategije oslonjene na podatke kako bi zaštitile njihovu privatnost.

Prema EDUCASE [“Common Challenges | EDUCAUSE” 2020] istraživanje među 16.162 studenta iz 71 američke visokoobrazovne institucije, pokazalo je da se samo 22% složilo ili se čvrsto složilo da razumije kako njihova ustanova koristi njihove osobne podatke, a samo 25% se složilo ili se čvrsto složilo da imaju koristi od prikupljanja podataka od strane njihove ustanove.

Cilj istraživanja prikazanog u ovom radu je istražiti koliko su visoka učilišta u Republici Hrvatskoj prilagodila svoje ophođenje s osobnim podacima svih dionika u edukacijskom procesu od stupanja na snagu Opće uredbe o zaštiti podataka.

2. ZAŠTITA OSOBNIH PODATAKA

Zaštita osobnih podataka kao temeljno ljudsko pravo odnosi se na pravo zaštite podataka svakog pojedinca iz kojih se može doznati ili zaključiti identitet određene osobe. Osobni podaci se danas trebaju štititi više nego prije, poglavito jer se cijelo tržište orijentiralo na Internet poslovanje te podaci postaju sve vrjedniji.

2.1. ZAŠTITA OSOBNIH PODATAKA U HRVATSKOJ

Zaštita osobnih podataka te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj uređuje se Uredbom (EU) 2016/Općom uredbom o zaštiti podataka [Europski parlament i Vijeće Europske Unije, 2016] i Zakonom o provedbi Opće uredbe [NN 42/2018]. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka u Republici Hrvatskoj osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama.

Opća uredba o zaštiti podataka propisuje kako bi se podaci trebali obrađivati na pošten i zakonit način za određenu i legitimnu svrhu te se mogu obrađivati samo podaci koji su neophodni za određenu svrhu.

Općom uredbom o zaštiti podataka definirani su detaljni zahtjevi za poduzeća i organizacije koja prikupljanju osobne podatke, pohranjuju ih te upravljaju osobnim podacima [Vaša Europa, 2020]. Opća uredba se primjenjuju na organizacije koje obrađuju osobne podatke pojedinaca u EU-u te organizacije izvan EU-a koje su usmjerene na ljude koji žive u EU-u. Opća uredba se

ne primjenjuje ako se obrađuju podaci o preminulim osobama, pravnim osobama ili ako obradu obavlja osoba za vlastite potrebe/osobne potrebe. Osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Oni uključuju informacije temeljem kojih osoba može biti izravno ili neizravno identificirana, to su podaci kao što su: ime i prezime, adresa, broj osobne iskaznice ili putovnice, primanja, kulturni profil, adresa internetskog protokola (IP adresa), podaci u posjedu bolnice ili liječnika (koji služi kao jedinstvena identifikacijska oznaka u zdravstvene svrhe). Posebne kategorije podataka su informacije o rasnom ili etničkom podrijetlu, spolnoj orijentaciji, političkim stavovima, vjerskim ili filozofskim uvjerenjima, članstvu u sindikatu, genetskim, biometrijskim ili zdravstvenim podacima i osobni podaci povezani s kaznenim osudama i djelima osim ako to nije dopušteno pravom EU-a ili nacionalnim pravom.

„Općom uredbom o zaštiti podataka ojačane su mjere za zaštitu podataka, pojedincima se pružaju dodatna i veća prava te se osigurava veća transparentnost i odgovornije ponašanje svih koji obrađuju osobne podatke obuhvaćene njezinim područjem primjene. Njome se neovisnim tijelima za zaštitu podataka dodjeljuju snažnije i usklađene provedbene ovlasti te se uspostavlja novi sustav upravljanja. Njome se stvaraju i jednaki uvjeti za sva poduzeća koja posluju na tržištu EU-a, bez obzira na to gdje imaju poslovni nastan, te se osigurava slobodan protok podataka unutar EU-a, čime se jača unutarnje tržište“ [COM (2020) 264, 2020]. Opća uredba o zaštiti podataka značajno proširuje i ojačava glavna načela i pravila, izravno dodaje genetske i biometrijske podatke kao posebnu vrstu podataka, ima za cilj dovesti do veće usklađenosti prava zaštite podataka u državama članicama EU-a kao i dosljednije primjene i provedbe pravila, omogućava jača (i neka nova) prava ispitanika te omogućava prekograničnu suradnju između nadzornih tijela za zaštitu podataka.

2.2. NAČELA ZAŠTITE OSOBNIH PODATAKA

Opća uredba o zaštiti podataka navodi šest principa tj. načela koje institucije trebaju slijediti kada prikupljaju, procesiraju i pohranjuju osobne podatke korisnika [Europski parlament i Vijeće Europske Unije, 2016].

Prvo načelo se odnosi na zakonitost, poštenost i transparentnost. Kako bi se obrada podataka smatrala zakonitom potrebno je ispunili jedan od sljedećih uvjeta za obradu osobnih podataka: (1) pojedinac je dao privolu, (2) osobni podaci su potrebni za ispunjavanje ugovorne obveze prema pojedincu, (3) osobni su podaci potrebni kako bi poduzeće ispunilo zakonsku obvezu, (4) osobni su podaci potrebni za zaštitu životnog interesa pojedinca, (5) osobni podaci obrađuju se u okviru zadaće od javnog interesa i (6) obrada podataka nužna je za ostvarivanje legitimnih interesa poduzeća pod uvjetom da time nisu ozbiljno narušena temeljna prava i slobode pojedinca čiji podaci se obrađuju. Obradu osobnih podataka može provoditi voditelj i izvršitelj obrade. Voditelj obrade je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka. Izvršitelj obrade je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

Drugo načelo je ograničenje svrhe. Pod time se podrazumijeva da bi institucije trebale prikupljati podatke samo za svrhu o kojoj su obavijestili ispitanika te su dobili privolu za to (ili poliježe drugim uvjetima zakonitosti obrade). Potrebno je objasniti svrhu obrade, a sami podaci se mogu spremati onoliko dugo koliko je potrebno za izvršavanje te svrhe.

Sljedeće načelo je smanjenje količine podatka. Ovo načelo objašnjava prikupljanje onih osobnih

podataka od strane institucija koji su im potrebni u svrhu obrađivanja podataka. Sukladno tome poduzeća ne bi trebala prikupljati na primjer dva identifikatora pojedinca (OIB i JMBAG) jer je dovoljan jedan kako bi se osoba identificirala.

Četvrto načelo odnosi se na točnost. Poduzeća koja obrađuju podatke trebaju poduzeti razumne mjere kako bi podaci bili točni.

Peto načelo se odnosi na ograničenje pohrane podataka. Poduzeća trebaju izbrisati osobne podatke kada im više nisu potrebni za daljnje obrađivanje podataka.

Zadnje, šesto, ali ne manje važno načelo odnosi se na cjelovitost i povjerljivost podataka. Osobni podaci moraju se obrađivati na način koji osigurava odgovarajuću sigurnost osobnih podataka, uključujući zaštitu protiv neovlaštenog ili nezakonitog obrađivanja i zaštitu protiv slučajnog gubitka, uništenja ili oštećenja.

3. ISTRAŽIVANJE PRILAGODBE MREŽNIH STRANICA VISOKIH UČILIŠTA U REPUBLICI HRVATSKOJ ZAHTJEVIMA ZAŠTITE OSOBNIH PODATAKA

Istraživanja pokazuju da se privatnost smatra glavnim problemom u digitalnom društvu, međutim pojedinci otkrivaju svoje osobne podatke za male prednosti/benefite [Kokolakis 2017].

Institucije visokog obrazovanja prikupljaju velike količine osobnih podataka temeljem kojih pojedinac može biti identificiran. U većini slučajeva podaci se spremaju u različite baze podataka koje se dupliciraju u različitim odjelima ili organizacijskim jedinicama. Velika količina podataka, kao i pristup podacima od strane nastavnika, zaposlenika, vanjskih suradnika, studenata prema Yerby and Floyd [2018] predstavlja prijetnje osiguranju sigurnosti tih informacija. Opća uredba o zaštiti podataka [L 119/3] obavezala je institucije visokog obrazovanja da preispitaju i usklade svoje procedure i poslovne procese koji uključuju obradu osobnih podataka. Habbabeh i suradnici [Habbabeh, Schneider, and Asprion 2019] predlažu instrument koji se može koristiti s ciljem podizanja svijesti o zaštiti osobnih podataka u skladu s Općom uredbom o zaštiti podataka. Zimmeck i suradnici [Zimmeck et al. 2019] su predstavili MAPS (eng. *Mobile App Privacy System*) kojim su ispitivali Android aplikacije s obzirom na objavljivanje politika privatnosti i praksi koje koriste kako bi osigurali privatnost korisnika. Ispitivanje se baziralo na analizi koda i primjeni tehnika strojnog učenja. U ispitivanje je bilo uključeno 1 035 853 Android aplikacija s Google Play Store. Yerby i Floyd [2018] su ispitivali svjesnost nastavnika i zaposlenika fakulteta o informacijskoj sigurnosti. Rezultati su pokazali da obje ispitivane skupine pokazuju srednju ili visoku razinu svjesnosti informacijske sigurnosti.

3.1. PRIPREMA ISTRAŽIVANJA

Kako bi se provjerilo u kojoj su mjeri visoka učilišta u Republici Hrvatskog uskladila svoje poslovanje s promijenjenim pravilima vezanim uz zaštitu podataka provedeno je istraživanje mrežnih mjesta visokih učilišta.

Među najvažnije promjene koje je donijela Opća uredba o zaštiti podataka ubrajaju se uvođenje novog načela „odgovornosti [pouzdanosti]“ i institucije službenika za zaštitu podataka. Prema

Korff i Georges [2019] te dvije novine su povezane jer su službenici za zaštitu podataka upravo ti koji će u praksi morati osigurati usklađenost s načelom odgovornosti/pouzdanosti od strane i unutar organizacija kojima pripadaju.

Vrlo je važno da i studenti znaju kako mogu upotrebljavati podatke kojima imaju pristup putem različitih sustava u sklopu svojeg studija te kako odgovorno rukovati s njima. Kao takva, privatnost se odnosi na sposobnost odgovornog korištenja digitalnih alata, digitalnih medija i digitalnih resursa. To uključuje i da osoba postupa u skladu s pravima na privatnost te s pravilima i propisima etičke uporabe Interneta. Gudmundsdottir i suradnici [Gudmundsdottir, et al., 2020] u svojem istraživanju su ispitivali percepciju studenata vezano uz privatnost. Provjeravali su znaju li studenti zaštiti svoju privatnost online, znaju li poštivati pravila o zaštiti privatnosti drugih i znaju li poštivati pravila vezana uz autorstvo. Također, isto istraživanje proveli su i nad nastavnicima koji su zaposleni na sveučilištima u Norveškoj i Španjolskoj.

Neka inozemna sveučilišta zaštiti privatnosti posvećuju puno pažnje pa se na njihovim mrežnim mjestima mogu pronaći detaljne informacije kako se upotrebljavaju osobni podaci prijavljenih studenata, aktivnih studenata, prijavitelja za posao, sudionika u istraživanju [University of Cambridge, 2020]. Sveučilište Stirling primjerice ima pripremljene upute gdje su navedene informacije o tome što su osobni podaci, kada se primjenjuje privola, što je to obavijest o privatnosti (eng. *privacy notice*), što je to procjena utjecaja na zaštitu podataka, kada se fotografije mogu smatrati osobnim podatkom, kada je dozvoljen digitalni marketing prema studentima i ostalim dionicima, kako studenti mogu koristiti osobne podatke drugih, kako se koriste podaci prikupljeni u znanstvenim istraživanjima [University of Stirling, 2019]. Sveučilište u Edinburgu osim podataka o korištenim praksama za rukovanje osobnim podacima ima objavljene i primjere privola, informacijskog paketa (koji služi za informiranje) kao i informacije o informacijskim sustavima koji se koriste za prikupljanje, obradu i pohranjivanje podataka [University of Edinburgh, 2020.]. Sveučilište u Jyväskylä ima osim ostalog objavljene predloške privola i objašnjenja s obzirom na različite temelje prema kojim se provodi istraživanje, nadalje ima i objavljen obrazac za provedbu procjene utjecaja na zaštitu podataka kao i upute s informacijama za sudionike u istraživanju [University of Jyväskylä, 2020]. Za svoje istraživače, ali i ostale dionike sveučilište u Twente [University of Twente, 2020.] je pripremilo online aplikaciju gdje mogu prijaviti obradu podataka koju će provoditi. Nadalje, vrlo detaljno objašnjavaju koji informacijski sustavi i alati su dozvoljeni za korištenje, a koji ne, s opisima. Za studente su pripremljena najčešće postavljena pitanja kojima se opisuje što se očekuje od njih vezano uz zaštitu svoje i tuđe privatnosti tijekom studiranja na sveučilištu te kako se obrađuju njihovi osobni podaci za potrebe napredovanja na studiju.

Sukladno tome, u ovome istraživanju na mrežnim mjestima visokih učilišta u Republici Hrvatskoj provjeravano je:

1) Postoji li na mrežnim mjestima Pravilnik o zaštiti osobnih podataka?
2) Postoji li na mrežnim mjestima objavljena Politika privatnosti?
3) Postoje li na mrežnim mjestima objavljeni zahtjevi za ostvarivanje prava vezanih uz zaštitu osobnih podataka?
4) Postoje li na mrežnim mjestima objavljene informacije o službeniku za zaštitu podataka?
5) Postoje li na mrežnim mjestima upute za zaposlenike kako je potrebno rukovati osobnim podacima koje prikupljaju i obrađuju?
6) Postoje li na mrežnim mjestima upute za istraživače kako je potrebno rukovati osobnim podacima koje prikupljaju i obrađuju?
7) Postoje li na mrežnim mjestima upute za studente kako je potrebno rukovati osobnim

podacima koje prikupljaju i obrađuju?
8) Postoje li na mrežnim mjestima informacije o korištenim IKT servisima?

Metodom inspekcije provjeravano je postoje li na određenom mrežnom mjestu informacije kojim visoka učilišta informiraju o praksi koju koriste kako bi se osigurala privatnost studenata, zaposlenika, znanstvenika i drugih uključenih dionika.

3.2. PROVEDBA ISTRAŽIVANJA

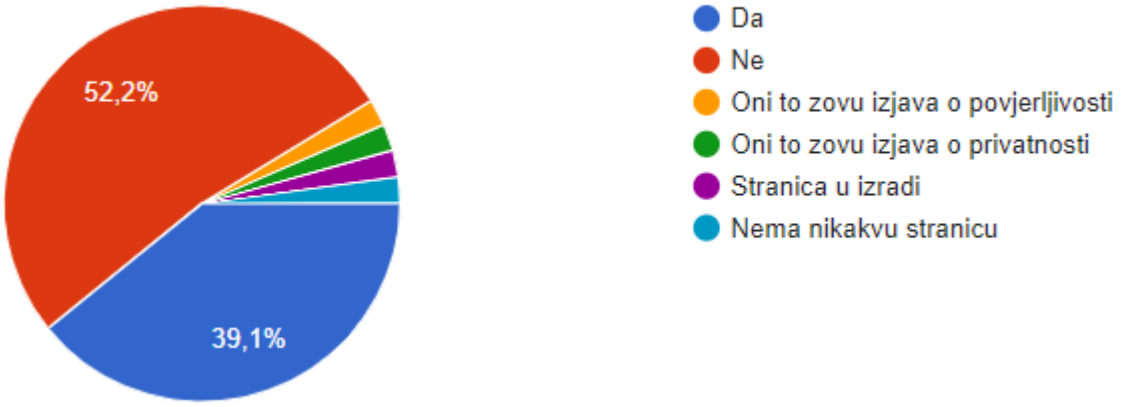
Prema tipu visokih učilišta sukladno Mozvag pregledniku [Preglednik studijskih programa - Odabir tipa n.d.] u Republici Hrvatskog postoji 128 visokih učilišta, od toga 105 njih je javno visoko učilište, a 23 njih je privatno visoko učilište. Istraživanje je uključivalo ispitivanje 46 mrežnih stranica visokih učilišta u Republici Hrvatskoj. U istraživanje je uključeno 8 javnih sveučilišta (ispitivanje nije uključivalo 82 sastavnice javnih sveučilišta), 12 javnih veleučilišta, 3 visoke javne škole, 2 privatna sveučilišta, 6 privatnih veleučilišta, 15 privatnih visokih škola. Ispitivanje nije uključivalo ispitivanje mrežnih mjesta sastavnica javnih učilišta prvenstveno zbog mišljenja autora da su sveučilišta odgovorna za definiranje praksi, procedura i načina ostvarivanja prava svih studenata i zaposlenika vezano uz privatnost.

3.3. REZULTATI

Istraživanje je provedeno tako da se utvrđivalo postoje li određeni dokumenti ili informacije (definirane u poglavlju 3.1.) na mrežnim mjestima visokih učilišta.

Prvo pitanje odnosilo se na provjeru postoji li na mrežnim mjestima Pravilnik o zaštiti osobnih podataka. Iz grafikona Prikaz 1. se može vidjeti kako se kod većeg udjela (52,2%) visokih učilišta Pravilnik o zaštiti osobnih podataka ne nalazi na njihovim mrežnim mjestima, dok kod 39,1% ispitanih visokih učilišta postoji objavljen Pravilnik. Kod ovog pitanja zanimljivo je da većina mrežnih mjesta nema posebnu mrežnu stranicu gdje se mogu pronaći informacije o praksama zaštite privatnosti. Isto tako zanimljivo je da neka visoka učilišta Pravilnik (službeni dokument potpisan od strane npr. dekana) nazivaju Izjava o povjerljivosti ili Izjava o privatnosti. Kod jednog visokog učilišta stavljen je link na Pravilnik koji nije valjan, dok jedno visoko učilište nema svoje mrežno mjesto.

Prikaz 1. Odgovori na pitanje „Postoji li na mrežnim mjestima Pravilnik o zaštiti osobnih podataka?“ (postotak %)

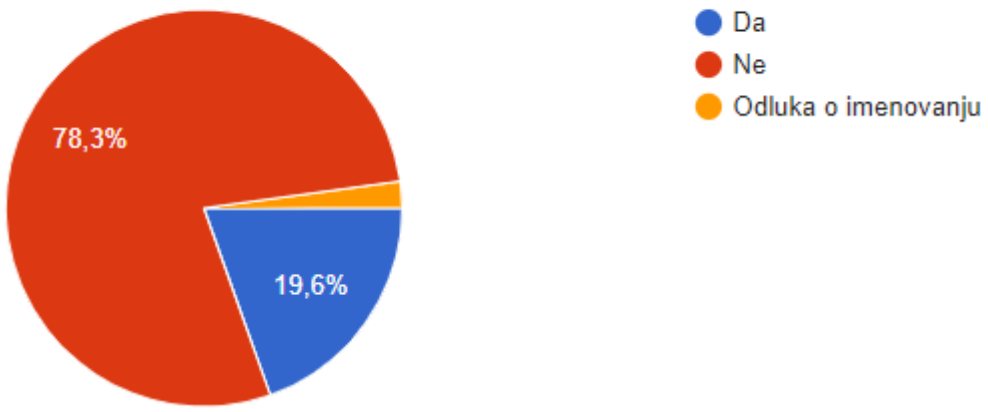


Drugo pitanje je glasilo „Postoji li na mrežnim mjestima objavljena Politika privatnosti?“. Kod 54.4% visokih učilišta postoji politika, dok kod 43.4% ne postoji (kod 2.2% se ne otvara stranica). Politika privatnosti u pravilu je sažeti opis kako određena organizacija rukuje podacima. Stoga je kod nekih visokih učilišta uočeno kako politiku privatnosti nazivaju još i obavijest o privatnosti, pravila privatnosti ili izjava o zaštiti privatnosti.

Za pitanje „Postoje li na mrežnim mjestima objavljeni zahtjevi za ostvarivanje prava vezanih uz zaštitu osobnih podataka?“, kod većine visokih učilišta ne postoji (80,4%), što znači da postoji kod samo 19,6% visokih učilišta. Na navedenim mrežnim mjestima objavljeni su obrasci koje korisnik može skinuti i popuniti te temeljem toga ostvariti svoje pravo (npr. za brisanje, za prijenos podataka i slično).

Nadalje za pitanje „Postoje li na mrežnim mjestima objavljene informacije o službeniku za zaštitu osobnih podataka?“, kao što je vidljivo na Prikaz 2. kod 78,3% visokih učilišta ne postoji objavljen taj podatak, kod 19,6% postoji, a ostalih 2.1% to nazivaju odluka o imenovanju (objavljen je dokument o službenom imenovanju službenika za zaštitu podataka).

Prikaz 2. Odgovori na pitanje „Postoje li na mrežnim mjestima objavljene informacije o službeniku za zaštitu podataka?“ (postotak %)



Kod pitanja da li postoje na mrežnom mjestu upute za istraživače, zaposlenike i studente u vezi zaštite osobnih podataka sva tri odgovora su negativna što znači da kod niti jednog visokog učilišta ne postoje navedene informacije. I informacije o korištenim informacijsko komunikacijskim servisima se isto nisu nalazile niti na mrežnom mjestu (od 46 visokih učilišta).

4. ZAKLJUČAK

Iako bi visoka učilišta trebala biti nosioci pozitivnih promjena i imati vodeću ulogu u promicanju dobrih praksi, kao i podizanju svijesti o važnosti zaštite podataka, iz istraživanja prikazanog u ovom radu vidljivo je da to nije slučaj u Republici Hrvatskoj. Ograničenje koje je potrebno uzeti u obzir prilikom interpretacije ovih rezultata odnosi se na činjenicu kako u ovo istraživanje nisu bile uključene sastavnice javnih sveučilišta. Sveučilišta su krovne institucije koje bi svojim sastavnicama trebale pružiti sve informacije kako bi se pozitivne prakse jednako primjenjivale na svim sastavnicama.

Renomirana sveučilišta u drugim državama Europske unije izvrstan su primjer kako se treba postaviti prema načelima zaštite podataka te se na njihovim mrežnim mjestima mogu pronaći vrlo detaljne informacije o svim korištenim praksama, procedurama kao i primjerima.

Daljnje istraživanje obuhvaćat će analizu reprezentativnog broja sveučilišta iz država članica Europske unije kako bi se identificirali ključni elementi objavljeni na njihovim mrežnim mjestima, a odnose se na zaštitu privatnosti. Temeljem provedenog istraživanja pripremit će se preporuke za skup elemenata koje je potrebno objaviti i komunicirati sa svim dionicima u visokom obrazovanju.

LITERATURA

1. Amo, Daniel, Marc Alier, Francisco José García-Peñalvo, David Fonseca, and María José Casañ. 2020. "Protected Users: A Moodle Plugin To Improve Confidentiality and Privacy Support through User Aliases." *Sustainability* 12: 1–16. https://doi.org/10.3390/su12062548.
2. CISCO. 2019. "Consumer Privacy Survey The Growing Imperative of Getting Data Privacy Right." CISCO Cybersecurity Series 2019, Data Privacy. 2019. https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf.
3. COM (2020) 264. 2020. "KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU Zaštita Podataka Kao Jedan Od Stupova Jačanja Položaja Građana i Pristupa EU-a Digitalnoj Tranziciji-Dvije Godine Primjene Opće Uredbe o Zaštiti Podataka 1 PRAVILA O ZAŠTITI PODATAKA KAO JEDAN OD STUPOVA JAČANJA POLOŽAJA GRAĐANA I PRISTUPA EU-A DIGITALNOJ TRANZICIJI." https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-.
4. "Common Challenges | EDUCAUSE." 2020. 2020. https://www.educause.edu/ecar/research-publications/the-evolving-landscape-of-data-privacy-in-higher-education/common-challenges.
5. "Data Privacy Trends 2020: What You Need to Know." 2020. 2020. https://www.formassembly.com/blog/data-privacy-trends-2020/.
6. eMarketer. n.d. "Why Customer Data Platforms Are Hot Right Now - EMarketer Trends, Forecasts & Statistics." 2018. Accessed July 28, 2020. https://www.emarketer.com/content/why-customer-data-platforms-are-hot-right-now.
7. Europski parlament i Vijeće Europske Unije. 2016. "Uredba (EU) 2016/679 - Opća Uredba o Zaštiti Podataka." *Službeni List Europske Unije* 119 (3): 1–88. https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=HR.
8. Gartner. 2020. "Gartner Predicts for the Future of Privacy 2020." 2020. https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/.
9. Gudmundsdottir, Greta Bjork, Hector Hernandez Gasso, Juan Carlos Colomer Rubio, and Ove Edvard Hatlevik. 2020. "Student Teachers' Responsible Use of ICT: Examining Two Samples in Spain and Norway. Computers & Education, 152, 103877 | 10.1016/j.Compedu.2020.103877." *Computers & Education* 152. https://sci-hub.tw/10.1016/j.compedu.2020.103877.

10. Habbabeh, Ali, Bettina Schneider, and Petra Maria Asprion. 2019. “Data Privacy Assessment: An Exemplary Case for Higher Education Institutions.” *International Journal of Management, Knowledge and Learning* 8 (2): 221–41.
11. Jones, Kyle M L, Andrew Asher, Abigail Goben, Michael R Perry, Dorothea Salo, and Kristin A Briney. 2020. “Title ‘We’re Being Tracked at All Times’: Student Perspectives of Their Privacy in Relation to Learning Analytics in Higher Education.” *J. Assoc. Inf. Sci. Technol.* 71: 1044–59.
12. Kokolakis, Spyros. 2017. “Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon.” *Computers and Security*. Elsevier Ltd. https://doi.org/10.1016/j.cose.2015.07.002.
13. Korff, Douwe, and Marie Georges. 2019. “The DPO Handbook Guidance for Data Protection Officers in the Public and Quasi-Public Sectors on How to Ensure Compliance with the European Union General Data Protection Regulation.” http://www.fondazionebasso.it/2015/wp-content/uploads/2018/04/T4Data_Brochure.pdf.
14. L 119/3. n.d. *UREDBA (EU) 2016/ 679 EUROPSKOG PARLAMENTA I VIJEĆA - Od 27. Travnja 2016. - o Zaštiti Pojedinaca u Vezi s Obradom Osobnih Podataka i o Slobodnom Kretanju Takvih Podataka Te o Stavljanju Izvan Snage Direktive 95/ 46/ EZ (Opća Uredba o Zaštiti Podataka)*.
15. “Preglednik Studijskih Programa - Odabir Tipa.” n.d. Accessed July 29, 2020. https://mozvag.srce.hr/preglednik/pregled/hr/tipvu/odabir.html.
16. Saleforce. 2019. “Customer Engagement Trends: Global Research - Salesforce Blog.” 2019. https://www.salesforce.com/blog/2019/06/customer-engagement-trends.html.
17. University of Cambridge. 2020. “Main Data Protection Provisions and Topics | Information Compliance.” 2020. https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance/provisions.
18. University of Edinburgh. n.d. “Data Protection | The University of Edinburgh.” Accessed August 3, 2020. https://www.ed.ac.uk/data-protection.
19. University of Jyväskylä. n.d. “Privacy Policy of the University of Jyväskylä, Guidelines and Templates for Research — University of Jyväskylä.” 2020. Accessed July 30, 2020. https://www.jyu.fi/en/university/privacy-notice/privacy-policy-of-the-university-of-jyvaskyla.
20. “University of Stirling, DATA PROTECTION GUIDANCE HANDBOOK.” 2019.
21. University of Twente. n.d. “Privacy: Personal Data | Cyber Safety.” Accessed July 30, 2020. https://www.utwente.nl/en/cyber-safety/privacy/.
22. Vaša Europa, Europska unija. 2020. “Zaštita Podataka Na Temelju Opće Uredbe o Zaštiti Podataka - Vaša Europa.” 2020. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm.
23. Yerby, Johnathan, and Kevin Floyd. 2018. “Faculty and Staff Information Security Awareness and Behaviors.” *Journal of The Colloquium for Information System Security Education*. Vol. 6. https://cisse.info/journal/index.php/cisse/article/view/90.
24. “Zakon o Provedbi Opće Uredbe o Zaštiti Podataka.” n.d. Accessed July 28, 2020. https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html.
25. Zimmeck, Sebastian, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang,

Joel Reidenberg, N. Cameron Russell, and Norman Sadeh. 2019. “MAPS: Scaling Privacy Compliance Analysis to a Million Apps.” *Proceedings on Privacy Enhancing Technologies* 2019 (3): 66–86. https://doi.org/10.2478/popets-2019-0037.