Implementacija GDPR-a u mala poduzeća

Stepan, Tea

SVEUČILIŠTE SJEVER
SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 105/OJ/2018

IMPLEMENTACIJA GDPR-A U MALIM PODUZEĆIMA

Tea Stepan

Varaždin, ožujak 2019.

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij KOMUNIKOLOGIJA I ODNOSI S JAVNOSTIMA

DIPLOMSKI RAD br. 105/OJ/2018

IMPLEMENTACIJA GDPR-A U MALIM PODUZEĆIMA

Studentica:

Tea Stepan, mat.br. 0523/336D

Mentor:

doc. dr. sc. Darijo Čerepinko

Varaždin, ožujak 2019.

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR–42000 Varaždin

Prijava diplomskog rada

studenata IV. semestra diplomskog studija Odnosi s javnostima

IME I PREZIME STUDENTA	Tea Stepan
MATIČNI BROJ	0523/336D
NASLOV RADA	Implementacija GDPR-a u mala poduzeća
NASLOV RADA NA ENGL. JEZIKU	GDPR implementation for small businesses
KOLEGIJ	OJ i internet
MENTOR	doc. dr. sc. Darijo Čerepinko
ČLANOVI POVJERENSTVA	1. doc.dr.sc. Tvrtko Jolić - predsjednik povjerenstva 2. doc.dr.sc. Anita Jeličić - članica 3. doc. dr. sc. Darijo Čerepinko - mentor 4. doc.dr.sc. Nikša Sviličić - zamjenski član

Zadatak diplomskog rada

BROJ: 105/OJ/2018

OPIS

GDPR uredba (General Dana Protection Regulation) je novi zakonski oblik zaštite prava podataka pojedinca. Primjena uredbe je obavezna u svim članicama Europske unije od 25. svibnja 2018. godine. S obzirom na aktualnost teme, ovaj rad će se baviti analizom implementacije uredbe u manja poduzeća. Cilj diplomskog rada je detaljno prikazati procese koji prethode implementaciji GDPR-a. Namjera rada je skupiti bitne informacije o implementaciji GDPR-a na jednom mjestu koje mogu poslužiti kao informativno štivo za zainteresirane poslovne subjekte.
U radu će biti obrađeno:

- definicija i obrazloženje GDPR-a
- pojam autentikacije, anonimizacije, pseudominizacije i profiliranja
- obrazloženje termina osjetljivih podataka
- faze implementacije uredbe u poslovanje poduzeća
- kreiranje obrazaca (izvještaji i izjave)
- poteškoće u provedbi
- automatizirana i neautomatizirana obrada podataka
- načela i zakonitosti obrade
- imenovanje i obaveze voditelja obrade, prava ispitanika
- primjeri u praksi

Istraživanje će se temeljiti na anonimnom anketnom ispitivanju s ciljem utvrđivanja stavova o većem ili manjem osjećaju sigurnosti pojedinca nakon obavezne zakonske primjene uredbe, znanju o primjeni, a rezultati istraživanja mogu ukazivati na propuste u edukaciji ili nezainteresiranosti, odnosno zainteresiranosti javnosti za ovo polje.

U VARAŽDINU, DANA 21. 12. 2018.

POTPIS MENTORA

SVEUČILIŠTE SJEVER KOPRIVNICA

DIR 01 OJ

Sažetak

Opća uredba o zaštiti osobnih podataka postaje sastavni dio poslovanja, iako su mnoga mala poduzeća imala poteškoća s njezinom provedbom zbog nedovoljno informacija pružanih javnosti prije stupanja uredbe na snagu 25. svibnja 2018. godine. GDPR je obavezan za sve organizacije, profitne i neprofitne.

Faze primjene počinju od prepoznavanja potrebe za implementacijom, vršenje GAP analize, procjene rizika, kreiranje potrebne popratne dokumentacije (izrada formulara) i testiranje te provedba. U radu postoje primjeri iz prakse i rješenja Agencije za zaštitu osobnih podatka (nadležno tijelo za nadzor provedbe GDPR-a). Ključno istraživačko pitanje koje je obrađeno u radu se odnosi na razinu informiranosti javnosti i stopu sigurnosti koju građani osjećaju u vezi zaštite osobnih podataka. Javnost smatra da se GDPR u hrvatskim poduzećima uopće ne provodi ili se provodi samo fiktivno, što dokazuju i rezultati istraživanja.

Ključne riječi: Opća uredba o zaštiti podataka, faze implementacije, GDPR, zaštita osobnih podataka, DPO, mala poduzeća, razina informiranosti

Abstract

The General Data Protection Regulation has become an integral part of the business, although many small businesses have had difficulties with its implementation due to insufficient information given to the public before the GDPR started to be mandatory on May 25, 2018. GDPR is necessarily for all organizations, both profitable and non-profitable.

The implementation phase starts from recognizing the need for implementation, performing GAP analysis, risk assessment, creating the required supporting documentation (forms) and testing and implementation. This paper containes analyses of practices and solutions of the Agency for the Protection of Personal Data (the supervisory authority for the implementation of the GDPR in Croatia). A key research question addressed in this paper is the level of public awarness and the level of security that citizens feel regarding the protection of personal data. The public believes that the use of GDPR is non existing or only fictitious in most businesses, as the research results prove.

Key words: General Data Protection, Phases of implementation, GDPR, Personal Data Protection, DPO, Small Businesses, Level of awarness

Popis korištenih kratica

GDPR	General Data Protection Regulation
EU	Europska Unija
AZOP	Agencija za zaštitu osobnih podataka
IT	Informatička tehnologija
QA	Questions and Answers (pitanja i odgovori)
DPO	Data Protection Officer (službenik za zaštitu osobnih podataka)
OUZP	Opća uredba o zaštiti podataka
KBC	Klinički bolnički centar
CERT	Computer Emergency Response Team

Sadržaj

1. Uvod

Digitalizacijom poslovanja nastaju rupe u zakonodavstvu vezane uz obradu osobnih podataka. Određene zemlje članice Europske unije, kao što je na primjer Njemačka, primjenjuju snažnu zaštitu osobnih podataka pojedinca. Pokušavajući izjednačiti procese zaštite podatka na razini EU, a istodobno smanjiti učestale skandale vezane u netransparentno rukovanje osobnim podacima, donosi se direktiva koja je od 25. svibnja 2018. godine obavezna za sve države članice. Cilj uredbe je pružanje kontrole podataka ispitaniku, pružanje moći odlučivanja građanima Europske unije. Reguliraju se obaveze svih neprofitnih i profitnih organizacija koje su dužne ispunjavati svoje obaveze u području zaštite osobnih podataka. Najvažniji dijelovi uredbe odnose se na temelje obrade osobnih podataka i prava ispitanika.

U prvom dijelu radu će ukratko biti objašnjena srž GDPR-a, osnovna svrha, zakonski okvir, navedeni subjekti na koje se uredba odnosi. Slijedi prikaz povezanih zakona i uredba koji su prethodili uredbi i znatno utjecali na njeno formiranje. Nakon upoznavanja sa zakonskim okvirom, prelazi se na najvažnije pojmove u uredbi kao pomoć pri tumačenju GDPR-a kao što su pojam privole, pojmovi mjera zaštita, anonimizacija i pseudonimizacija.

Struktura poslovnih subjekata u RH ukazuje na većinski udio mikro i malih poduzeća u gospodarstvu. Značaj koji ova vrste poduzeća imaju na ekonomiju države je važan, a upravo se takva vrsta poduzeća susrela s najviše nepoznanica u vezi implementacije GDPR-a. S obzirom na to da često mala ili mikro poduzeća nemaju predviđeni budžet za angažiranje vanjske konzultantske usluge za implementacije Opće uredbe o zaštiti podataka, nastojalo se prikazati faze koje mali poduzetnik/poduzetnica, uz dodatnu pomoć pretraživanja interneta ili eventulano traženja savjeta AZOP-a za specifične situacije, može sam/sama primijeniti u svojem poduzeću. Cilj izrade ovog diplomskog rada je kreiranje jednostavnog dokumenta koji može poslužiti kao bazni dokument za implementaciju GDPR-a ili štivo informativnog karaktera za sve zainteresirane (mali priručnik).

Problemi s kojima se mala poduzeću susreću često proizlaze iz nedovoljno jasnog općeg tumačenja uredbe, a na cijelu situaciju najveći učinak ima percepcija javnosti o samoj uredbi, odnosno nedovoljna razina informiranosti ili kriva predodžba o značenju uredbe. Nakon što je uredba postala obavezna, bilo je uvriježeno krivo mišljenje kojim se ispitanicima za svaku obradu osobnih podataka obavezno davao formular privole, zbog straha od sankcija i visoko propisanih kazni. Uvođenjem u praksu i detaljnim čitanjem i

tumačenjem uredbe, spoznalo se da privola nije nužna za obradu podataka, već samo jedan od temelja koji omogućuje upravljanje osobnim podacima.

Izvori informacija koji su pridonijeli izradi ovog rada sastoje se od zakonskih dokumenata, osobnog iskustva, literature na engleskom jeziku (u Hrvatskoj nije izdana knjiga o GDPR-u za vrijeme pisanja ovog rada) i vjerodostojnih internet izvora.

Izradu teorijskog dijela prati istraživanje kojim se pokušava doznati realna i samoprocijenjena razina informiranosti o GDPR-u i njihov odnos, kao i mišljenja ispitanika i njihovi stavovi vezani uz stopu sigurnosti koju osjećaju ili ne osjećaju nakon implementacije GDPR-a.

2. GDPR

2.1. Obrazloženje GDPR-a

Cilj GDPR-a je, prema autorici Ripoll Servent (2017; 121) pružanje zajedničkih standarda za zaštitu podataka koji može biti primjenjiv na svjetskoj razini, rješavanje spornih pojmova – definiranje "osobnih podataka", kreiranje novih prava kao što je pravo na zaborav, prenosivost osobnih podataka i stvaranje sankcija (pravnih i novčanih) za kršenje prava građana. Ističe načelo opće zaštite podataka – uredba mora biti integrirana u razvijanje novih usluga i građanima se automatski treba nuditi najveća moguća zaštita bez njihovog napora da sami u postavkama podešavaju veća prava.

„*Opća uredba o zaštiti podataka (GDPR), koja je 25. svibnja 2018. godine stupila na snagu, osmišljena je da osobne podatke građana zaštiti od komercijalne zloporabe. Drugim riječima, vaši su osobni podaci vaše vlasništvo pa, kao što ne želite da raznorazne tvrtke nekontrolirano raspolažu vašim novcem i nekretninama, jednako tako bilo bi dobro da nemaju neometan pristup i slobodnu volju kad je riječ o vašem imenu, OIB-u, adresi i ostalim podacima koji vas obilježavaju kao osobu*.“ (Span d.o.o., www.gdpr2018.eu)

Najviše poteškoća nastaje s velikim kompanijama – navode Baumann i Schünemann (2017)**;** mnogi servisi na internetu, s naglaskom na društvene mreže imaju monopolne pozicije i korisnici prihvaćaju uvjete korištenja (automatski i obrade podataka) zbog nemogućnosti izbora, odnosno kao uvjet za pripadnost skupini. Ekstremna posljedica neprihvaćanja uvjeta korištenja može biti i društvena isključenosti.

2.2. Osnovna svrha

Digitalizacija, rastuće tržište online proizvoda i usluga, svakodnevna kupnja i razmjena na milijune osobnih podataka, glavni su razlog postojanja GDPR-a. Uredbom se nastoji spriječiti moguće malverzacije – netransparentna obrada podataka, prodaja ili prosljeđivanje osobnih podataka trećim stranama bez znanja ispitanika.

De Guise (2017.; 9) upozorava na evoluciju kriminala na webu koja ugrožava poduzeća. Nekad su brige o sigurnosti na internetu podrazumijevale viruse koji su uzrokovali padove sustava ili „crve“ - krivce za brisanje podataka. Posljednjih par godina u porastu je iznuđivanje, ucjene hakera usmjerene prema pravnim osobama. Napad je često planiran, žrtva pomno birana. Kako bi se osigurali, prvo usmjeravaju pažnju na brisanje back-upa, zatim slijedi obrada izvornog sistema. IT kriminalci se usredotočuju na krađu podatka koje mogu preprodati trećoj osobi ili zamjenu za otkupninu podatke „vratiti“ poduzeću.

Predviđene su i sankcije za nepoštovanje GDPR uredbe, i to:

- Do dva posto ukupnog godišnjeg prometa ili 10 milijuna eura (ovisno što je više) za kršenje GDPR-a u tehničkom smislu
- Do četiri posto ukupnog godišnjeg prometa ili 20 milijuna eura (kažnjava se s većim iznosom) za teže povrede – ponavljanje kršenja, netransparentni prijenos podataka iz države u državu, oglušenje na upute organa za zaštitu osobnih podataka

2.3. Zakonski okvir

Pojavom GDPR-a je uređeno, dopunjeno i osuvremenjeno pravo na zaštitu osobnih podataka. Kroz povijest su se pojavili zakoni kojima su stvoreni temelji prava, a globalnom digitalizacijom je stvorena potreba za reguliranjem većeg opsega osobnih podataka.

2.3.1. Područje Europe

- Europska konvencija o ljudskim pravima, nastala u Rimu, 5. studenog 1950. godine – spominjanje prava na privatnost u dopisivanju i životu, članak 8.

„1. Svatko ima pravo na poštivanje svog privatnog i obiteljskog života, doma i dopisivanja. 2. Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih. „ (Konvencija za zaštitu ljudskih prava i temeljnih sloboda, članak 8.)

- Konvencija 108 Vijeća Europe, sastavljena u Strasbourgu, 28. siječnja 1981., govori o zaštiti pojedinca prilikom automatizirane obrade podataka. Ratificirale su ju sve države članice EU. Kasnije, 2001. godine donosi se Dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka. U Hrvatskoj se 2003. godine, sukladno spomenutoj konvenciji i njenoj dopuni, donosi Zakon o potvrđivanju konvencije za zaštitu osoba glede automatizirane orade osobnih podataka i dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka. Pojavljuje se drugačiji pristup: detaljnija objašnjenja prava osoba na saznanja o čuvanju osobnih podataka, pojavljivanje uloge upravitelja zbirke i definirana svojstva podataka:

„Osobni podaci koji su predmet automatizirane obrade trebaju biti:

- *probavljeni i obrađeni u dobroj vjeri i zakonito*
- *pohranjeni u određene i zakonite svrhe i ne smiju biti uporabljeni na način koji je nespojiv*
- *odgovarajući, mjerodavni i ne suvišni u odnosu na svrhe u koje su pohranjeni;*
- *točni i, ako je to potrebno, ažurirani,*
- *sačuvani u obliku koji onemoguće identifikaciju subjekata podataka tijekom razdoblja koje nije duže nego što nalaže svrha u koju su pohranjeni.“*

*(*Zakon o potvrđivanju konvencije za zaštitu osoba glede automatizirane orade osobnih podataka i dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, članak 5.)

2.3.2. Područje Republike Hrvatske

- Ustav Republike Hrvatske - 37. članak ustava – objašnjenje termina „privola“, pojava „ispitanika“:

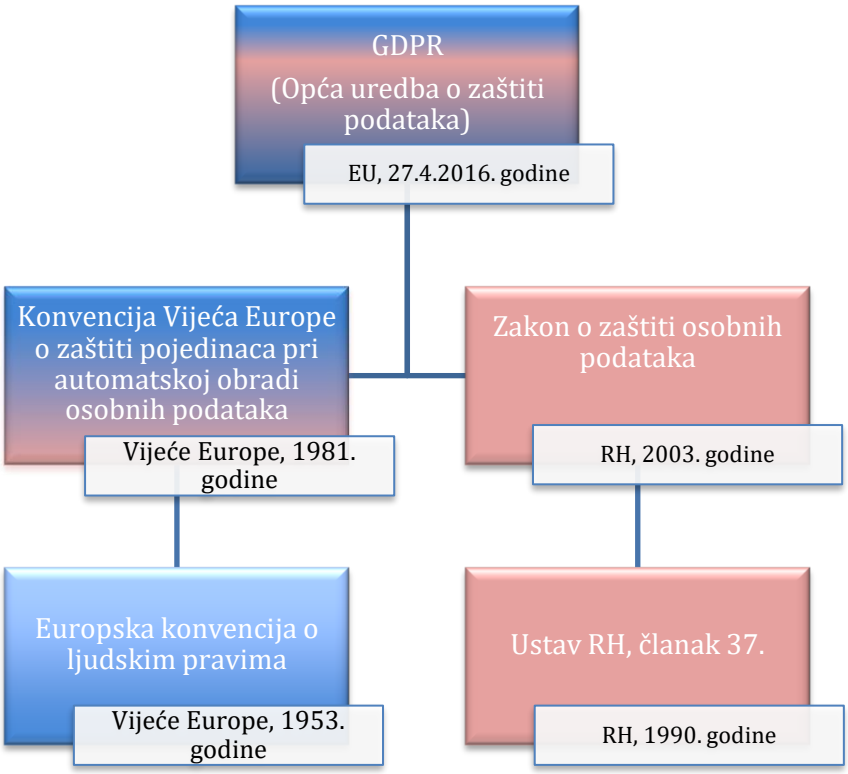
„Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihova prikupljanja.“ (Ustav Republike Hrvatske, članak 37.)

- Zakon o zaštiti osobnih podataka, na snazi od 4. srpnja 2003. do 25. svibnja 2018. godine (NN, br.106/12) – osniva se Agencija za zaštitu osobnih podataka i uređuju njezine ovlasti i područje djelovanja.

Vezano uz Zakon o zaštiti osobnih podataka, usvojene su i važne uredbe vezane uz istu problematiku:

a) Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka - za sve koji imaju više od 5 zaposlenika

b) Uputa o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN, br. 139/2004)



Grafikon 1: Zakoni vezani uz GDPR

2.4. Subjekti na koje se odnosi uredba

„Ova se uredba ne primjenjuje na obradu osobnih podataka koju fizičke osobe obavljaju u okviru isključivo osobne ili kućne aktivnosti te stoga nije povezana s profesionalnom ili komercijalnom djelatnošću. U osobne i kućne aktivnosti može se ubrajati korespondencija i posjedovanje adresa ili društveno umrežavanje te internetske aktivnosti poduzete u kontekstu takvih aktivnosti.„ (Članak 18. Uredba EU 2016/679 Europskog parlamenta i Vijeća)

Kreirana je s ciljem zaštite građana Europske unije, a primjenjuje se na sve organizacije koje obrađuju osobne podatke, a:

- Posluju na području Europske unije
- Posluju s građanima Europske unije (izvanteritorijalna primjenjivost)

Moore (2018.) savjetuje pogled na GDPR kao priliku za dokazivanje spremnosti; dosljedno održavanje sigurnosti podataka i dobro razrađene politike i procedure doprinose novom, sigurnijem početku upravljanja podataka u organizaciji. Pozitivan stav prema uredbi može pomoći stvoriti efikasniju zaštitu klijenata i omogućiti lakše shvaćanje srži problema.

Međutim, autori Voigt i Von dem Bussche (2017), navode kako pravne osobe ne uživaju pravnu zaštitu GDPR-a, već se ona odnosi samo na pojedince i njihova temeljna prava iz Povelje o temeljnim pravima Europske unije. Podaci o pravnim osobama se smatraju osobnim podacima tek ako sadrže informacije koje su usko povezane s pojedincem, npr. funkcija u poduzeću ili slično. Također, osoba koja je vlasnik poduzeća i jedini zaposlenik, smatra se fizičkom osobom jer je nemoguće razdvojiti osobne i pravne podatke o pojedincu.

.

3. Terminologija u uredbi

3.1. Osobni podaci, osjetljivi podaci, službenik za obradu podataka

Prema IT Governance Privacy Team-u (2017), osobni podatak je onaj koji se odnosi na prepoznatljivu fizičku osobu. Fizičke osobe se mogu identificirati na dva načina:

1. Izravnom identifikacijom – ako informacije sadrže podatke o osobi koji identificiraju pojedinca
2. Neizravnom identifikacijom – opisom informacija na način koji omogućuje otkrivanje identiteta osobe dodatnim istraživanjem ili naporom.

Identifikator je podatak koji otkriva o kojoj se osobi radi, a najčešće se radi o imenu, OIB-u, geo podacima, IP adresi, telefonskom broju, fizičkim čimbenicima, ekonomskim, fiziološki, mentalnim obilježjima ili genetski materijal. Također se u ulozi identifikatora mogu naći kulturni i socijalni identitet osobe. Kada informacija nije osobni podatak? Kada ne postoji način da se poveže s fizičkom osobom.

Pojam obrade osobnih podataka, prema GDPR-u, podrazumijeva: prikupljanje, bilježenje, organiziranje, strukturiranje, pohranu, prilagodbu ili izmjenu, pronalaženje, uporabu, otkrivanje prijenosom, ograničavanje, brisanje ili uništavanje podataka.

AZOP definira službenika za zaštitu podataka kao zaposlenika/zaposlenicu (interno ili eksterno) koji je zadužen kontrolirati provođenje GDPR uredbe. Za obavljane ove dužnosti, osoba mora imati određene kvalifikacije i razumjeti zakon i svjetske i domaće propise, a potrebne su i IT vještine. U Zakonu nije propisano koje kvalifikacije mora imati, no agencija navodi da službenik (Data Protection Officer) ne može biti osoba protiv koje se vode postupci u području povrede etičkog kodeksa poduzeća (ili je protiv nje izrečena mjera).

Opća uredba o zaštiti podataka izdvaja posebnu kategoriju – osjetljive podatke:

- Rasno ili etničko podrijetlo
- Politička, vjerska mišljenja i filozofska uvjerenja
- Clanstvo u sindikatu

- Genetski i biometrijski podaci
- Zdravstvene informacije
- Podaci o spolnom životu i seksualnoj orijentaciji ispitanika

3.2. Ispitanik i prava ispitanika

Ispitanik je svaka fizička osoba čiji se osobni podaci prikupljaju, a voditeljem obrade nazivamo poduzeće koje obrađuje takve podatke.

Prava ispitanika prema Općoj uredbi o zaštiti podataka (2018):
- pravo na ispravak
- pravo zaborava (brisanje)
- povlačenje date privole
- prigovor na obradu podataka (prigovor na profiliranje)
- ograničenje obrade
- prenosivost podataka (u čitljivom formatu)
- izravan prijenos

3.3. Pojam privole

Prema Lambertu (2018, 94), ako je proces obrade podataka temeljen na privoli (pristanku), voditelj obrade mora moći dokazati da je pojedinačni subjekt, odnosno ispitanik pristao na obradu osobnih podataka. Privola u pisanom obliku mora biti:

- Razumljiva i u lako dostupnom obliku
- Pisana na jasan način
- Upotrebljen jednostavan jezik
- Jasno se mora razlikovati od drugih pitanja

Osim osnovnih smjernica sadržaja privole, u Općoj uredbi za zaštitu osobnih podataka se navode i informacije koje moraju biti pružane u dokumentu privole, u svrhu pravodobnog i istinitog informiranja osobe o pravima i procesima:

- Pouka o pravu na pristup, ispravak, brisanje, ograničavanje obrade i prigovor

- Pouka o pravu na povlačenje privole
- Pouka o pravu na podnošenje prigovora nadležnom tijelu
- Informaciju o tome je li pružanje podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora
- Posljedice (ako postoje) koje subjekt snosi ako ne ustupi osobne podatke

Primjer privole:

Zaglavlje, podaci o poduzeću koje
obrađuje informacije.

NASLOV: **IZJAVA O DAVANJU SUGLASNOSTI ZA OBRADU OSOBNIH PODATAKA (ILI PRIVOLA)**

Prihvaćanjem ove izjave dajete privoli da daljnju obradu vaših osobnih podataka u ovdje navedene svrhe:

-_____
-_____
-_____ (upisivanje svrha)

Prikupljamo i obrađujemo sljedeće Vaše podatke:
-_____
-_____
-_____ (upisati sve osobne podatke koji se planiraju obrađivati)

Potpisom potvrđujete svoju suglasnost u vezi obrade vaših osobnih podataka. Razdoblje u kojem će osobni podaci biti pohranjeni: prema Zakonu sve dok se ostvaruje svrha obrade ili u skladu s ostalim zakonskim propisima koji mogu uključivati arhivsku građu.

Vaši podaci će biti zaštićeni od neovlaštenog pristupa ili zlouporabe, te će se s njima postupati sukladno mjerodavnim propisima uz odgovarajuće sigurnosne korake.

(ako poduzeće ima voditelja obrade, popunjava jedan ulomak o opsežnim informacijama i ovlastima službenika). Voditelj obrade kontrolira pristup vašim podacima, a dijeli ih samo sa zaposlenicima kojima su oni neophodni radi provedbe poslovnih zadataka. Prosljeđivanje trećim osobama je moguće samo u slučajevima propisanim zakonom.

Prosljeđivanje vaših podataka (samo u slučaju ispunjavanja ugovora):
a) pružateljima dostavnih usluga – isporuka vaše narudžbe
b) ovlašteni servis – u slučaju reklamiranja proizvoda naših dobavljača, kupljenih u našem poduzeću.

Vaša prava:
- brisanje, izmjena, ažuriranje vaših podataka
- pravo na ulaganje prigovora na obradu
- pravo na zaborav
- pravo na povlačenje privole
- pravo na prenosivost podataka

Podaci o ispitaniku i mjestu i datumu davanja privole: mjesto i datum, ime i prezime i vlastoručni potpis (formular ispisan na dva ili više A4 lista zahtjeva potpis na svakoj stranici).

3.4. Pojam mjera zaštita, anonimizacije i pseudominizacije

Prema CERT-ovoj publikaciji o anonimizaciji i pseudonimizaciji (2018), postoji određen broj mjera zaštite koje je moguće primijeniti za smanjenje rizika od povrede sigurnosti osobnih podataka.

Mjere zaštite podataka prema CERT-u (2018):
- fizička zaštita infrastrukture – zaključavanje sobe s poslužiteljima, ograničavanje pristupa neovlaštenim osobama
- zaštita infrastrukture od ciber napada – upotreba vatrozida, ažuriranje software-a (sigurnosne zakrpe), korištenje antivirusa
- šifriranje podataka – u slučaju napada, podaci su neupotrebljivi bez ključa za dešifriranje.

U svom radu, Dainty i Keyser (2016) detaljnije objašnjavaju zadovoljavajuću razinu fizičke zaštite. Prema autorima, svi serveri bi trebali biti zatvoreni u prostoru s fizičkim barijerama, ključanice na vratima, zatvoreni prozori, računala pričvršćena za stolove i instalirani alarmni sustav.

U mjere zaštite spadaju i anonimizacija i pseudonimizacija podataka. Anonimizacijom se naziva postupak trajnog sprječavanja moguće identifikacije osobe iz izdvojenih podataka. Pseudonimizacija predstavlja proces gdje se podataka kojim možemo identificirati osobu zamjeni sa pseudonimom. Na odvojenoj se lokaciji drže podaci koji povezuju identifikator i dodijeni pseudonim. Pseudonimizirani podaci se ne smatraju anonimnima i treba ih tretirati prema svim načelima GDPR-a.

Pečat privatnosti, odnosno, "Privacy Seal" je postupak certificiranja procesa obrade podatka koji kupcima jamči transparentu obradu podataka i garantira zakonito ophođenje s informacijama o ispitaniku. Autori De Hert i Kamara (2018; 24) navode činjenicu da pečati privatnosti nisu obavezni prema GDPR-u, no najveća prednost im je jačanje povjerenja kupca i prodavatelja.

4. Faze implementacije

4.1. Prepoznavanje potrebe

Uvođenjem uredbe, njena provedba je postala obavezna za sve pravne subjekte u Republici Hrvatskoj, bez obzira radi li se o profitnim ili neprofitnim organizacijama. Krajem svibnja 2018. godine, mnoga poduzeća nisu imala predodžbu što je to GDPR i na koje načine ga treba provoditi. Paralelno mediji prenose vrlo oskudne i suhoparne informacije o tome što uredba jest, a naglašavani su visoki iznosi kazni za nepoštivanje.

Nakon što je shvaćena potreba za implementacijom, postavlja se pitanje provođenja. Treba li se ona odvijati unutar tvrtke ili angažirati vanjsko poduzeće koje je specijalizirano za GDPR?

Na mrežnim stranicama AZOP-a postoje već gotovi obrasci i objašnjenja, no obrasci se razlikuju ovisno o opsegu podataka tumačenja samog zakona i njegove primjene u praksi.

4.1.1. Interno planiranje provedbe

Tumačenje nove uredbe i razvijanje procesa koji prate poslovanje organizacije iziskuje puno truda i znanja. Za pravilnu primjenu potreban je i određen stupanj obrazovanja, a neizbježno je informatičko i pravno iskustvo. Osoba koja bi trebala interno provesti sve potrebne korake za implementaciju snosi veliku odgovornost, a upitna je mogućnost objektivnog sagledavanja situacije. Hoće li se planiranje provedbe uredbe odvijati interno ili eksterno ovisi i o veličini poduzeća i opsegu fluktuacije podataka. Radi li se o mikro poduzeću s dvije zaposlene osobe, vrlo vjerojatno se proces planiranja i uvođenja može provesti unutar poduzeća, proučavanjem sadržaja na AZOP stranicama, provjerenim i autentičnim web stranicama, stručnim člancima ili razmjenom iskustva s poduzećima slične djelatnosti. Međutim, komplikacije mogu nastati u većim organizacijama.

Prednost: manji troškovi (ako na raspolaganju imamo odgovarajuću osobu koja uz dnevne poslove može obaviti i poslove vezane uz GDPR, znači već zaposlena osoba).

Nedostaci: ugrožena subjektivnost, mogući propusti zbog nedovoljno iskustva, nemogućnost brzog reagiranja, potencijalne visoke kazne uzrokovane nepokrivanjem svih područja upravljanja osobnim podacima.

4.1.2. Eksterno planiranje provedbe

Organizacije većinom koriste konzultantske usluge poduzeća specijaliziranih za provođenje GDPR-a. Obrazovanje zaposlenika jedne takve konzultantske tvrtke je mješovito, a najčešće se pojavljuju (u kombinaciji) zanimanja pravnika, informatičara, programera i poslovnih analitičara. Ovakav spoj potrebnih znanja i vještina može ponuditi konkretna rješenja za implementaciju.

Prednosti: objektivan pristup, prijašnje iskustvo, brža GAP analiza, samouvjerenost, kontinuirana podrška (ovisno o paketu usluge), stručna edukacija, „user friendly“ objašnjenje pojmova, pojednostavljenje procesa.

Nedostaci: moguće oduljenje procesa zbog nedovoljne komunikacije zaposlenika poduzeća koje traži i poduzeća koje isporučuju uslugu, potencijalno visoki troškovi ovisno o opsegu podataka koje treba popratiti u implementaciji.

U Hrvatskoj trenutno djeluje desetak poduzeća (prema pretraživanju interneta za pružatelje usluge implementacije GDPR-a dana 5.2.2019. godine). Novost na tržištu je razvijanje software-a koji služi za lakše praćenje i pregled obrade, danih privola, zahtjeva i otvorenih incidenata, uključujući i povijest za svaki od ovih koraka. Tvorci aplikacije kao najveću prednost ističu lakše upravljanje životnim ciklusom osobnih podataka i jednostavno eksportiranje izvještaja za AZOP.

4.2. GAP analiza

Provedbom GAP analize mjerimo razliku između postojeće situacije i situacije kojoj težimo. Procjena trenutnog stanja nam može pomoći da popunimo nedostatke, odnosno „rupu“, koja nam onemogućava ispunjenje GDPR uredbe. Ključno je dobiti odgovore na pitanja o strukturi podataka kojima upravljamo, različita vrsta podataka zahtjeva drugačiji pristup i rješenje. Smjer implementacije ovisi o saznanjima prikupljenim metodom analize. Uspješnost rezultata krije svoje temelje u detaljnoj analizi korištenih osobnih podataka. Nit vodilja su općenita pitanja koja nastoje pokriti apsolutno sve poslovne procese, te iz dobivenih informacija donositu odluke o planu postupanja. Pitanja se postavljaju unutar dvije kategorije, u prvoj se odvija klasifikacija i skupljanje svih podataka, dok u drugoj

nastaje selekcija pomoću temelja obrade osobnih podataka – izdvaja se popis zakonskih osnova koje su uporište za pohranjivanje osobnih podataka.

4.2.1. Vrste osobnih podataka koje poduzeće obrađuje i pohranjuje

U svakodnevnom poslovanju isprepliće se bezbroj osobnih podataka – ime, prezime, adresa, mail adresa. Vrste osobnih podataka možemo podijeliti na tri skupine ovisno o izvoru:

- podaci koje poduzeće prikuplja od kupaca
- podaci koje poduzeće prikuplja od dobavljača
- podaci koje poduzeće prikuplja od zaposlenika

Najjednostavniji način pomoću kojeg se može saznati narav i vrsta podataka kojima se upravlja u poduzeću je analizom jednog radnog dana. Potrebno je prikupiti više zaposlenika na različitim radnim mjestima ako se radi o kompleksnijem poduzeću i zapisati svaki susret ili rukovanje s bilo kakvom vrstom podataka. Pitanja za usmjeravanje:

- U kojoj situaciji dolazi do preuzimanje i obrade podataka?
- O kojim se točno podacima radi?
- U koju svrhu skupljamo te podatke?

Zaposlenik A, B i C zapisuju situacije u kojima dolazi do preuzimanja i korištenja osobnih podataka, sastavljaju detaljnu tablicu u koju bilježe koje podatke preuzimaju. Na kraju analize, sve tablice se spajaju u jednu i nastaje „Analiza o vrsti osobnih podataka kupaca“.

a) podaci koje poduzeće obrađuje od svojih kupaca

Proces kupnje rezultira preuzimanjem osobnih podataka od kupaca na više razina. Kanali prodaje su različiti, stoga preuzimaju i drugačije vrste podataka. Najveću opasnost predstavljaju nepotrebni podaci koji se prikupljaju u marketinške svrhe bez traženja privole ispitanika.

Primjer u praksi:

Zamislimo situaciju u kojoj se izmišljeno poduzeće Bikko d.o.o. bavi prodajom dekorativnih predmeta. Bikko d.o.o. svakodnevno zaprima upite o proizvodima, zaposlenici odgovaraju na mailove i telefone, a poduzeće ima i web shop putem kojeg prodaju svoje proizvode i šalju na adrese kupcima. Analiza poslovnog procesa mora sadržavati svaki korak, npr:

- Web shop - obrađuje, pohranjuje, prosljeđuje dostavnoj službi: ime, prezime, adresa, broj telefona i mail adresa, OIB za potrebe isporuku naručene robe (za što ima i legitimni interes). Bikko d.o.o. ne može robu isporučiti ako kupac poduzeću ne otkrije svoje točne osobne podatke. Ime, prezime i adresa su neophodna stavka koju moraju proslijediti dostavnoj službi radi dostave; broj mobitela je većinom obavezan radi lakšeg preuzimanja paketa. Mail adresa (iako neobavezna) se većinom koristi kao kanal obavijesti o statusu paketa: „Potvrda narudžbe“, „Vaša narudžba je poslana.“, „Pratite svoj paket“. Podaci koji se koriste za izradu računa: Ime, prezime...

- korištenje internetske stranice (uključujući web shop) – pomoću kolačića i ostalih alata za praćenje dobiva se informacija o navikama i načinu korištenja web stranice.

- direktna prodaja – prilikom zaprimanja narudžbe, kroz prodajni proces se ponekad pojavljuje radni nalog – interni dokument kojeg popunjava prodavač i u koji upisuje podatke kupca i na kraju u znak ovjere daje kupcu na potpis. Mogući podaci: ime, prezime, telefon, mail adresa, kućna adresa, potpis... Kao mogućnost postoji i snimanje prodajnog prostora kojeg kupci posjećuju. Videozapis se također smatra osobnim podatkom.

- telefonska prodaja – ista vrsta podataka kao i u slučaju direktne prodaje, samo bez potpisa, a podatak o ispitaniku koji se može skupljati je eventualno glas i sadržaj razgovora – u slučaju snimanja poziva.

- prodaja putem maila ili ostalih kanala – Facebook, chat...

b) podaci koje poduzeće obrađuje od svojih dobavljača

Poduzeća koja se bave prodajom uglavnom imaju i dobavljače. Princip analize osobnih podataka može biti isti kao i kod analize podataka kupaca, uz sitne izmjene.

Primjer u praksi:

Bikko d.o.o. (prodaja dekorativnih predmeta) posluje s više od 30 dobavljača u inozemstvu i tuzemstvu. Spektar podataka koje skuplja o dobavljačima je vrlo širok. Jedan dobavljač ima više zaposlenika s kojima nabava komunicira, pa je proporcionalno

i veći broj podataka. - podaci o poduzeću unutar ERP sustava; naziv dobavljača, ime i preizime voditelja prodaje, broj telefona, broj mobitela, mail adresa. Osim podataka o osobama, spremaju se i opći podaci o poduzeću: naziv poduzeća, sjedište, broj računa, OIB pravne osobe. Podaci o pravnim osobama su javni i dostupni i ne smatraju se osobnim podatkom, no podaci o fizičkim osobama unutar poduzeća podliježu GDPR uredbi.

- susreti uživo s dobavljačima – eventualno snimanje prostora u kojima je sastanak ili audio zapis razgovora (diktafon, snimanje putem mobitela) kao podsjetnik na obavljene razgovore.

- telefonski razgovori s dobavljačima – snimanje poziva upućenih prema dobavljačima ili obrnuto, pohranjivanje razgovora na disk ili cloud.

c) podaci koje poduzeće skuplja od svojih zaposlenika

Zaposlenici su dio strukture i poslovanja poduzeća stoga je neizbježno sakupljati osobne podatke o njima. Organizacija vodi evidenciju o svojim zaposlenicima i članovima njihovih obitelji na više razina. Interna razina obuhvaća osnovne i proširene podatke, a na eksternoj razini se obrađuju podaci vezani uz isplatu plaća i ostalih prava (računovodstva). Ovaj dio GAP analize zahtjeva osvrt osobe zaposlene u ljudskim potencijalima i/ili administratora. Bikko d.o.o. dobiva račune od službenih brojeva zaposlenika i raspolaže s ispisom poziva.

Primjer u praksi:

Bikko d.o.o. zapošljava sedam zaposlenika. Osoba zaposlena na radnom mjestu administratora vodi evidenciju o svakom zaposleniku u elektroničkom i tiskanom obliku. Poduzeće skuplja i ostale osobne podatke: informacije o lokaciji, video nadzor i primanje kopije elektroničke pošte.

- tiskani oblik – najčešće se sastoji od dosjea zaposlenika koja pak sadrži razne dokumente: životopis, PK kartica, kopije diploma kao dokaz o završenom obrazovanju, kopije dokumenata o završenim tečajevima, potvrda o mirovinskom statusu, broj ibana, itd. Osim ovih podataka, poduzeće svojem eksternom računovodstvu prosljeđuje elektroničke podatke o zaposleniku: ime, prezime, adresa, IBAN, OIB, datum rođenja, ugovor o radu, stručna sprema, zadnje završeno školovanje. Razlog zbog kojeg ovi podaci bivaju proslijeđeni trećoj strani su isplate plaća.

- matična knjiga radnika – sličan dokument dosjeu zaposlenika, no vodi se u Excel tablici, a stavke koje sadrži su: ime, prezime, adresa, oib, način zaposlenja: određeno – neodređeno, datumi sklapanja i isticanja ugovora.

- lokacijske informacije – ugradnja GPS-a u službene automobile pomoću kojih poduzeće prati kretanje vozila, u svakom trenutku mogu otkriti mjesto na kojem se zaposlenik nalazi.

- praćenje komunikacije – direktor prima kopiju službenih mailova zaposlenika, a na računalima se bilježi povijest pretraživanja uz pohranjivanje na cloud. Mjesečni račun za službeni mobitel sadrži i ispis poziva i podatke o potrošnji.

- video nadzor – poslovni prostori su pokriveni kamerama i snimaju djelatnike na radnom mjestu – prodajno mjesto, uredi, zajedničke prostorije: kuhinja i soba za sastanak.

- podaci o članovima obitelji zaposlenika - broj djece, ime i prezime djeteta, adresa prebivališta, broj zdravstvenog osiguranja djeteta i rodni list. Ovi podaci se pohranjuju radi ostvarivanja određenog prava kako što je isplata prigodnih godišnjih darova/dar za dijete.

4.2.2. Temelji obrade podataka (zakonska osnova)

GDPR nalaže pohranjivanje i obradu samo neophodnih podataka. Svaki tuđi osobni podatak kojim se koristimo mora imati zakonsku osnovu ili privolu.

„Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihova prikupljanja.„ (Članak 37. Ustav Republike Hrvatske)

Nakon što je utvrđena količina i vrsta osobnih podataka koja se obrađuje u organizaciji, potrebno je utvrditi razlog zbog kojeg je podatak prikupljen, imajući na umu da se svaki podatak koji ne služi jednoj od ovih svrha opisanih u Općoj uredbi o zašiti podataka mora prestati prikupljati:

„a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više potrebnih svrha

b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora

c) obrada je nužna radi poštovanja pravnih obaveza voditelja obrade

d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe

e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade

f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, pogotovo ako je ispitanik dijete.„

(Uredba EU 2016/679, poglavlje 2, članak 6.)

Za svaku podjelu ispitanika se izrađuje tablicu u koju je potrebno upisati temelj obrade, a u slučaju izostanka osnove, poduzeće nije ovlašteno prikupljati određene podatke (bez privole ispitanika).

Vrsta ispitanika	Osobni podaci	Izvor podataka	Razlog obrade	Zakonski okvir
Zaposlenik/ca	Ime i prezime	Zaposlenik/ca	Ugovor o radu Isplata plaća	Zakon o radu Zakon o porezu na dohodak Pravilnik o porezu na dohodak
	OIB			
	Datum rođenja			
	Adresa			
	Državljanstvo			
	Brojevi mirovinskog i zdravstvenog osiguranja			
	IBAN			
	Podaci o trajanju radnog vremena			
	Završeno obrazovanje			

Tablica 1: Primjer jednostavnog ispitivanja temelja obrade podataka

4.3. Procjena rizika

Procjenom se dobivaju informacije o ranjivim točkama – na kojim mjestima može doći do povrede osobnih podatka, koje točke su posebno rizične i izložene eventualnim tužbama građana i kojim segmentima treba posvetiti veću pažnju, a pritom i edukaciju zaposlenika. Javno su dostupni razni prijedlozi formulara koji služe procjeni rizika. Forma i sadržaj nisu zakonski propisani, dokument služi kao pomoćni formular u implementaciji GDPR-a, pružajući smjernice radnoj skupini koja je zadužena za provedbu.

Sadržaj formulara se može modificirati prema potrebama poduzeća i vrsti podatka s kojima organizacija upravlja. Primjer dijela formulara autora Božića, preuzet s mrežnih stranica Ostendo Consulting poduzeća (https://www.ictbusiness.info/kolumne/gdpr-vaznost-procjene-rizika) :

Opis zahtjeva	Odgovor
Možete li dokazati da ste dobili odgovarajuću privolu za svaku obradu gdje je to potrebno (primjer, možete li dokazati za koje vam je obrade koja osoba kada dala privole)?	☐
Jeste li uspostavili sustav upravljanja zaštitom podataka koji osigurava dokaze o usklađenosti svih vaših obrada osobnih podataka sa zahtjevima Uredbe (članak 24. paragraf 1 Uredbe)?	☐
Jeste li prilagodili svoje procese provjere sigurnosti novim zahtjevima članka 32 Uredbe? Konkretno, da li ste uspostavili procese zaštite podataka temeljene na procjeni rizika koja u obzir uzima prirodu, opseg, kontekst i svrhu obrada, učinkovitost postojećih sigurnosnih kontrola i rizik vjerojatnosti negativnog događaja, te ozbiljnost utjecaja takvog događaja na prava i slobode pojedinca?	☐
Jeste li uspostavili učinkoviti sustav upravljanja koji osigurava redovitu provjeru, procjenu i poboljšavanje sigurnosnih mjera za zaštitu osobnih podataka?	☐
Koristite li kod zaštite pohranjenih osobnih podataka mjere poput pseudonimizacije ili enkripcije, kako bi ih zaštitili od neovlaštenog pristupa i obrade?	☐
Jeste li identificirali potrebu za provođenjem procjene učinka na	☐

zaštitu osobnih podatka (DPIA) u nekim svojim proizvodima (procesima, obradama) ?	
Je li vaša organizacija uspostavila učinkovitu metodu (proces, proceduru) za identifikaciju potrebe za provođenjem procjene učinka na zaštitu osobnih podataka (DPIA)?	☐
Jeste li definirali i dokumentirali odgovarajuću metodologiju procjene učinka na zaštitu osobnih podataka (DPIA) u vašoj organizaciji?	☐
Jeste li testirali svoju metodologiju procjene utjecaja na zaštitu osobnih podataka (DPIA)?	☐

Tablica 2 – pomoćni formular za procjenu rizika

4.4. Kreiranje dokumentacije za provedbu

GAP analiza i procjena rizika rezultiraju jasnijim pogledom na situaciju. S obzirom na to da se kroz prijašnje dvije faze istaknula vrsta osobnih podatka koji fluktuiraju unutar poduzeća i izračunati rizici povrede zaštite osobnih podataka, logično je kreirati dokumentaciju na koji će se oslanjati proces implementacije GDPR-a. Faza počinje produciranjem obrazaca kao što su:

- Evidencija aktivnosti obrade osobnih podataka
- Privola (suglasnost za obradu osobnih podataka)
- Odluka o imenovanju službenika za zaštitu podataka
- Izvješće o imenovanju službenika za zaštitu podataka
- Izvješće o aktivnostima službenika za zaštitu podataka
- Izvješće o povredi osobnih podataka
- Obavijest ispitaniku o povredi njegovih osobnih podataka
- Odluka o proceduri upravljanja zamolbama i životopisima u svrhu zaposlenja
- Interni pravilnik poduzeća o postupanju s osobnim podacima
- Pravilnik o izradi

Sadržaj evidencije aktivnosti obrade osobnih podataka:

Strukturirana tablica prikazuje podatke o osobnim podacima, izvora osobnih podataka, svrhu obrade, načine obrade, mjesto obrade, mjesto pohrane, rok čuvanja, primatelja, zakonitost obrade, mjere kontrole i prava ispitanika.

Odluka/izvješće o imenovanju službenika za zaštitu podataka

U odluci organizacija kao voditelj obrade i izvršitelj obrade imenuje službenika za zaštitu podataka i navodi obaveze koje ovo mjesto zahtjeva; informiranje, savjetovanje voditelja obrade ili zaposlenika, kontrola nad provedbom uredbe u poslovanju organizacije, surađivanje s AZOP-om. Naglašava se i obaveza tajnosti i povjerljivosti, koja traje i nakon što je osoba prestala obavljati dužnost službenika za zaštitu podataka.

Izvješće o imenovanju službenika za zaštitu podataka (DPO) je dokument kojeg organizacija dostavlja AZOP-u kako bi agenciju obavijestila o postojanju DPO-a. Formular zahtjeva samo osnovne podatke: ime voditelja obrade, adresu, podatke o DPO-u; ime i prezime, kontakt podatke i mjesto rada.

Izvješće o povredi osobnih podataka i Obavijest ispitaniku o povredi njegovih podataka

Organizacija bi trebala ulagati veliki trud i neprestano kontrolirati procese koji dovode do obrade osobnih podatka, no ako unatoč tome dođe do povrede, poduzeće je dužno obavijestiti oštećenog ispitanika i agenciju o okolnostima i informacijama o vrsti štete. Ispisuju se podaci o voditelju obrade (sjedište, oib), ime i prezime službenika za zaštitu podataka (a ako DPO ne postoji, podaci druge kontakt osobe), opis nastale povrede podataka i vremenski okvir nastale povrede (kada se dogodila, kada je voditelj obrade saznao za istu), koje su vjerojatne posljedice i koje mjere voditelj obrade poduzima kako bi zaštitio ispitanika i riješio nastali problem. Izvješće o povredi osobnih podataka prima AZOP, a Obavijest ispitaniku o povredi njegovih podataka se šalje osobi koja je nesvjesno pretrpjela štetu prilikom pohranjivanja ili obrade osobnih podataka.

Interni pravilnik poduzeća o postupanju s osobnih podacima

Pravilnik kojim se formalno regulira obaveza transparentnog ophođenja zaposlenika u vezi obrade osobnih podataka. Nije obavezan, no smatra se temeljnim internim aktom na kojeg se vežu ostali formulari. Svrha mu je navesti izvor (zakon), definirati osnovne pojmove kao što su: osobni podaci, ispitanik, voditelj obrade, službenik za obradu osobnih podataka, sustav pohrane, privola, primatelj, treća strana... U nastavku dokumenta može biti pojašnjeni propisani način postupanja prema zakonu; transparentnost, točnost i zaštita, zakonitost obrade (navesti slučajeve) i prava ispitanika.

4.5. Edukacija zaposlenika

Ispravnu primjena i transparentnost i poštivanje GDPR-a ovisi o spremnosti i želji zaposlenika koji sudjeluju u obradi podataka. Nakon pripreme svih materijala, obrazaca i izvještaja, potrebno je educirati kadar koji će u svakodnevnom ili povremenom kontaktu s kupcima primjenjivati načela uredbe.

4.5.1. Metode edukacije:

- Slanje materijala mail-om zaposlenicima – podjelu izričito tiskanog materijala ne možemo smatrati sigurnom zbog mogućeg gubitka. Najkasnije dva dana prije prezentacije, svaki zaposlenik bi trebao dobiti na pregled materijale i najavu, odnosno sadržaj prezentacije po točkama.
- Kreiranje baze podataka sa svim temeljnim informacijama i QA upitnikom – unaprijed odgovorena često postavljana pitanja mogu uštedjeti vrijeme korisniku i pružatelju usluge. Baza materijala i QA mogu biti postavljeni na web stranici poduzeća, vidljivo samo za zaposlenike, zaštićeno korisničkim imenom i lozinkom.
- Održavanje powerpoint prezentacije s obaveznim dijelom za razgovor - korištenje razumljivog jezika, prilagoditi prezentaciju svakoj prisutnoj osobi. Poticati prisutne na postavljanje pitanje i kritičko promišljanje.
- Fizička podjela materijala zaposlenicima – obrasci koji prate prezentaciju i olakšavaju slušatelju praćenje i shvaćanje suštine.
- Webinari – pregledavanje prethodno snimljenog video i audio sadržaja na internetu s ciljem educiranja
- Poticanje na vlastito istraživanje – nepredvidivost poslovanja i primjena novih zakonskih okvira sigurno će stvoriti situacije koje možda nisu pokrivene planom. Zaposlenike treba uputiti na kanale koji im mogu pružiti pravodobne i istinite informacije pomoću kojih sami kreiraju ispravna rješenja.

4.6. Testiranje i provedba

Razdoblje testiranja traje beskonačno i djeluje simultano s procesom provedbe. Moguće je, da će se u nekoj situaciju pokazati da zaposlenici nisu dovoljno educirani ili se može dogoditi do sad neviđeni problem. Uredba je obavezna tek nešto više od pola godine i potrebno je dopustiti da prođe razdoblje u kojem će se na pravilan i jasan način tumačiti njezina svrha, zadaće i načini na koje je predviđeno rješavanje problema u praksi. Nesvakidašnje, iznimne situacije donose razne probleme u obradi podataka, a kad je nejasno što treba čini, organizacije ili ispitanici se obraćaju AZOP-u za mišljenja. Provedba podrazumijeva ispunjavanje obaveza organizacije: poštivanje prava ispitanika, zaštita podataka, transparentno ophođenje prema zakonitostima obrade i primjenjivanje svih stečenih znanja iz prethodnih faza. Mogući ishodi koji mogu utjecati na tijek implementacije: promjene u djelatnosti poduzeća – obrada drugačije vrste podataka, promjena vodstva, promjena DPO-a ili propust u GAP analizi ili procjeni rizika kojim se nije predvidio nastanak problema.

Konzultantske tvrtke kojima je primarna djelatnost savjetovanje organizacije i podrška prilikom implementacije nude i mogućnost obavljanja DPO-a kao vanjskog službenika. Prednosti angažiranja vanjskih suradnika dolazi do izražaja prilikom nejasnih situacija u kojima konzultanti mogu biti korisni savjetnici zbog već sličnih iskustva i imaju ulogu membrane između organizacije i AZOP-a.

5. Poteškoće u poslovanju

Uredba ne opisuje stvarne događaje i primjere koji će se dogoditi u normalnom poslovnom okruženju, već je poslovni subjekt dužan sam tumačiti i primjenjivati uredbu na svakodnevne situacije. Važno je naglasiti odnos zakona, lex specialis - lex generalis – zakon koji temeljitije obrađuje određenu temu ima veću pravnu snagu od zakona koji ima opće značenje. U praksi je potrebno pregledati nadležan zakon, ovisno o slučaju koji se radi, npr. Zakon o medijima uspoređujemo s GDPR-om.

Fotografiranje događaja

Fotografija je osobni podatak, identifikator – prikaz osobe koja se može izravno prepoznati. Ova stavka donosi mnoge poteškoće u poslovanju u marketinškom odjelu poduzeća. Zaista je teško provoditi promociju eventa ako se na društvenoj mreži ne može objaviti fotografija važnog poslovnog događaja s nepoznatom masom ljudi. Za svaku fotografiju na kojoj postoji mogućnost identifikacije osobe koja prisustvuje događaju, mora postojati privola (koju organizacija mora moći dokazati), što bi značilo da je potrebno priskrbiti pisanu suglasnost. Poduzeća koriste programe za obradu fotografija pomoću kojih obično zamute osobe na fotografiji, odnosno anonimiziraju sadržaj, a u prvi plan stavljaju neki predmet.

Evidencija radnog vremena

Agencija je izdala mišljenje kojim komentira naum KBC Zagreba za vođenjem kontrole radnog vremena otiskom prsta. Potrebno je prikupiti privole zaposlenika (svaku zasebno) i objasniti u koju svrhu će se njihovi biometrijski podaci obrađivati i pohranjivati, pritom ne stvarajući pritisak. Preporuka je prilagoditi način evidencije manje invazivnoj metodi, kao što je na primjer upotreba magnetske kartice i fizičko zapisivanje dolazaka i odlazaka u knjigu evidencije.

Snimanje poslovnog prostora

Obavezno je jasno i čitko postavljanje obavijesti o snimanju prostora kojim se ispitanik kreće. Snimati se smiju samo zajedničke prostorije (nije dopušteno postavljanje videokamera u svlačionicama, toaletima...). S obzirom na GDPR uredbu, agencija preporučuje izradu natpisne table koja osim obavijesti o snimanju sadrži i podatke o

voditelju obrade i kontakt podatke. Reducirani opseg privatnosti na radnom mjestu snose zaposlenici čiji su pokreti i radnje snimane bez osnove, odnosno prema mišljenju AZOPA, ako su radne prostorije snimane, a zaposlenici ne obavljaju rizične poslove zbog kojih bi snimanje video nadzora bilo neophodno. U ovom slučaju, agencija preporučuje drugačiju metodu nadzora. Videozapisi se smiju čuvati najviše 6 mjeseci od nastanka materijala, a nakon toga ih treba trajno ukloniti. Zapisi je dopušteno čuvati duže ako je u tijeku sudski postupak ili u slučaju uloge dokaznog materijala ili javnog interesa.

6. Nacrt za provedbu istraživanja

6.1. Uvod

Uvođenjem GDPR uredbe nastala je pomutnja, ponajviše u poduzećima koja nisu primila bilo kakvu vrstu edukacije, niti su imali saznanja što im je činiti i kako prilagoditi poslovne procese. Povod za pisanje diplomskog rada na temu „Implementacija GDPR-a u malim poduzećima“ je želja za objedinjenje informacija o provedbi GDPR na jednom mjestu, a rad može poslužiti kao informativni priručnik za sve zainteresirane.

6.2. Cilj istraživanja

Cilj istraživanja je steći dojam o razumijevanju ispitanika o svrsi GDPR uredbe. U prvom dijelu istraživanja će se ispitivati informiranost javnosti o temi. Drugi dio će poslužiti kao preslika osjećaja sigurnosti građana, odnosno stupnju sigurnosti kojeg GDPR uzrokuje kod ispitanika.

6.3. Problem

Nakon četiri godine pregovora u vezi GDPR – General Data Protecting Regulation ili Opće uredbe o zaštiti osobnih podataka, ona je stupila na snagu 25.5.2018. godine. Pripremno razdoblje je bilo nedovoljno „oglašeno“, a i nakon usvajanja prijedloga o implementaciji ove uredbe u Zakon, nedostajalo je edukacija i više javnosti dostupnih informacija.

6.4. Istraživačko pitanje

Imaju li građani predodžbu o značenju GDPR uredbe? Jesu li uopće zainteresirani saznati što se događa s njihovim podacima? Stavljen fokus na osjećaj sigurnosti, koja je posljedica utjecaja GDPR-a, odnosno osjećaju li se građani sigurnije?

6.5. Hipoteze i varijable

H1: Javnost nije dovoljno upoznata s GDPR uredbom

H2: Ispitanici ne osjećaju veći stupanj sigurnosti na internetu zbog implementacije ove uredbe.

H3: Građani nisu zainteresirani saznati što se događa s njihovim podacima.

Nezavisne varijable – rod, dob, vrsta obrazovanja i ostala socio-demografska pitanja.

Zavisne varijable – pitanja o informiranosti o GDPR-u, vrsta dosadašnjeg iskustva, vrijeme kad je osoba saznala za GDPR, stavovi i vrednovanja ispitanika, osjećaj sigurnosti kao posljedica utjecaja GDPR-a.

6.6. Način provedbe istraživanja i metodologija:

Instrument istraživanja je anketni upitnik. Proces anketiranja će započeti 16. veljače i trajati do 25. veljače 2019. godine. Metoda anketiranja je planirana za provedbu putem Google obrasca. Vrsta istraživanja je kvantitativne naravi, temelji se na ispitivanju postavljenih tvrdnji, odnosno hipoteza.

6.7. Planiranje obrade podataka

S obzirom na to da se anketa provodi putem Google obrasca, nakon popunjenja zadovoljavajućeg broja anketa, obrada će se vršiti importiranjem podataka u Excel. Kad svi podaci budu obrađeni i izrađeni grafovi, slijedi deskriptivni dio s detaljnim tumačenjem dobivenih informacija.

6.8. Planirane vrste uzorka

Namjerni uzorak**:**

- korištenje prigodnog uzorka – u uzorak se biraju članovi populacije koji su pri ruci, npr. studenti diplomskih studija Sveučilišta Sjever (izvanredni, dva smjera), kolege s radnog mjesta, poznanici. Razlog odabira ovog uzorka: veći broj popunjenih anketa u

kraćem vremenskom roku zbog osobne povezanosti istraživača s odabranim članovima populacije.

- korištenje uzorka lavine ili lančane reakcije – uzorak „poznavatelja“, od nekoliko članova populacije se traži da anketni upitnik proslijede osobama za koje smatraju da su prigodni za ispitivanje.

Slučajni uzorak:

- Jednostavni slučajni uzorak

Nivo istraživanja – mikro nivo – odabrani pojedinci, članovi kućanstva ili grupa osoba po odabiru istraživača.

6.9. Ograničenja istraživanja

Istraživanje se ne može shvatiti kao opće mjerilo informiranosti javnosti o GDPR uredbi. S obzirom na pretpostavku da će ispitanici većinom biti mlađa, visoko obrazovana populacija, istraživanje bi ciljano trebalo provesti i među raznolikim dobnim skupinama i s različitim stupnjem obrazovanja. Istraživanje može poslužiti kao preliminarno.

6.9.1. Dosadašnja istraživanja

Vrlo je malo istraživanja na ovu temu (pronađeno samo 3), s obzirom na to da je tema zaista aktualna, više su se oslanjala na analizu GDPR-a s pravnog stajališta.

Naziv rada	Autor	Vrsta rada	Ustanova	Predmet istraživanja
Utjecaj GDPR standarda o zaštiti podataka na informacijske sustave	Dominik Bilušković	Završni rad	Sveučilište J. J. Strossymayera u Osijeku, Ekonomski fakultet u Osijeku	Usporedba GDPR-a sa Zakonom o zaštiti podataka
Analiza opće uredbe o zaštiti	Nevena Arar	Diplomski rad	Sveučilište u Zagrebu, Pravni fakultet	Analiza GDPR-a s pravnog aspekta

podataka				(značajke, koristi...)
Utjecaj Opće uredbe o zaštiti osobnih podataka na digitalni marketing	Martina Blažević	Diplomski rad	Sveučilište J. J. Strossymayera u Osijeku, Ekonomski fakultet u Osijeku	Istraživanje - analiza primjene GDPR-a u telekomunikacijskom poduzeću

Tablica 3: Dosadašnja istraživanja vezana uz GDPR

7. Prikaz istraživačkih pitanja

Zaštita osobnih podataka

Ljubazno vas molim da popunite anonimni anketni upitnik. Rezultati će biti analizirani u diplomskom radu na smjeru "Odnosi s javnostima". Kratica GDPR u anketi označava Uredbu o zaštiti osobnih podataka. Molim vas, na pitanja odgovarajte zaista iskreno, kako bi pridonijeli što točnijim rezultatima istraživanja.

*Obavezno

Kojeg ste roda? *

- Ž
- M
- Ne želim se izjasniti

Koliko imate godina? *

- 18 - 23
- 24 - 29
- 30 - 35
- 36 - 41
- više od 41

Odaberite razinu obrazovanja (završenu ili u tijeku): *

- Srednja škola
- Preddiplomski studij
- Diplomski studij
- Doktorski studij

Jeste li zaposleni? *

- Jesam
- Nisam

U kojoj ste mjeri upoznati s uredbom GDPR (Opća uredba o zaštiti osobnih podataka)? *

- Nisam upoznat/a
- Površno sam upoznat/a

- Djelomično sam upoznat/a
- Vrlo dobro sam upoznat/a
- Detaljno sam upoznat/a

Kada ste prvi put čuli za GDPR? * #

- Od dana stupanja na snagu (25.5.2018.)
- Prije više od godinu dana
- Prije više od dvije godine
- Nisam čula/čuo za GDPR (anketa završava ako osoba nije čula za GDPR)

GDPR određuje čuvanje mojih osobnih podataka u obliku koji omogućuje identifikaciju: *#

- Samo 6 mjeseci i to isključivo u svrhe radi kojih se osobni podaci obrađuju
- Godinu dana u svrhe radi kojih se osobni podaci obrađuju
- Onoliko koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju
- Nisam sigurna/siguran

Osobni podaci koji su zaštićeni GDPR-om su: *

- Ime i prezime, email adresa, datum rođenja i OIB
- Ime i prezime, email adresa, OIB, IP adresa, podaci o obrazovanju, kreditno zaduženje
- Ime i prezime, email adresa, datum rođenja, OIB, biometrijski podaci, kreditno zaduženje, podaci o zdravlju, podaci o seksualnoj orijentaciji
- Podaci koji otkrivaju moj identitet ili se mogu povezati sa mnom
- Nisam sigurna/siguran

Prema GDPR-u, moji osobni podaci se smiju obrađivati samo ako im dam privolu (dopuštenje) za to: *#

- Da
- Ne
- Nisam sigurna/siguran

Kome biste se obratili ako bi netko obrađivao vaše podatke na nezakonit način? *#

- Nadležnoj policijskoj upravi

- Agenciji za zaštitu osobnih podataka
- Udruzi za zaštitu prava potrošača
- Medijima

Koliko ste upoznati s količinom i vrstom podataka koje web "kolačići" prikupljaju o vama? *

- Nisam upoznat/a
- Površno sam upoznat/a
- Djelomično sam upoznat/a
- Vrlo dobro sam upoznat/a
- Detaljno sam upoznat/a

Što se događa ako ne pritisnite ništa ili kliknete zatvori (X) prilikom prikazivanja prozorčića o korištenju kolačića (cookies)? *

- Prihvaćam prikupljanje informacija
- Smatram da se ništa ne događa jer sam ignorirao/la obavijest
- Pohranjivanje kolačića se ne primjenjuje na mom uređaju
- Nisam sigurna/siguran

U kojoj se mjeri slažete s navedenim tvrdnjama? *

	Uopće se ne slažem	Ne slažem se	Niti se slažem, niti se ne slažem	Slažem se	U potpunosti se slažem
Propisane kazne za nepoštivanje GDPR-a su prevelike	○	○	○	○	○
RH je na vrijeme krenula s pripremama za GDPR	○	○	○	○	○
RH je građanima pružila adekvatnu edukaciju	○	○	○	○	○
Javnost raspolaže s premalo informacija vezanih uz uredbu	○	○	○	○	○

Imate li naviku u postavkama pročitati koje podatke skupljaju društvene mreže o vama? *

- Da, zanima me
- Ponekad pročitam
- Ne, nije mi važno
- Ne koristim niti jednu društvenu mrežu

Ako čitate, koji je razlog čitanja?
(Samo za osobe koje su u prethodnom odgovoru odgovorile s A ili B)

- U aplikaciji / na web stranici mi je ponuđen pregled podatka koje prikupljaju
- Sam/a sam istraživao/la i prije GDPR uredbe
- Počela/počeo sam čitati nakon uvođenja GDPR uredbe

Ocijenite svoje dosadašnje iskustvo u vezi provođenja GDPR-a: *

- Pozitivno
- Negativno
- Neutralno

- Nemam iskustva

Na koji je način uvođenje GDPR-a utjecalo na vas? *

- Veću pozornost posvećujem sigurnosti mojih podataka
- Uopće nije utjecalo na mene
- Nisam sigurna/siguran

Osjećate li se sigurnije prilikom posjećivanja web stranica ili primanja newsletter-a nakon uvođenja GDPR uredbe? *

- Da
- Ne
- Nisam sigurna/siguran

Smatrate li da hrvatska poduzeća zaista provode GDPR? *

- Smatram da zaista provode
- Smatram da fiktivno provode
- Smatram da uopće ne provode

Jeste li ikad iskoristili pravo povlačenja privole za obradu podataka ili pravo zaborava? *

- Da
- Ne

Ako jeste, koji je bio razlog?
(Samo za osobe koje su u prethodnom odgovoru odgovorile s "DA")

- Nisam više željela/želio da određeno poduzeće raspolaže s mojim podacima
- Smatrala/smatrao sam da je svrha pohranjivanja mojih podataka završila
- Htjela/htio sam isprobati na koji način funkcionira povlačenje privole
- Postojala je mogućnost zlouporabe mojih podataka
- Ostalo

Ocjenama od 1-5 odredite u kojoj mjeri se slažete s navedenim tvrdnjama: *

	Uopće se ne slažem	Ne slažem se	Niti se slažem, niti se ne slažem	Slažem se	U potpunosti se slažem
GDPR je korisna uredba koja štiti moja prava	○	○	○	○	○
GDPR funkcionira loše u praksi	○	○	○	○	○
Na lakši način mogu privući svoju privolu za obradu podataka	○	○	○	○	○
Ova uredba je prisilila pružatelje usluga da pojačaju sigurnost korisnika	○	○	○	○	○
Poduzeća su ponovno zatražila dopuštenje za slanje newsletter-a	○	○	○	○	○
Nakon uvođenja GDPR-a nije se smanjio broj SPAM pošte	○	○	○	○	○
Ako primjetim nepravilnosti, jasnije mi je kako prijaviti problem	○	○	○	○	○
Vjerojatnost za krađu identiteta je ista kao i prije uredbe	○	○	○	○	○

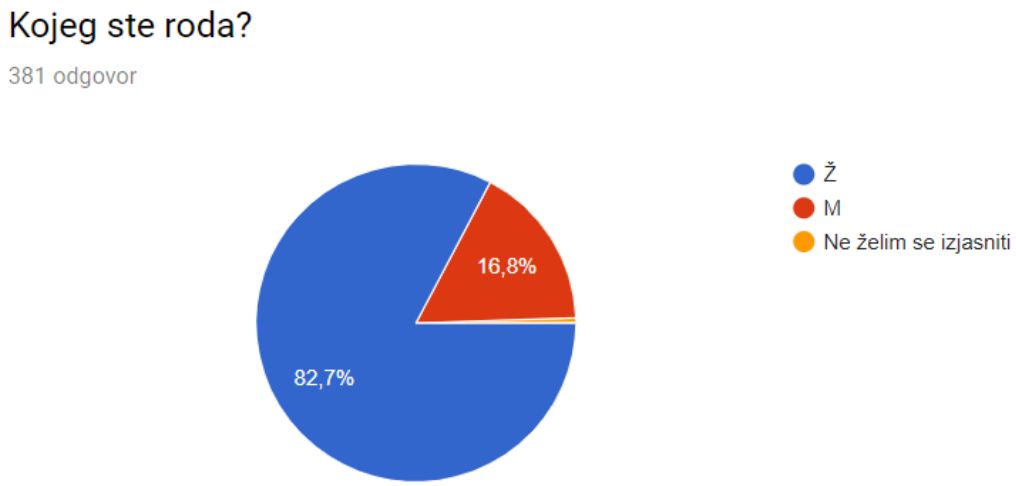
Jeste li primijetili pozitivne pomake u obradi osobnih podatka nakon uvođenja GDPR-a? *

- Apsolutno jesam
- Jesam, ali ima puno prostora za poboljšanja

- Nema drastičnog pomaka u sigurnosti podataka
- Nisam obraćao/la pažnju

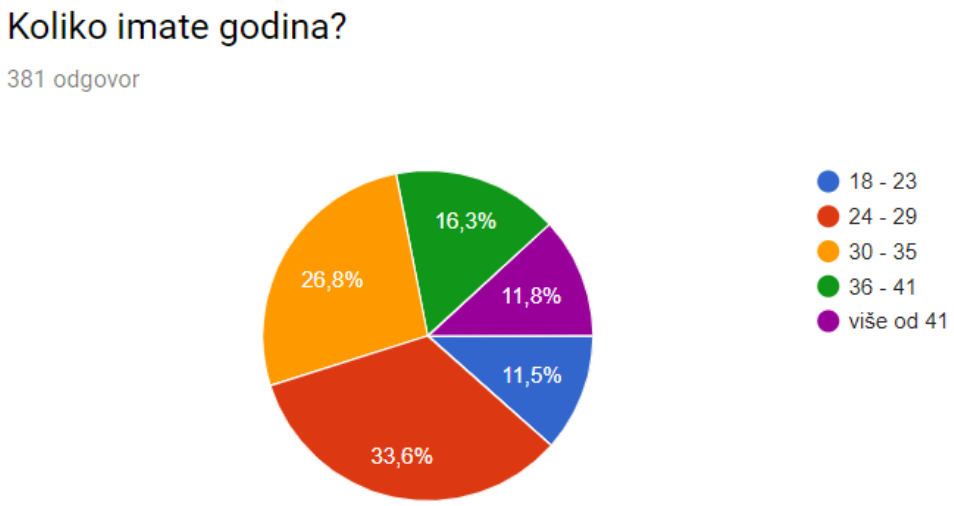
Pitanja označena ljestvama (#) su preuzeta iz zajedničkog seminarskog rada Čižmešija i Stepan (2018.)

8. Rezultati istraživanja



Grafikon 2: Omjer rodova

U ovom sociodemografskom pitanju očitujemo dane podatke o rodu ispitanika: od ukupno 381 ispitanih, većina je ženskog roda, 82,7 %, a 16,8 % muškog. Dvije se osobe (0,5 %) nisu željele izjasniti o rodnom opredjeljenju.

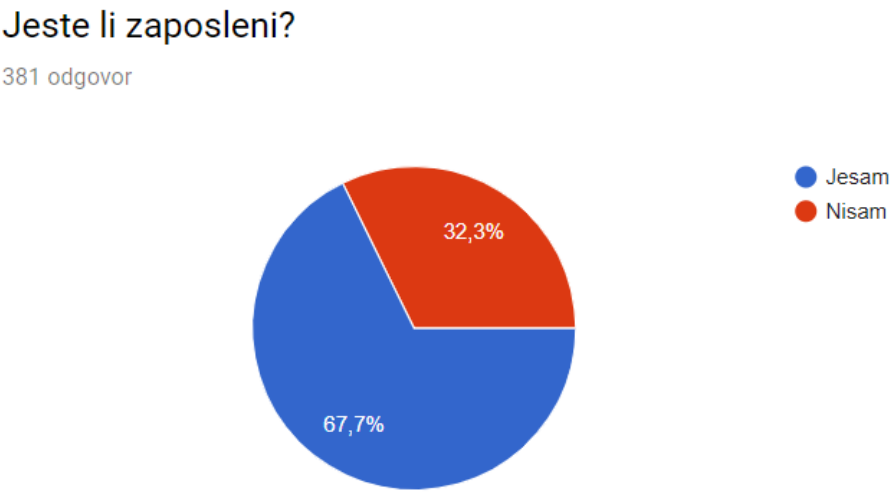


Grafikon 3: Dob ispitanika

Većina ispitanika ima 24-29 godina (33,6 %), zatim slijedi dobna skupina od 30-35 godine (26,8 %), druga po veličini je skupina od 36-41 s 16,3 %. Na kraju skoro pa podjednako zastupljene skupine najmlađe i starije populacije; 18-23 godine (11,5 %), 36-41 (11,8 %)

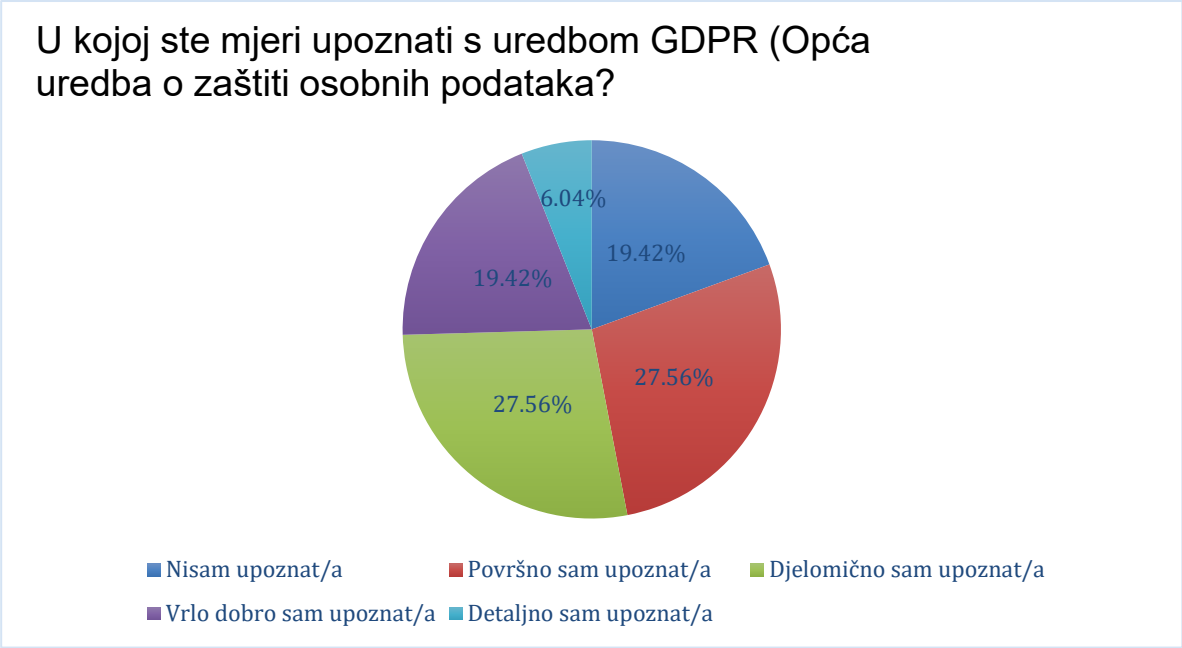
Grafikon 4: Razina obrazovanja

U pitanju "Odaberite razinu obrazovanja", većina visoko obrazovana s čak 54,3 %, postotak nastao zbrajanjem ispitanika koji su završili preddiplomski (23,9 %) , diplomski (28,6) i doktorski studij (1,8 %). Najniža navedena razina obrazovanja je zastupljena s 45,7 %.



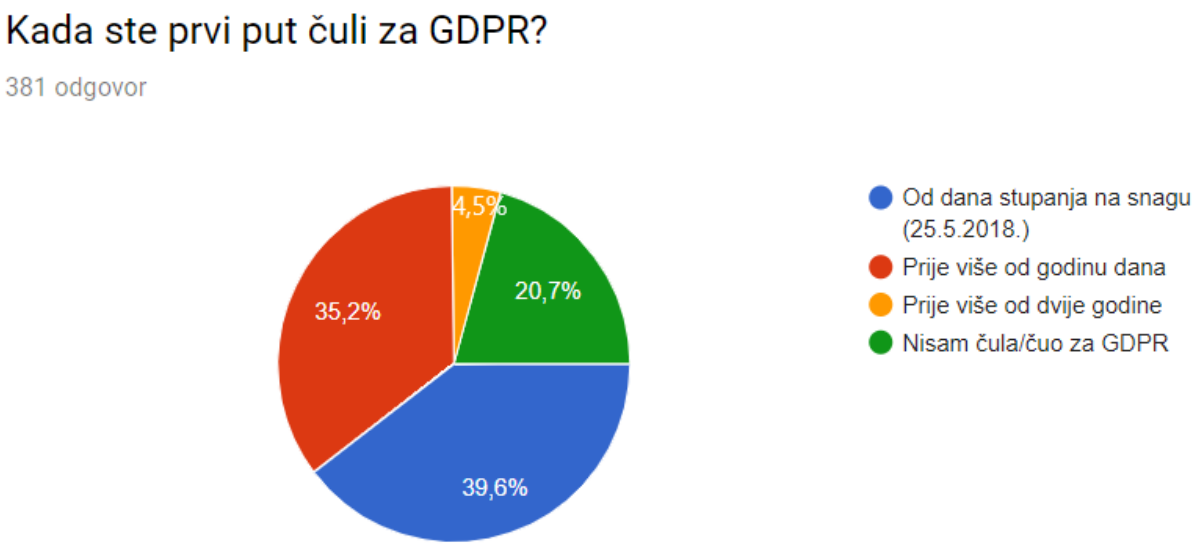
Grafikon 5: Zaposlenost

Većina ispitanika je na pitanje o statusu zaposlenosti odgovorila pozitivno (67,7%), a ostali su izjavili da su trenutno nezaposleni – 32,3 %.



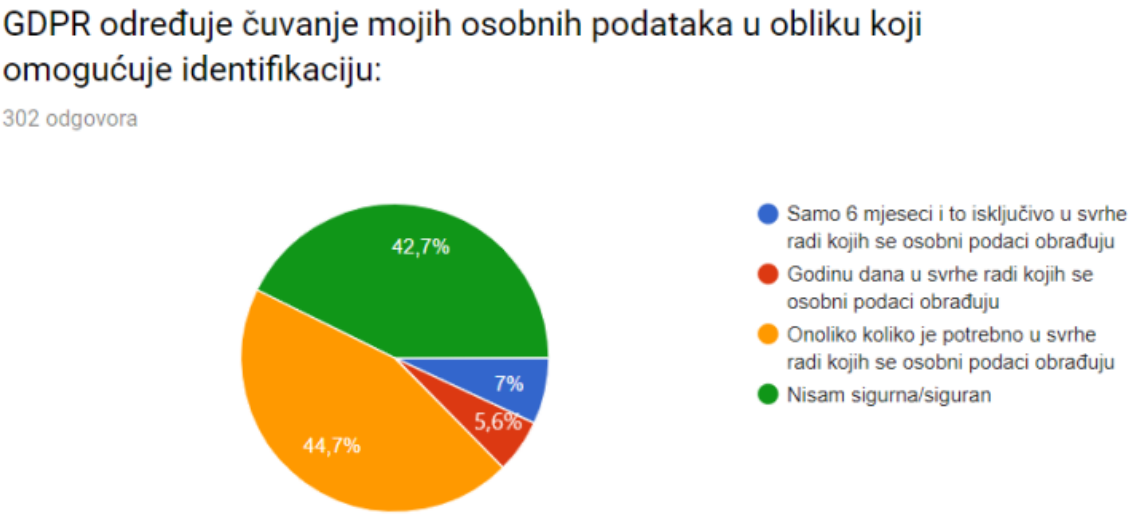
Grafikon 6: Mjera upoznatosti s GDPR-om

U pitanju "U kojoj ste mjeri upoznati s uredbom GDPR (Opća uredba o zaštiti osobnih podataka?" se od ispitanika tražilo da pomoću samoprocjene odrede stupanj informiranosti o uredbi. Narav pitanja je subjektivna. Podjednak broj odgovora zastupaju ponuđene opcije "Djelomično sam upoznat/a" i "Površno sam upoznat/a" s 27,56 %. "Detaljno sam upoznat/a" i "Vrlo dobro sam upoznat/a" također dijele isti postotak – 19,42 %, dok je samo 6,04 % osoba izjavilo da uopće nisu upoznati s terminom GDPR-a.



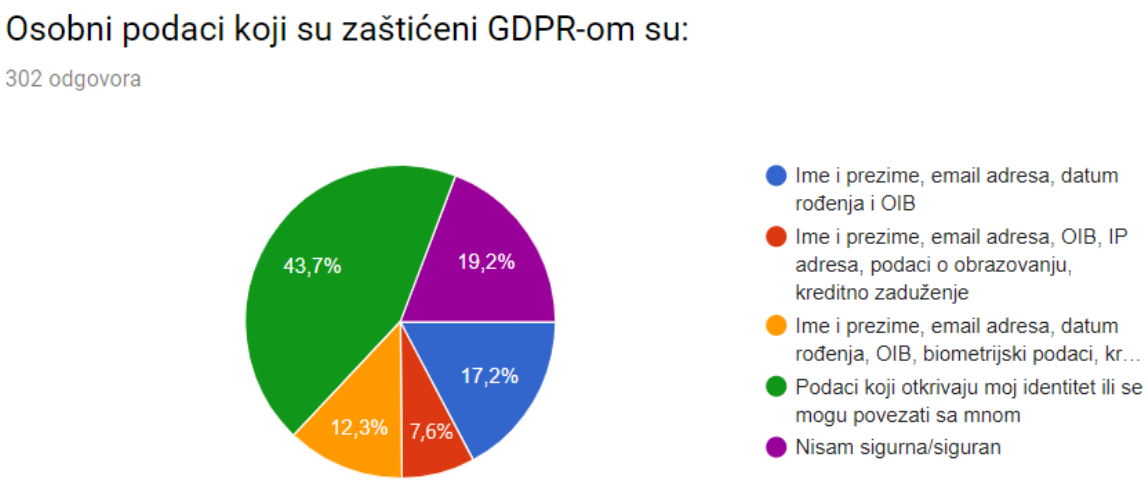
Grafikon 7: Prvi susret s pojmom GDPR-a

Većina ispitanik je na pitanje "Kada ste prvi put čuli za GDPR., odgovorila da su za termin saznali na dan stupanja na snagu (39,6 %), što možemo povezati s medijskim objava vezanim uz tu temu, druga najveća skupina je "Prije više od godinu dana" 35,2 %, a treća visoko zastupljena skupina je selektivna – za GDPR nije "čulo" čak 20,7 %,. Za ispitanike koji su izjavili da nisu čuli za GDPR je anketa završila, te jedino ta skupina nije nastavila upitnik zbog nemogućnosti davanja točnih odgovora na sljedeća pitanja. Posljednja po veličini je skupina koja je izjavila da su saznali za GDPR prije više od dvije godine.



Grafikon 8: Identifikacija

Početak dijela upitnika koji mjeri razinu upoznatosti javnosti s GDPR uredbom. Točan odgovor je "Onoliko koji je potrebno u svrhe radi kojih se osobni podaci obrađuju" – 44,7 %, što bi značilo da je većina ispitanika krivo odgovorila na pitanje ili nije znala odgovor. Čak 42,7 % ispitanika nije sigurno. Odgovor "Samo 6 mjeseci i to isključivo u svrhe radi kojih se osobni podaci obrađuju" je odabralo 7 %.



Grafikon 9: Vrsta podataka zaštićenih GDPR-om

Ispitanici su trebali navesti koji su osobni podaci zaštićeni GDPR-om, a odgovor "Podaci koji otkrivaju moj identitet ili se mogu povezati sa mnom" predstavlja točan odgovor (43,7 %), dok više od polovice ispitanih nije znala navesti vrstu podataka: 19,2 % ispitanika nije sigurno, 17,2 % smatra da se radi o imenu, prezimenu, email adresi, datumu rođenja i OIB-u, 7,6 % smatra da je točan odgovor ime i prezime, email adresa, IP adresa, podaci o obrazovanju, kreditno zaduženje. Dio ispitanika; 12,3 % se odlučilo za odgovor u kojem je navedeno da se radi o imenu, prezimenu, email adresi, datumu rođenja, OIB-u, biometrijskim podacima, kreditnom zaduženju.

Grafikon 10: Privola

Čak 88,1 % ispitanika je krivo odgovorilo na pitanje "Prema GDPR-u, moji osobni podaci se smiju obrađivati samo ako im dam privolu (dopuštenje) za to.", odgovorivši "Da". Točan odgovor "Ne" je pružalo samo 4 % ispitanika, dok ih 7,9 % posto nije bilo sigurno.

Grafikon 11: Nezakonita obrada

"Kome biste se obratili ako bi netko obrađivao vaše podatke na nezakonit način?", pitanje postavljeno na principu točnog i netočnih odgovora; većina ispitanika (68,5 %) je odabrala

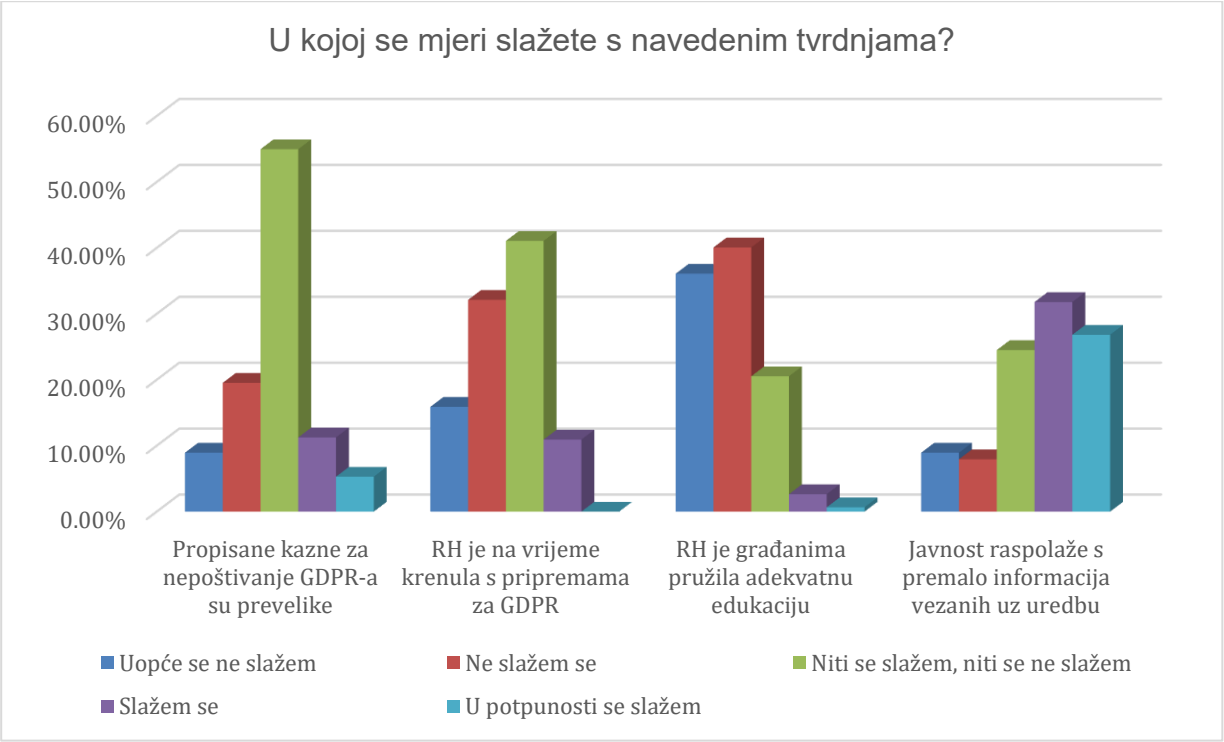
točan odgovor "Agenciji za zaštitu osobnih podataka", sljedeća skupina po redu je "Nadležnoj policijskoj upravi" što predstavlja krivi odgovor (26,8 %), a ostatak odgovora je slabo zastupljen; 3,3 % ispitanih bi se obratilo Udruzi za zaštitu potrošača, a samo 1,3 % ispitanih se odlučilo za pomoć obratiti medijima.

Grafikon 12: Upoznatost s prikupljanjem kolačića

Pitanje "Koliko ste upoznati s količinom i vrstom podataka koje web kolačići prikupljaju o vama?" je temeljeno na subjektivnoj samoprocjeni ispitanika, samo 13 % ispitanih je upoznato vrlo dobro (12 %) i detaljno (1 %), dok ostatak tvrdi da su površno upoznati (31 %), zatim djelomično upoznati (29 %). Čak 27 % ispitanih uopće nije upoznato s tematikom.

Grafikon 13: Obavijest o prikuljanju kolačića

Više od polovice ispitanika je dalo krivi odgovor ili nisu znali dati odgovor (21,9 %) na pitanje "Što se događa ako ne pritisnite ništa ili kliknete zatvori X prilikom prikazivanja prozorčića o korištenju kolačića (cookies)?" Njih 25,2 % smatra da se ne događa ništa jer su ignorirali obavijest, 19,2 % misli se pohranjivanje kolačića ne primjenjuje na njihovom uređaju. Otprilike trećina ispitanika (33,8 %) je odabrala točan odgovor "Prihvaćam prikupljanje informacija."



Grafikon 14: Slaganje s tvrdnjama

Pitanje je postavljeno pomoću izjavnih rečenica koje zahtijevaju izjašnjavanje ispitanika o stupnju slaganja ili neslaganja s izjavom i to: uopće se ne slažem, ne slažem se, niti se slažem, niti se ne slažem, slažem se i u potpunosti se slažem.

Na izjavu "Propisane kazne za nepoštivanje GDPR-a su prevelike", većina je dogovorila da se niti slažu niti ne slažu (54,97 %).

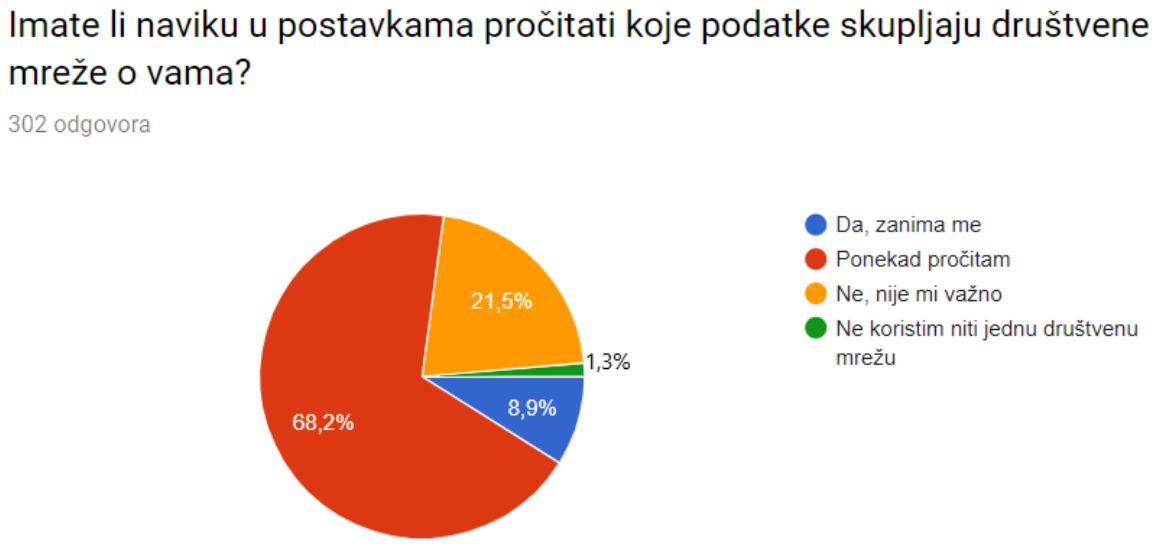
Najviše ispitanika je na izjavu "RH je na vrijeme krenula s pripremama za GDPR" odgovorilo neslaganjem (48,01 %), i to: uopće se slaže 15,89 % i ne slaže se 32,12 %. "Niti se slažem, niti se ne slažem" je odabralo 41,06 % ispitanih.

S izjavom "RH je građanima pružila adekvatnu edukaciju" se ne slaže najviši postotak ispitanika i to: 36,09 % se uopće ne slaže, a 40,07 % se ne slaže, dok se samo 0,66 % u potpunosti slaže, odnosno 2,65 % se slaže s navodom.

Najveći postotak ispitanika se slaže s navodom da javnost raspolaže s premalo informacija vezanih uz uredbu i to: 31,79 % se slaže, a 26,82 % se u potpunosti slaže. Ostatak ispitanika se niti slaže niti ne slaže (24,50 %), a preostale dvije opcije neslaganja su slabo zastupljene.

	Uopće se ne slažem	Ne slažem se	Niti se slažem, niti se ne slažem	Slažem se	U potpunosti se slažem	Ukupno
Propisane kazne za nepoštivanje GDPR-a su prevelike	8,94%	19,54%	54,97%	11,26%	5,30%	100,00%
RH je na vrijeme krenula s pripremama za GDPR	15,89%	32,12%	41,06%	10,93%	0,00%	100,00%
RH je građanima pružila adekvatnu edukaciju	36,09%	40,07%	20,53%	2,65%	0,66%	100,00%
Javnost raspolaže s premalo informacija vezanih uz uredbu	8,94%	7,95%	24,50%	31,79%	26,82%	100,00%

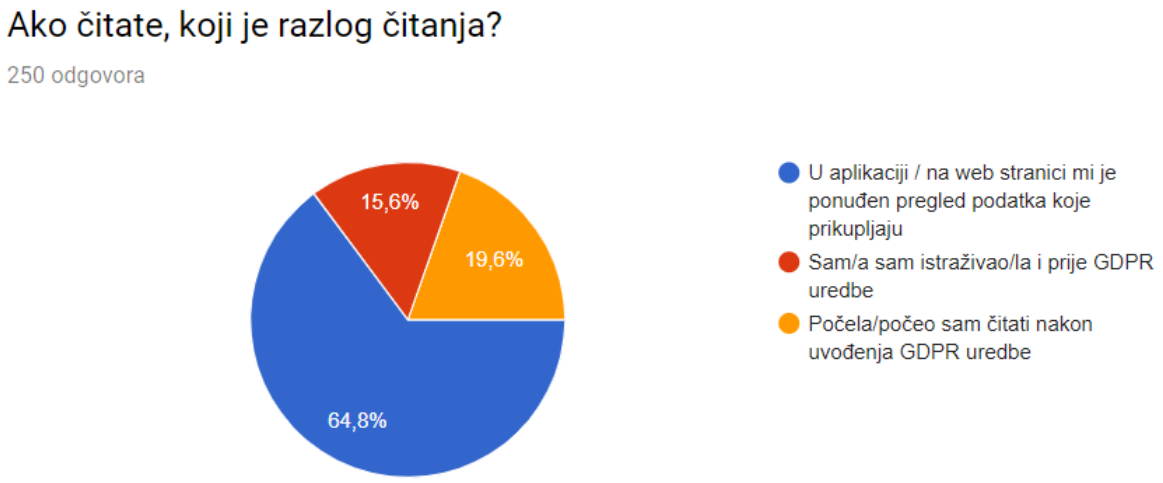
Tablica 4: Prikaz postotka uz grafikon 14



Grafikon 15: Navike čitanja obavijesti o prikupljanju podataka

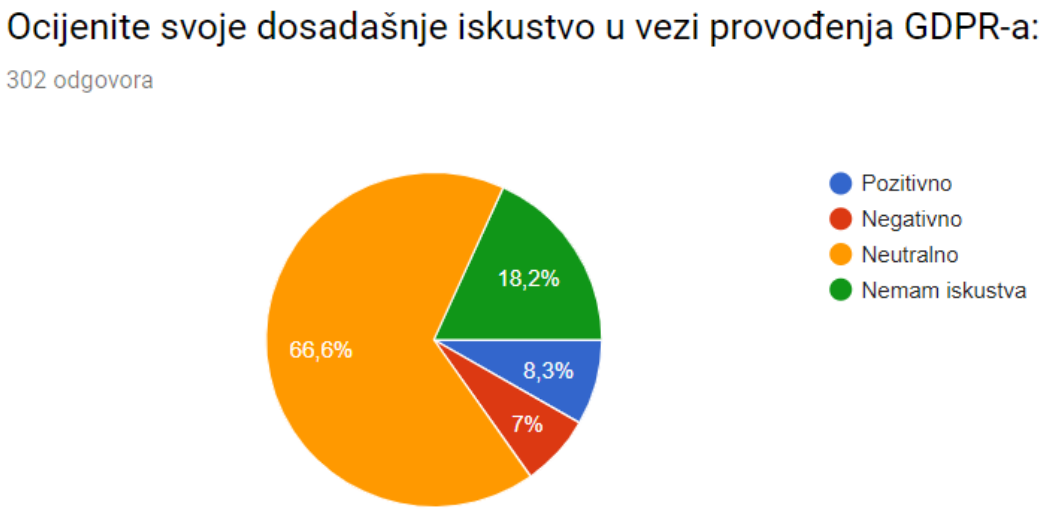
U pitanju o navikama čitanja postavka o skupljanju podatka na društvenim mrežama, najviše ispitanika je odgovorio da ponekad pročita (68,2 %), dok je 21,5 % ispitanika izjavilo da ih ne zanima, odnosno da im nije važno što društvene mreže skupljaju o

korisniku. Samo 8,9 % ispitanika redovito čita u postavkama privatnosti opseg podataka koji društvene mreže prikupljaju. Četiri osobe (1,3 %) nisu mogle odgovoriti na pitanje jer ne koriste niti jednu društvenu mrežu.



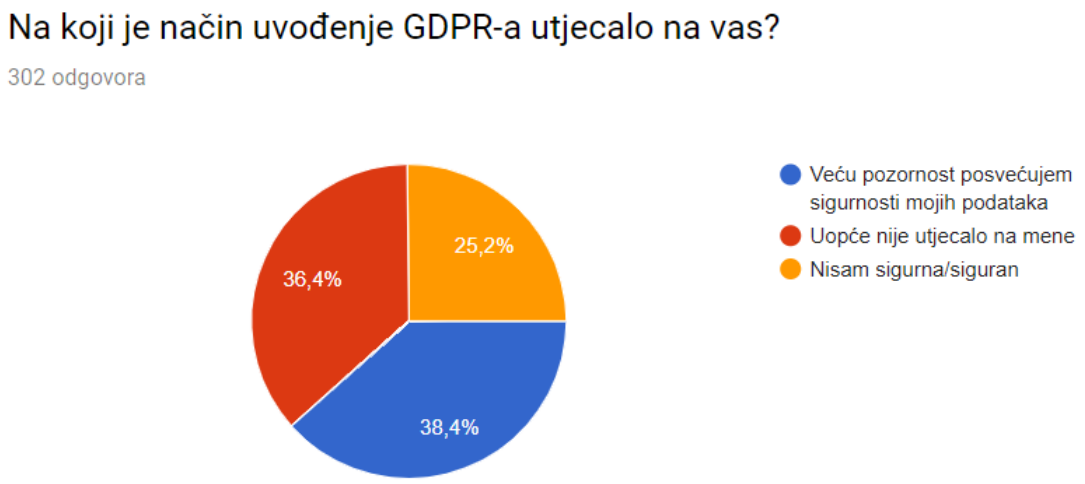
Grafikon 16: Razlog čitanja obavijesti

Većina ispitanika čita postavke jer su im ponuđene u aplikaciji (64,8 %). Zanimljiv je postotak od 19,6 % korisnika koji su počeli čitati nakon uvođenja GDPR-a, a 15,6 ispitanika je to pitanje interesiralo i prije GDPR uredbe.



Grafikon 17: Iskustvo u vezi GDPR-a

Od ispitanika se očekivalo da označe prema ponuđenim odgovorima vrstu iskustva koju su do sad doživjeli u vezi GDPR uredbe. Većina je odabrala odgovor "neutralno" (66,6 %). Pozitivno iskustvo je imalo 8,3 posto ispitanika, negativno 7 %, a 18,2 % nije moglo ocijeniti iskustvo pošto ga nisu imali.

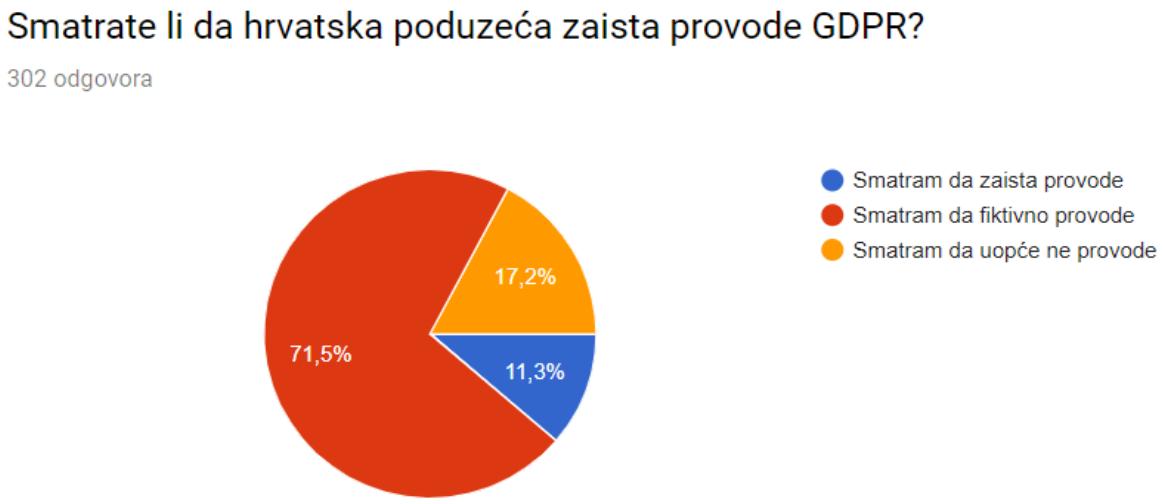


Grafikon 18: Utjecaj GDPR-a na pojedinca

U postavljenom pitanju o utjecaju GDPR-a na osobu, 38,4 % ispitanih izjavljuje da veću pozornosti posvećuju sigurnosti svojih podataka. Čak 36,4 % tvrdi da GDPR uopće nije utjecao na njih, dok 38,4 % nije sigurno.

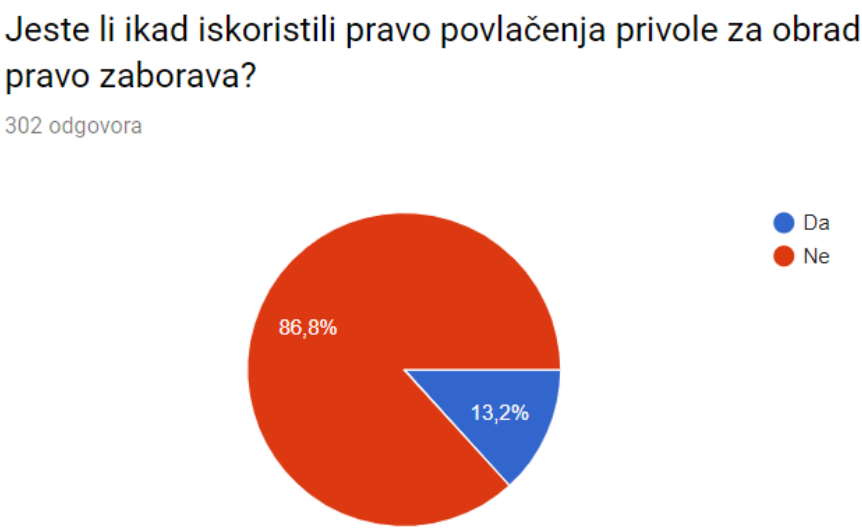
Grafikon 19: Mjerenje osjećaja sigurnosti

Većina ispitanika je na pitanje o osjećaju sigurnosti nakon uvođenja GDPR-a prilikom posjećivanja web stranica odgovorila negativno, odnosno da se ne osjećaju sigurnije zbog Uredbe o zaštiti podataka (63,6 %). Nije sigurno 21,9 % ispitanih, a 14,6 % je izjavilo da se osjećaju sigurnije.



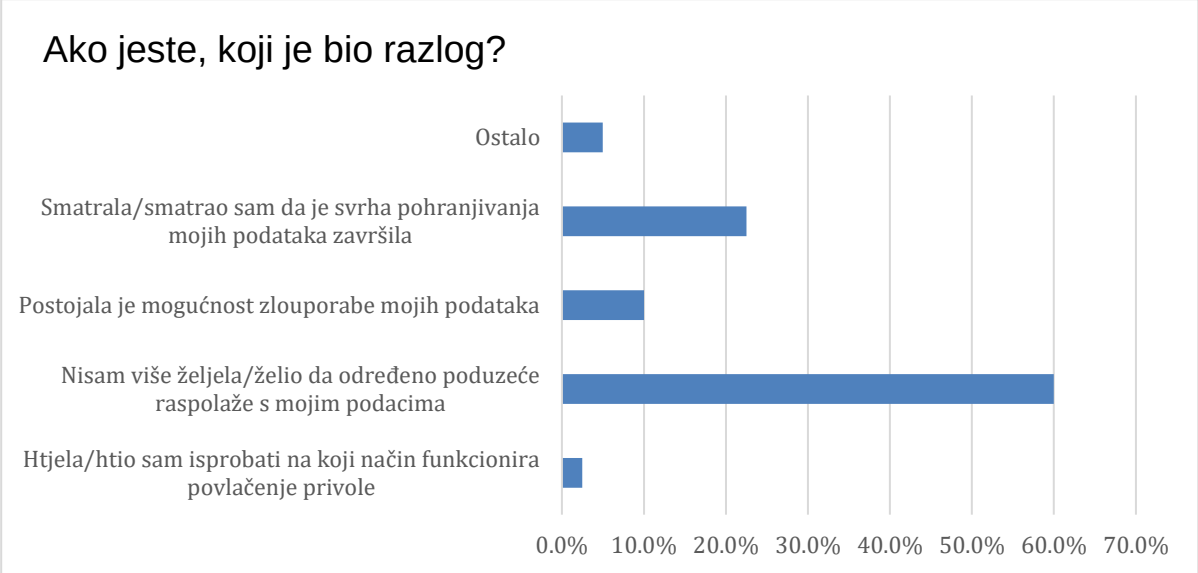
Grafikon 20: Provođenje GDPR-a u hrvatskim poduzećima

U ovom pitanju se jasno preslikava mišljenje građana o provođenju GDPR-a u hrvatskim poduzećima. Visokih 88,7 % smatra da se ne provodi, od toga 71,5 % izjavljuje da se fiktivno provodi, a 17,2 % da se uopće ne provodi, dok samo 11,3 % smatra da se zaista provodi.



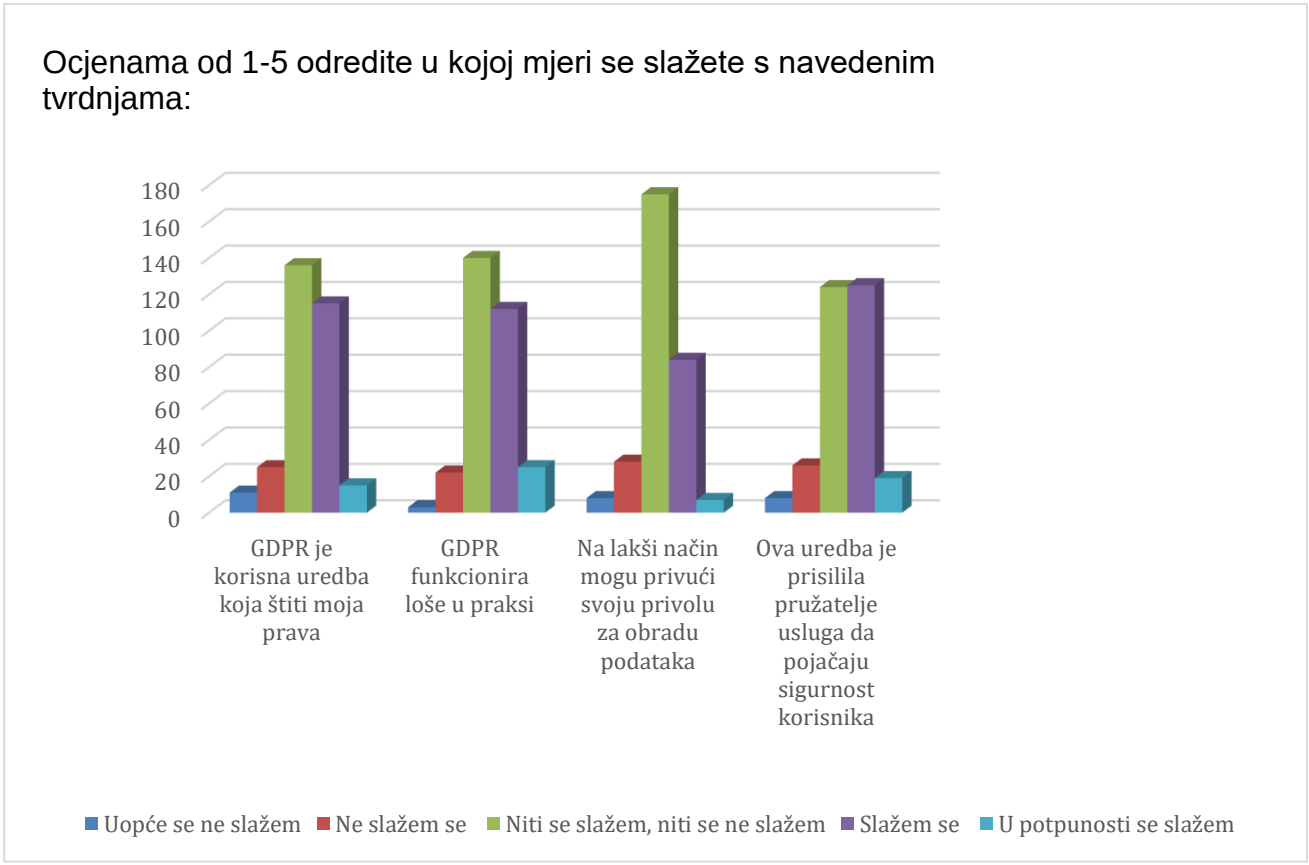
Grafikon 21: Pravo zaborava i povlačenje privole

Ispitanici su trebali odgovoriti na dva ponuđena odgovora, odnosno jesu li ili nisu iskoristili svoje pravo povlačenja privole za obradu podataka ili pravo zaborava. Većina ispitanika nikad nije iskoristila ni jedno od ponuđenih opcija (86,8 %), a samo 13,2 % je izjavilo da jesu iskoristili.



Grafikon 22: Razlog povlačenja privole ili korištenja prava na zaborav

Pitanje koje su popunjavale samo osobe koje su pozitivno odgovorile na prethodno (ukupno 40 ispitanika). Između ponuđenih odgovora je bilo potrebno odabrati razlog zbog kojeg su iskoristili pravo zaborava ili povlačenje privole za obradu podatka. Najčešći razlog (60,00 %) je želja ispitanika da određeno poduzeće više ne raspolaže s njihovim osobnim podacima, zatim je 22,50 % osoba navelo da su smatrali da je svrha pohranjivanja njihovih podataka završila. Postojanje mogućnosti zlouporabe podataka je odabralo 10 posto ispitanih, a 2,5 % je htjelo isprobati na koji način funkcionira povlačenje privole. Za odgovor "Ostalo" su se odlučile samo 4 osobe (5 %).



Grafikon 23: Iskazivanje mjere slaganja s tvrdnjama 1

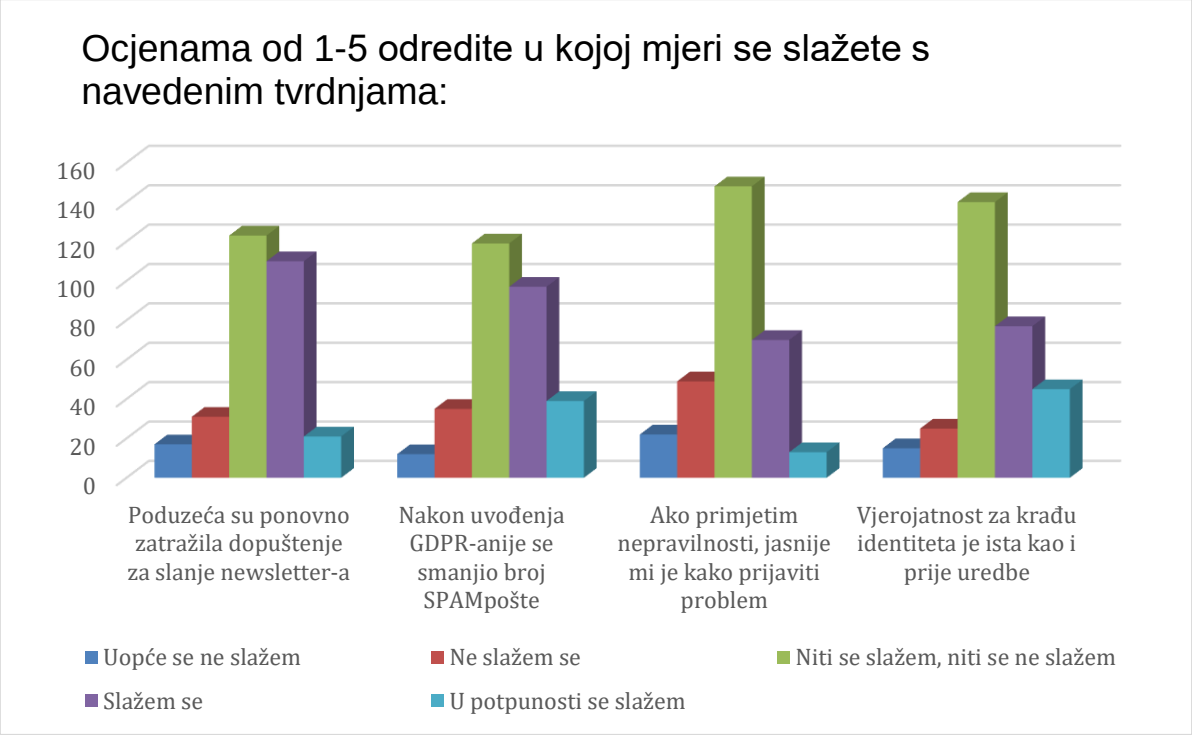
Pitanje je postavljeno pomoću izjavnih rečenica koje zahtijevaju izjašnjavanje ispitanika o stupnju slaganja ili neslaganja s izjavom i to: uopće se ne slažem, ne slažem se, niti se slažem, niti se ne slažem, slažem se i u potpunosti se slažem.

Na sva 4 pitanja su najzastupaniji odgovori "niti se slažem, niti se ne slažem" i "slažem se", dok su preostali odgovori zastupljeni u minimalnoj mjeri. S izjavom "GDPR je korisna uredba koja štiti moja prava", se složilo 38,08 % ispitanika, a neopredijeljenog

mišljenja je čak 45,03%, dok je za izjavu "GDPR funkcionira loše u praksu", neopredijeljenog mišljenja 46,36 % sudionika. Skoro pa podjednak broj ispitanika se odlučio za niti se slažem i niti se ne slažem (41,06%), i slažem se (41,39 %) s tvrdnjom "Ova uredba je prisilila pružatelje usluga da pojačaju sigurnost korisnika".

	Uopće se ne slažem	Ne slažem se	Niti se slažem, niti se ne slažem	Slažem se	U potpunosti se slažem
GDPR je korisna uredba koja štiti moja prava	3,64%	8,28%	45,03%	38,08%	4,97%
GDPR funkcionira loše u praksi	0,99%	7,28%	46,36%	37,09%	8,28%
Na lakši način mogu privući svoju privolu za obradu podataka	2,65%	9,27%	57,95%	27,81%	2,32%
Ova uredba je prisilila pružatelje usluga da pojačaju sigurnost korisnika	2,65%	8,61%	41,06%	41,39%	6,29%

Tablica 5: Prikaz postotaka uz grafikon 23

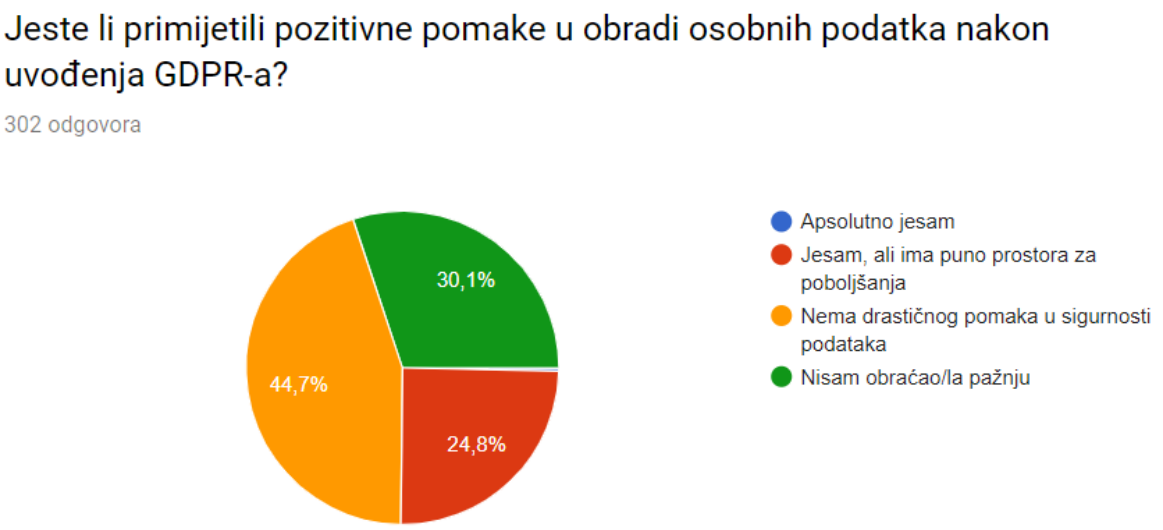


Grafikon 24: Iskazivanje mjere slaganja s tvrdnjama 2

Trend iste vrste odgovora se nastavlja i na ostala pitanja, te najviše prednjači odgovor "niti se slažem, niti se ne slažem" i to 40,73 % za tvrdnju da su poduzeća ponovno zatražila dopuštenje za slanje newsletter-a. Sljedeća po redu skupina odgovora je "slažem se" s 36,42 %, dok je samo 5,63 % ispitanih izjavilo da se uopće ne slažu s navedenom izjavom. S izjavom "Nakon uvođenja GDPR-a nije se smanjio broj SPAM pošte" se uopće ne slaže najmanji postotak ispitanih (3,97 %), ne slaže se 11,59 %. Niti se slaže, niti se ne slaže 49,01 %, dok se slaže 32,12 % i u potpunosti slaže 12,91 %. Najviše ispitanika (49,01) se niti slaže, niti ne slaže s izjavom "Ako primijetim nepravilnosti, jasnije mi je kako prijaviti problem". Osim ovog neutralnog odgovora, sljedeća skupina po veličini je "slažem se" s 23,18 %. Skupine koje odražavaju najjači stav "u potpunosti se slažem" (4,30 %) i "uopće se ne slažem" (7,28 %) su zastupljene u maloj mjeri. Sličnu situaciju možemo zapaziti i na odgovorima sudionika na tvrdnju "Vjerojatnost za krađu identiteta je ista kao i prije uredbe", niti se slaže, niti se ne slaže najveći broj ispitanika s 49,01 %, slaže se 25,50 %, u potpunosti se slaže 14,90 %. S izjavom se ne slaže 8,28 %, a uopće ne slaže 4,97 %.

	Uopće se ne slažem	Ne slažem se	Niti se slažem, niti se ne slažem	Slažem se	U potpunosti se slažem
Poduzeća su ponovno zatražila dopuštenje za slanje newsletter-a	5,63%	10,26%	40,73%	36,42%	6,95%
Nakon uvođenja GDPR-a nije se smanjio broj SPAM pošte	3,97%	11,59%	39,40%	32,12%	12,91%
Ako primjetim nepravilnosti, jasnije mi je kako prijaviti problem	7,28%	16,23%	49,01%	23,18%	4,30%
Vjerojatnost za krađu identiteta je ista kao i prije uredbe	4,97%	8,28%	46,36%	25,50%	14,90%

Tablica 6: Prikaz postotaka uz grafikon 24



Grafikon 25: Situacija nakon uvođenja GDPR-a

Pitanje se temelji na procjeni ispitanika o mogućim pozitivnim pomacima u obradi osobnih podataka nakon uvođenja GDPR-a, s tim da je samo jedna osoba (0,3 %) odgovorila da je apsolutno primijetila pozitivne promjene, 24,8 % je primijetilo pozitivne promjene ali smatraju da ima prostora za poboljšanja. Da nema drastičnog pomaka u sigurnosti podataka smatra 44,7 % ispitanika, a čak 30,1 % anketiranih nije obraćalo pažnju.

8.1. Dokazivanje hipoteza

H1: Javnost nije dovoljno upoznata s GDPR uredbom

Formula za izračun postotka neinformiranosti za osobe koje su "čule za GDPR".

(Broj neinformiranih + broj osoba koje nisu čule za GDPR) / ukupan broj ispitanika (381)

H1	Broj ispitanika	Neinformirano	%
GDPR određuje čuvanje mojih podataka	302	167	55,30%
Osobni podaci koji su zaštićeni GDPR-om su	302	170	56,29%
Prema GDPR-u moji osobni podaci se mogu obrađivati samo ako dam privolu (dopuštenje) za to:	302	290	96,03%
Kome biste se obratili ako bi netko obrađivao vaše podatke na nezakonit način?	302	95	31,46%
Što se događa ako ne pritisnite ništa ili kliknete zatvori (X) prilikom prikazivanja prozorčića o korištenju kolačića (cookies)?	302	200	66,23%
Stopa neinformiranosti		922	**61,06%**

Tablica 7: Izračun za dokazivanje opće neinformiranosti

Formula za izračun postotka opće neinformiranosti:

Prosjek od svih pitanja za koja se pretpostavlja da prikazuju vrijednost, odnosno razinu informiranosti.

(Ukupan broj neinformiranih po pitanjima + ukupan broj osoba koje nisu čule za GDPR) / (ukupan broj ispitanika * 5)

H1	*Broj ispitanika	Neinformirano	Nisu "čuli za GDPR"	%
GDPR određuje čuvanje mojih podataka..	302	167	79	64,57%
Osobni podaci koji su zaštićeni GDPR-om su..	302	170	79	65,35%

Prema GDPR-u moji osobni podaci se mogu obrađivati samo ako dam privolu (dopuštenje) za to...	302	290	79	96,85%
Kome biste se obratili ako bi netko obrađivao vaše podatke na nezakonit način?	302	95	79	45,67%
Što se događa ako ne pritisnite ništa ili kliknete zatvori (X) prilikom prikazivanja prozorčića o korištenju kolačića (cookies)?	302	200	79	73,23%
Stopa neinformiranosti		922	395	**69,13%**

Tablica 8: Izračun za dokazivanje H1

Hipoteza je dokazana, analizom istraživačkih pitanja vezanih uz hipotezu može se vidjeti da je većina ispitanika neinformirana, a stopa neinformiranosti iznosi 69,13 %

.

H2: Ispitanici ne osjećaju veći stupanj sigurnosti na internetu zbog implementacije ove uredbe.

H2	Broj ispitanika*	Negativna konotacija	%
Osjećate li se sigurnije prilikom posjećivanja web stranica ili primanja newsletter-a nakon uvođenja GDPR uredbe?	236	192	81,36%
Smatrate li da hrvatska poduzeća zaista provode GDPR?	302	216	71,52%
GDPR je korisna uredba koja štiti moja prava.	166	36	21,69%
GDPR funkcionira loše u praksi.	162	137	84,57%
Na lakši način mogu privući svoju privolu za obradu podataka.	127	36	28,35%

va uredba je prisilila pružatelje usluga da pojačaju sigurnost korisnika.	178	34	19,10%
Nakon uvođenja GDPR-anije se smanjio broj SPAM pošte	183	139	75,96%
Ako primjetim nepravilnosti,jasnije mi je kako prijaviti problem.	154	71	46,10%
Vjerojatnost za krađu identiteta je ista kao i prije uredbe.	162	122	75,31%
Jeste li primijetili pozitivne pomake u obradi osobnih podatka nakon uvođenja GDPR-a?	210	135	64,29%
Stopa "nesigurnosti"			**56,82%**

Tablica 9: Izračun za dokazivanje H2

*Izostavljeni ispitanici koji nisu sigurni: (uopće se ne slažem + ne slažem se + slažem se + u potpunosti se slažem) = ukupan broj.

Hipoteza 2 je dokazana. Analizom pitanja vezanih uz stopu sigurnosti uzrokovanu GDPR-om dolazi se do zaključka da više od polovice ispitanika nije primjetilo poboljšanja u vezi sigurnosti podataka. Sudionicima nisu jasniji procesi i ne vjeruju da se GDPR zapravo provodi u RH stoga ne dolazi do povećanog osjećaja sigurnosti.

H3: Građani nisu zainteresirani saznati što se događa s njihovim podacima.

H3	Broj ispitanika	Negativna konotacija	%
Koliko ste upoznati s vrstom i količinom podataka koje web kolačići prikupljaju o vama?	302	263	87,09%
Imate li naviku u postavkama pročitati koje podatke skupljaju društvene mreže o vama?	298	65	21,81%
Na koji je način uvođenje GDPR-a utjecalo na vas?	302	186	61,59%
Stopa nezainteresiranosti			**56,83%**

Tablica 10: Izračun za dokazivanje H3

Hipoteza koja tvrdi da građani nisu zainteresirani saznati što se događa s njihovom podacima je također dokazana. Osim pitanja koja indirektno ili direktno dokazuju hipotezu, najveći indikator je postotak i vrsta odgovora u anketi koji su većinom nezainteresirani, odnosno: nisam siguran/a, niti se slažem, niti se ne slažem koji odaju nezainteresiranost sudionika za GDPR koji nisu razvili mišljenje.

9. Zaključak

Opća uredba o zaštiti podataka ili GDPR (General Data Protection Regulation) je uredba kojoj je glavna zadaća povećati sigurnost i zaštiti osobne podatke građana Europske unije. U Hrvatskoj je obavezna primjena uredbe od 25. 5. 2018. godine za sve poslovne subjekte, neovisno radi li se o profitnim ili neprofitnim organizacijama.

Implementaciju GDPR-a je u malom poduzeću moguće provesti interno. Uspješnost implementacije ovisi o pravilnom tumačenju same uredbe i primjene na praksu i svakodnevne situacije. Faze ugradnje GDPR načela započinju prepoznavanjem potrebe, odnosno poštivanje Zakona. Pomoću GAP analize uviđa se razlika između trenutne situacije u poduzeću na polju osobnih podataka i situacije kojoj težimo (transparentno obrađivanje), pritom pazeći na temelje obrade podataka koji pružaju zakonsku osnovu za obradu. Procjenom rizika se otkrivaju slabe točke prilikom obrade podataka – koji procesi zahtjevaju detaljnu pažnju, izmjenu načela obrade i postoji li kritična, neosnovana obrada koja može biti predmet tužbe. Nakon što je utvrđen opseg i vrsta osobnih podataka te su obavljeni izračuni rizika, pristupa se kreiranju dokumentacije za provedbu. Dokumentacija obuhvaća formulare za suglasnost o obradi podataka (privola), pravilnik o obradi podatka, izvješće i evidenciju aktivnosti obrade osobnih podataka, obavijest ispitaniku o povredi njegovih osobnih podataka, odluku o proceduri upravljanja zamolbama i životopisima, odluku i izvješće o imenovanju službenika za zaštitu podataka. Prenošenjem znanja na sve zaposlenike i osiguravanjem kvalitetne edukacije stvara se manja mogućnost za povredu osobnih podataka. Edukacija bi se trebala vršiti kontinuirano i posebnu pažnju pridavati fluktuaciji zaposlenika unutar poduzeća (promjena radnog mjesta i drugačiji kontakt s kupcima), i dolazak novih koji još nisu informirani o načinima ophođenja s osobnim podacima. Testiranje i provedba zahtijevaju simultano odvijanje, procesi se ne mogu razdvojiti jer proces testiranja traje koliko i vijek poduzeća. Uvijek postoji mogućnost izmjene ili prilagodbe procesa zbog nastanka novih, nepredviđenih situacija.

U radu je prikazano provedeno istraživanje pomoću anketnog upitnika. Prva postavljena hipoteza se odnosila na stopu informiranosti građana o GDPR uredbi, odnosno pretpostavka da građani nisu dovoljno informirani. Hipoteza je dokazana i to visokim postotkom i ukazuje na manjak informacija o uredbi. Sljedeća hipoteza se odnosila na stupanj sigurnosti, tj. ispitivala je postoji li povećanje u osjećaju sigurnosti u vezi osobnih podataka i uvođenja GDPR-a. Istraživanjem je zaključeno da taj odnos ne

postoji jer većina ispitanika smatra ga se uredba uopće ne provodi u Republici Hrvatskoj. Treća hipoteza se odnosi na zainteresiranost građana – pokušavalo se doznati jesu li građani zainteresirani za uredbu i njezine pogodnosti koje donosi, međutim kroz cijelu analizu upitnika, stekao se dojam nezainteresiranosti ispitanika za sadržaj, što se indirektno moglo protumačiti iz velikog postotka odgovora "nisam siguran/a) i niti se slažem, niti se ne slažem. Obrada pitanja vezanih uz hipotezu je dokazala očekivano – građani većinom nisu zainteresirani saznati što se događa s njihovim osobnim podacima.

Cilj GDPR uredbe je osvijestiti građane i upoznati ih s njihovim pravima i mogućnošću odabira; tko i na koji način raspolaže s njihovim podacima. Za pravilno informiranje građana potrebna je edukacija koju treba osigurati država i zainteresiranost samih građana za temu zaštite osobnih podataka. Izostajanjem bilo kojeg od dva faktora, nemoguće je provesti pravilno informiranje, a time i navesti građane da više brinu o svojim osobnim podacima.

U Varaždinu, 15. ožujka 2019. godine

_____

Sveučilište
Sjever

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, TEA STEPAN *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog (*obrisati nepotrebno*) rada pod naslovom IMPLEMENTACIJA GDPR-a U MALIM PODUZEĆIMA *(upisati naslov)* te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)

_____
(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, TEA STEPAN *(ime i prezime)* neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog/diplomskog (*obrisati nepotrebno*) rada pod naslovom IMPLEMENTACIJA GDPR-A U MALIM PODUZEĆIMA *(upisati naslov)* čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)

_____
(vlastoručni potpis)

10. Literatura

1. Baumann, M. O.; Schünemann W. J. (2017): Introduction: Privacy, Data Protection and Cybersecurity in Europe: The Conceptual and Factual Field, U: Baumann, M. O.; Schünemann W. J. Privacy, Data Protection and Cybersecurity in Europe. Cham: Springer International Publishing, str. 1-11
2. Čižmešija, V.; Stepan T. (2018), Istraživanje informiranosti studenata o GDPR uredbi. Seminarski rad. Varaždin: Sveučilište Sjever
3. Dainty, C.; Keyser, T. (2016): The Information Governance Toolkit, Dataprotection, Caldicott, confidentiality. Boca Raton: CRC Press
4. De Guise, P. (2017): Data Protection Ensuring Data Availability. Boca Raton: CRC Press
5. Irene Kamara and Paul De Hert, P.; Kamara, I. (2018): Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape, U: Papakonstantinou, V.; Rodrigues, R. (2018): Privacy and Data Protection Seals. Berlin: T.M.C. Asser Press, str. 8-24
6. Hrvatski sabor (2005), Zakon o potvrđivanju konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz konvenciju za zaštitu osoba gleda automatizirane obrade osobnih podatka u vezi nadzornih tijela i međunarodne razmjene podataka
7. IT Governance, P. T. (2017): EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, drugo izdanje. Ely, Cambridgeshire: IT Governance Publishing
8. Lambert, P. B. (2018): Understanding the New European Data Protection Rules, Boca Raton: CRC Press
9. Moore, A. (2018): The GDPR & Managing Data Risk For Dummies. Chicheste: John Wiley & Sons, Ltd.
10. Voigt, P.; Von dem Bussche, A. (2017): The EU General Data Protection Regulation (GDPR), A Practical Guide. Cham: Springer International Publishing
11. Ripoll Servent, A. (2017) Protecting or Processing? : Recasting EU Data Protection Norms, U: Baumann, M. O.; Schünemann W. J. (2017): Privacy, Data Protection and Cybersecurity in Europe, Cham: Springer International Publishing, str. 115 – 128

Web literatura:

1. Agencija za zaštitu osobnih podataka; URL: https://azop.hr/ (2019-02-19)
2. Božić Velibor (2018); URL: https://www.ictbusiness.info/kolumne/gdpr-vaznost-procjene-rizika (2019-02-03)
3. Computer Emergency Response Team, URL: https://www.cert.hr/93866-2/ (2019-02-11)
4. Konvencija za zaštitu ljudskih prava i temeljnih sloboda, URL: //www.zakon.hr/z/364/(Europska)-Konvencija-za-za%C5%A1titu-ljudskih-prava-i-temeljnih-sloboda (2019-02-07)
5. 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 (2018), URL: https://www.zakon.hr/z/1021/Op%C4%87a-uredba-o-za%C5%A1titi-podataka---Uredba-(EU)-2016/679 (2019-01-04)
6. Ustav Republike Hrvatske, URL: https://www.zakon.hr/z/94/Ustav-Republike-Hrvatske (2018-12-29)
7. Span d.o.o. (2018); URL: https://gdpr2018.eu/ne-uspijevate-pronaci-put-iz-gdpr-labirinta-spanovo-rjesenje-je-personal-data-protector/ (2019-01-04)
8. Zakon o zaštiti osobnih podataka (2012), URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html (2019-02-07)

11. Popis tablica:

12. Popis grafova: