Obveze pravnih i fizičkih osoba u zaštiti osobnih podataka

Mežnarić, Dolores

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:122:820829

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 362/PE/2021

OBVEZE PRAVNIH I FIZIČKIH OSOBA U ZAŠTITI OSOBNIH PODATAKA

Dolores Mežnarić

Varaždin, ožujak 2021.

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij poslovne ekonomije

DIPLOMSKI RAD

OBVEZE PRAVNIH I FIZIČKIH OSOBA U ZAŠTITI OSOBNIH PODATAKA

Student:

Dolores Mežnarić, mat. br. 0682/336D

Mentor:

doc.dr. sc. Petar Mišević

Varaždin, ožujak 2021.

Sažetak

Stupanjem na snagu Opće uredbe o zaštiti podataka 25. svibnja 2018. godine promijenio se stav poduzeća prema postupanju s osobnim podacima. Poduzeća se susreću s novim izazovima koji su stavljeni pred njih kako bi svoje poslovanje i korištenje osobnih podataka doveli do usklađenosti s Uredbom. Uredba o zaštiti osobnih podataka donosi nove uloge i odgovornosti u procesu obrade osobnih podataka, pa su se do tada nepoznati pojmovi kao ispitanik ili subjekt obrade, voditelj obrade, izvršitelj obrade i službenik za zaštitu osobnih podataka morali implementirati u poslovanje. Svako poduzeće prikuplja drugu vrstu osobnih podataka ovisno o djelokrugu poslovanja pa su se i informacijski sustavi, koji su implementirani u organizaciji, morali prilagođavati jer prijašnja rješenja i dizajn nisu zadovoljavali pravima Uredbe. Na temelju Opće uredbe o zaštiti podataka u Hrvatskoj je uspostavljena Agencija za zaštitu osobnih podataka kao nadzorna agencija čiji je cilj savjetovati, informirati, upozoravati poduzetnike o njihovim pravima prilikom implementacije, a isto tako informirati sve zainteresirane građane o njihovim pravima prilikom obrade osobnih podataka. U radu je prikazano istraživanje o primjeni Opće uredbe o zaštiti podataka na poduzećima iz javnog i privatnog sektora koji posluju na području sjeverozapadne Hrvatske.

Ključne riječi: Uredba, GDPR, osobni podatak, voditelj obrade, ispitanik, usklađenje, primjena

Abstract

With the entry into force of the General Regulation on Data Protection on 25 May 2018, the company's attitude towards the handling of personal data changed. Businesses face new challenges facing them to bring their business and use of personal data into line with the regulation. The Regulation on Personal Data Protection brings new roles and responsibilities in the process of personal data processing, so previously unknown terms such as Respondent or Subject of Processing, Processing Manager, Processor, and Personal Data Protection Officer had to be implemented in business. Each company collects a different type of personal data depending on the scope of the business, so the information systems implemented in the organization had to be adapted because the previous solutions and design did not meet the rights of the regulation. Based on the Decree on Personal Data Protection in Croatia, the Personal Data Protection Agency was established as a supervisory agency whose goal is to advise, inform, warn entrepreneurs about their rights during implementation and also inform all interested citizens about their rights when processing personal data. The paper presents a study on the application of the Regulation on Personal Data Protection to companies from the public and private sector operating in the area of northwestern Croatia.

Keywords: regulation, GDPR, personal data, contorller , respondent, compliance, application

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

Prijava diplomskog rada

Definiranje teme diplomskog rada i povjerenstva

ODJEL Odjel za ekonomiju

STUDIJ diplomski sveu ilišni studij Poslovna ekonomija

PRISTUPNIK Dolores Mežnarić | MATIČNI BROJ 0682/336D

DATUM 05.03.2021. | KOLEGIJ Korporativna sigurnost

NASLOV RADA Obveze pravnih i fizičkih osoba u zaštiti osobnih podataka

NASLOV RADA NA ENGL. JEZIKU Obligations of company and crafts in the protection of personal data

MENTOR Petar Mišević | ZVANJE doc.dr.sc.

ČLANOVI POVJERENSTVA
1. izv.prof.dr.sc. Ante Rončević, predsjednik
2. izv.prof.dr.sc. Ljerka Luić,član
3. doc.dr.sc. Petar Mišević, mentor
4. doc.dr.sc. Mirko Smoljić, zamjenski član
5.

Zadatak diplomskog rada

BROJ 362/PE/2021

OPIS

Ubrzani tehnnološki napredak, razvoj interneta i digitalnog poslovanja uveliko su promjenili način prikupljanja i korištenja osobnih podataka u svakodnevnom poslovanju.
Povećan je rizik po sigurnost osobnih podataka građana EU zbog porasta kaznenih djela iz područja računalnog kriminaliteta te se opravdano javila potreba za uspostavljanjem novog zakonodavnog okvira kojim bi se preciznije obvezalo pravne i fizičke osobe u državama članicama EU koji u komercijalne i profesionalne svrhe obrađuju osobne podatke. Podaci su postali ključni resurs u razvoju digitalnog poslovanja.
Cilj rada je prezentirati novine koje donosi Uredba o zaštiti podataka i kolko se ista odražava na poslovanje organizacije.
U diplomskom radu je potrebno:
- prezentirati osnovne pojmove Uredbe o zaštiti podataka
- obveze voditelja i izvršitelja obrade, uloga službenika za zaštitu podataka
- načela obrade podataka i prava ispitanika
- organizacijske i tehničke mjere za usklađivanje s Uredbom o zaštiti podataka
- uloga AZOP-a kao regulatornog tijela u RH
- provesti istraživanje u obliku ankete o implementaciji GDPR-a u javnim i privatnim poduzećima te educiranosti zaposlenika o zakonskim obvezama voditelja i izvršitelja obrade.

ZADATAK URUČEN 20.04.2021. | POTPIS MENTORA

SVEUČILIŠTE SJEVER
KOPRIVNICA

Sadržaj

1. UVOD

Živimo u doba četvrte industrijske revolucije koja predstavlja pomicanje granica s fizičkog u digitalni svijet. Sve više se razvijaju robotika, nanotehnologija, biotehnologija, umjetna inteligencija, peta generacija mobilnih mreža i slično. Dolazi do promjene u načinu rada, komunikaciji, izražavanju, što omogućava lakšu zlouporabu osobnih podataka pojedinaca. Tehnološki napredak najviše se očituje u brzom razvoju interneta i digitalizacije koji su u potpunosti promijenili način prikupljanja i korištenja osobnih podataka.

Upravo zbog digitalizacije i razvoja interneta te digitalne ekonomije Europska unija je ustrajala u donošenju Opće uredbe o zaštiti podataka kojom se snažnije štite privatnost građana i njihovi osobni podaci te se nameću jasne obveze svim pravnim i fizičkim osobama koje osobne podatke građana Europske unije obrađuju u komercijalne i poslovne svrhe.

Europski parlament i Vijeće Europske unije 27. travnja 2016. godine usvojili su Uredbu EU 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te time stavlja izvan snage direktivu 95/46/EZ (Opća uredba o zaštiti podataka).

Prema nekim istraživanjima količina podataka koji će se stvoriti u tekućoj godini veća je od svih do sada stvorenih podataka. Kako se količina podataka povećava, proporcionalno raste broj napada na osobne podatke koji su pohranjeni na digitalnim platformama i samim time povećava se vjerojatnost gubitka podataka. Računalni kriminalitet postao je svakodnevica u kojoj se na različite načine upada u informatičke sustave pojedinaca ili pravnih osoba i tako neovlašteno koristi osobnim podacima. Svi ti novi izazovi potaknuli su stvaranje novog zakonodavnog okvira za zaštitu osobnih podataka jer onaj iz 1995. godine više nije mogao odgovoriti na izazove.

Opća uredba o zaštiti podataka (u daljnjem tekstu Uredba) regulira zaštitu podataka i privatnosti osobe unutar Europske unije (u daljnjem tekstu EU). Donosi propise koji reguliraju iznošenje takvih podataka u treće zemlje i vraća pod kontrolu građanima načine postupanja i korištenje osobnih podataka te njihovu redistribuciju. Direktiva je obvezna za sve članice Europske unije kao i treće strane koje na bilo koji način žele poslovati s tvrtkama unutar Europske unije.

Prije donošenja Uredbe svaka zemlja članica EU imala je svoje zakone kojima su zasebno regulirale prava na korištenje osobnih podataka pojedinaca. Gospodarski razvijene zemlje mogle su na bolji način zaštititi svoje osobne podatke od zemalja koje su industrijski i informatički nerazvijenije, pa je uvođenje Uredbe bilo nužno za ujednačavanje standarda zaštite na području EU.

Kako bi se olakšao proces obrade podataka, Uredbom su definirani svi sudionici, to su ispitanik, voditelj i izvršitelj obrade. Također, velika važnost se pridaje privolama bez kojih je zabranjeno obrađivati osobne podatke ako ne postoji zakonski okvir koji daje pravo obrade osobnih podataka i bez privole ispitanika. Glavna namjera Uredbe je olakšati poduzećima poslovanje u digitalnom okruženju. Uredbom se olakšava protok osobnih podataka između zemalja, a u isto vrijeme daje se građanima veća kontrola nad njihovim osobnim podacima.

Primjena Uredbe odnosi se na zemlje EU i zemlje članice Europskog gospodarskog prostora u koji pripadaju Norveška, Island i Lihtenštajn. Sve ostale organizacije koje žele biti prisutne na tržištu Europske unije i na njemu nuditi svoje usluge i robu obvezne su uskladiti svoje poslovanje s Uredbom.

Uredba se ne odnosi samo na tvrtke koje posluju s krajnjim korisnicima kao što su telekomunikacijske tvrtke, banke, maloprodajna poduzeća, već i na tvrtke koje posluju s drugim poduzećima zbog regulative za obradu podataka o zaposlenicima i partnerima. Fizičke osobe koje osobne podatke koriste izvan osobne ili kućne aktivnosti također su dužne uskladiti se s Uredbom da bi obrada osobnih podataka bila zakonita.

Cilj ovog diplomskog rada je istražiti anketnim upitnikom na koji način i u kojoj mjeri su poduzeća iz javnog i privatnog sektora na području sjeverozapadne Hrvatske implementirala Uredbu u svoje poslovanje. Jesu li proveli sve bitne korake za usklađenje i pravilno postupanje kod obrade osobnih podataka? Kako bismo anketu mogli na pravilan način analizirati, u prvom dijelu rada objasnit ćemo osnovne pojmove Uredbe, uloge i odgovornosti voditelja i izvršitelja obrade. Prikazat ćemo povijesni razvoj osobnih podataka te pobliže prikazati kakvu ulogu u svemu ima Agencija za zaštitu osobnih podataka (u daljnjem tekstu: AZOP) u Hrvatskoj.

2. OPĆENITO O OPĆOJ UREDBI O ZAŠTITI PODATAKA

2.1. Povijest zaštite osobnih podataka

Razvojem interneta i elektroničkom digitalizacijom poslovanja povećala se količina podataka koji se obrađuju o pojedincima u javnom, privatnom i državnom sektoru. Države su postale svjesne opasnosti od zloupotrebe korištenja informacijske tehnologije te opasnosti koju za sobom povlači iznošenje velikih količina podataka izvan granica države. Unutar država članica EU postojao je neujednačeni standard u zaštiti osobnih podataka.

Njemačka je usvojila prvi zakon o zaštiti podataka još 1970. godine, a nju su slijedile Švedska, Francuska i Danska. Donijele su savezni zakon o zaštiti podataka koji je uređivao izlaganje osobnih podataka koji se ručno pohranjuju i obrađuju u IT sustavu. Prilikom popisivanja stanovništva 1983. godine Njemački savezni sud je donio odluku o informatizaciji samo određenih podataka, koji definira kontekst u kojem se obrađuju osobni podaci tako da se zaštite pojedinci od neovlaštenog prikupljanja, korištenja i skladištenja osobnih podataka.

Dana 3. listopada 1985. godine potpisana je Konvencija Vijeća Europe 108 – ugovor koji štiti pojedinca u pogledu automatske obrade osobnih podataka. Ugovor je ratificiralo 47 članica Vijeća Europe.

Međunarodni zakoni koji definiraju zaštitu podataka[1]:

- Konvencija 108 Vijeća Europe – zakon o potvrđivanju konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz konvenciju MU br. 04/05
- Dodani protokol uz Konvenciju 108 – zakon o potvrđivanju izmjena i dopuna konvencije 108 U br. 12/05
- Priručnik o europskom zakonodavstvu o zaštiti podataka
- Opća uredba o zaštiti podataka EU 2016/679
- Handbook on European data protection law.

[1] https://azop.hr/zakonodavni-okvir/zakonodavstvo/medunarodno-zakonodavstvo 05.05.2020.

Republika Hrvatska je od 1990. godine od svojeg osamostaljenja kao članica EU u proteklom periodu normativno uređivala područje zaštite osobnih podataka. Hrvatski sabor je u lipnju 2013. godine donio Zakon o zaštiti osobnih podataka te se njime uređuje zaštita osobnih podataka o fizičkim osobama te nadzor, obrada i korištenje istih podataka u Republici Hrvatskoj.
Zakon je podijeljen u 11 područja koja obuhvaćaju sljedeće:

- temeljne odredbe
- obradu osobnih podataka
- obradu posebnih kategorija osobnih podataka
- povjeravanje poslova obrade osobnih podataka
- davanje podataka korisnicima
- iznošenje osobnih podataka iz Republike Hrvatske
- zbirke osobnih podataka
- evidenciju i središnji registar
- prava ispitanika i zaštitu prava
- nadzor nad obradom osobnih podataka
- zakonske odredbe te prijelazne i zaključne odredbe.

U Ustavu Republike Hrvatske (Narodne novine 56/90, 135/97, 08/98,113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 05/14, članak 37.), kao najvišem pravnom aktu jedne države, eksplicitno se govori o zaštiti osobnih podataka.
Članak 37. Ustava Republike Hrvatske:[2]

- „Svakome se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom.

[2] https://www.zakon.hr/z/94/Ustav-Republike-Hrvatske 13.02.2021.

- Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi.
- Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovog prikupljanja.“

Hrvatska kroz svoje propise jamči zaštitu svojim građanima da se njihovi podaci neće koristiti u nedozvoljene svrhe. Donošenjem kaznenog zakona definiraju se kazne za neovlašteno korištenje osobnih podataka pojedinca. Tako u Kaznenom zakonu (Narodne novine br.56/15, Članak 146) stoji tko će se kazniti i zbog kakvih postupaka.

Članak 146. Kaznenog zakona:[3]

„1) Tko protivno uvjetima određenim u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba, kaznit će se kaznom zatvora do jedne godine.

2) Tko protivno uvjetima određenim u zakonu iznosi osobne podatke iz Republike Hrvatske u svrhu daljnje obrade ili ih objavi ili na drugi način učini dostupnim drugome ili tko radnju iz stvaka 1. ovoga članka sebi ili drugome pribavi znatnu imovinsku korist ili prouzroči znatnu štetu, kaznit će se kaznom zatvora do tri godine.

3) Kaznom iz stavka 2. ovog članka kaznit će se tko djelo iz stavka 1. ovog članka počini prema djetetu ili tko protivno uvjetima određenim u zakonu prikuplja obrađuje ili koristi osobne podatke fizičkih osoba koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život te osobne podatke fizičkih osoba o kaznenom ili prekršajnom postupku.

4) Ako kazneno djelo iz stavka 1. do 3. ovog članka počini službena osoba u obavljanju svojih ovlasti, kaznit će se zatvorom od šest mjeseci do pet godina.“

„Kao punopravna članica Vijeća Europe, Republika Hrvatska je od ostvarenja svoje neovisnosti i samostalnosti postala stranka mnogih međunarodnih ugovora, pa tako i onih međunarodnih ugovora i instrumenata koji se odnose na ljudska prava. Konvencija o zaštiti osoba glede automatizirane obrade osobnih podataka, važan je dodatak već postojećem sustavu zaštite ljudskih prava i temeljnih sloboda, osobito prava na privatnost, koje je priznato

[3] https://zakonipropisi.com/hr/zakon/kazneni-zakon/146-clanak-nedozvoljena-uporaba-osobnih-podataka 13.02.2021.

i u članku 8. Konvencije za zaštitu ljudskih prava u poštivanju privatnog života. Temeljem konvencije o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, izrađena je Direktiva Europskog Parlamenta i Vijeća Europske Zajednice 95/EZ o zaštiti pojedinaca u okviru obrade osobnih podataka, te o slobodnom tijeku tih podataka, usvojena 20. veljače 1995. godine, a kojom se osnažuju i proširuju načela zaštite prava i slobode pojedinaca, posebno pravo na privatnost. Konvencija ima za cilj zajamčiti svakoj fizičkoj osobi zaštitu njezinih prava i temeljnih sloboda, osobito njezino pravo na zaštitu privatnosti pri automatiziranoj obradi osobnih podataka, na teritoriju svake ugovorne strane, bez obzira na njezino državljanstvo ili mjesto stanovanja".[4]

Dana 24. listopada 1995. godine usvojena je Direktiva 95/46/EZ Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi obrade osobnih podataka i o slobodnom protoku takvih podataka. U navedenoj direktivi definirani su osobni podaci, obrada takvih podataka, način i sustav arhiviranja osobnih podataka, tko su osobe koje imaju pristup osobnim podacima i na koji način rukuju s takvim podacima.

Važeća Uredba (EU) 2016/679 poznatija kao engl. General Data Protection Regulation skraćeno, GDPR stupila je na snagu 25. svibnja 2018. godine, a odobrena skoro dvije godine ranije dana 27. travnja 2016. godine kada su je izglasali Europski parlament i Europsko vijeće. Stupanjem na snagu Uredbe prestala je važiti direktiva 95/46/EZ, ali i nacionalni zakoni kao što je u Hrvatskoj Zakon o zaštiti osobnih podataka (NN br. 103/03, 118/06, 41/08,130/11).

Sve zemlje članice Europske unije dužne su primjenjivati Uredbu te se moraju uskladiti s njezinim odredbama. Uredba se odnosi na sve zemlje članice, ali i zemlje koje posluju s tvrtkama unutar Europske unije te su i one dužne primjenjivati i poštovati uredbu u odredbama načina prikupljanja i obrade podataka o građanima EU.

Gospodarski i tehnološki razvoj zemalja odvija se u okviru mogućnosti zemlje. Digitalnu transformaciju danas je nemoguće izbjeći i ona više nije izbor nego je neophodna za život, rad i komunikaciju. Zemlje koje su gospodarski razvijenije te imaju bolju infrastrukturu mogle su se brže prilagoditi izazovima digitalizacije. Prema analizi koju provodi Europska komisija

[4] *Prijedlog zakona o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka* http://www.sabor.hr/fgs.axd?id=4742 2. 3. 2020.

koja prati evoluciju digitalne kompetitivnosti članica EU, Hrvatska je na 21. mjestu od ukupno 29. država članica Europske unije te se nalazi u kategoriji manje uspješnih zemalja.[5] Prema tom istraživanju petina hrvatskih građana ne koristi se internetom, a napredak od 2018. godine je nezamjetan.

Nacionalna razvojna strategija Hrvatske do 2030. godine kao prioritet postavlja „digitalno društvo“ i razvoj digitalnih vještina. Ciljana vrijednost koja se navodi u strategiji je prosjek zemalja članica EU u digitalnoj transformaciji.[6]

Prema svemu navedenom vidljivo je da zaštita osobnih podataka nije ništa novo, ali je zbog sve bržeg napretka tehnologije potrebno uskladiti postojeće zakone i još bolje zaštititi privatnost pojedinaca. Svakodnevno smo svjedoci sve veće količine podataka koji se generiraju na pametnim telefonima, internetu, automobilima i slično te će se u budućnosti sve teže dolaziti do podataka, ali će tvrtke koje raspolažu velikom količinom podataka dobiti priliku njihova monetiziranja te će njihovom obradom, u skladu s Uredbom, kreirati nove modele i usluge.

2.2. Glavni pojmovi Uredbe

Za lakše razumijevanje Uredbe, potrebno je razjasniti i definirati glavne pojmove.

Osobni podaci odnose se na sve podatke pojedinaca čiji je identitet utvrđen ili se može utvrditi. Pojedinac je osoba koja se može identificirati pomoću određenih identifikatora kao što su identifikacijski broj, ime, podaci o lokaciji, ili pomoću više čimbenika koji tvore identitet tog pojedinca u koji svrstavamo fizičke, genetske, mentalne, ekonomske ili socijalne čimbenike.

U vrijeme razvoja tehnologije osobni podaci podrazumijevaju mnogo više nego se to do sada podrazumijevalo, u to sada spadaju i IP adresa računala, GPS lokacija mobilnih uređaja, kolačići na *web*-stranicama, fotografije koje se nalaze na mobilnim uređajima, podaci o

[5] https://ec.europa.eu/croatia/what_is_digital_transformation_changing_hr 13.03.2021.

[6] https://hrvatska2030.hr/rs3/sc11/ 23.03.2021.

stručnoj spremi i obrazovanju kao i podaci o plaći računu u banci, seksualnoj orijentaciji i svi drugi na temelju kojih se može utvrditi identitet pojedinca.

Stupanjem uredbe na snagu donesena je nova definicija osobnog podatka koja je definirana Člankom 4., stavkom 1., 13., 14., 15. Uredbe: [7]

> 1. „osobni podaci“ – znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi i koji se uredbom smatra ispitanikom, pojedinac se može identificirati izravno ili neizravno, uz pomoć osobnih identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikatori, svojstvenih fizičkih, fizioloških, genetskih, mentalnih, ekonomskih, kulturnih ili socijalni identitet tog pojedinca
>
> 13. „genetski podaci“ – odnose se na podatke koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja nam daju jedinstvene informacije o zdravlju ili fiziologiji tog pojedinoga i koji su dobiveni analizom biološkog uzorka dotičnog pojedinca
>
> 14. „biometrijski podaci“ – podaci koji se dobivaju tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca kao što su fotografije lica ili daktiloskopski podaci
>
> 15. „podaci koji se odnose na zdravlje“ – podaci koji su povezani s fizičkim ili mentalnim zdravljem pojedinaca, uključuje zdravstvene usluge kojima se daju informacije o njegovu zdravstvenom statusu.

Člankom 4., stavkom 2., 3., 4., 5., 6., 12. Uredbe definirana je obrada osobnih podataka:[8]

> 2. „obrada“ – svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim ili neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija,

[7] https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=EN, 12. 4. 2020.

[8] https://www.iusinfo.hr/Appendix/DDOKU_HR/DDHR20181007N112_14_1.pdf 12.04.2020.

strukturiranje, pohrana, prilagodba, ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenje ili stavljanje na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

3. „ograničavanje obrade“ – znači pohranjivanje osobnih podataka s ciljem ograničavanja njihove obrade u budućnosti;

4. „izrada profila“ – znači svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekta u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;

5. „pseudonimizacija“ – obrada osobnih podataka tako da se osobni podaci više ne mogu pripisati određenom ispitaniku bez upotrebe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi

6. „sustav pohrane“ – podrazumijeva svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, neovisno da li su centralizirani, decentralizirani ili rasprostranjeni na funkcionalnoj ili zemljopisnoj osnovi

12. „povreda osobnih podataka“ – svako namjerno ili nenamjerno kršenje koje dovodi do uništenja, gubitaka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni ili pohranjeni ili na drugi način obrađivani.

Prilikom obrade osobnih podataka, ako ne postoji pravni temelj za obradu osobnih podataka, potrebno je tražiti privolu. Privola je definirana člankom 4. Stavkom 11. Uredbe. [9]

11. „privola“ ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želje ispitanika kojim on, izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

[9] https://www.iusinfo.hr/Appendix/DDOKU_HR/DDHR20181007N112_14_1.pdf 12.04.2020.

3. ULOGA I ODGOVORNOST VODITELJA OBRADE I IZVRŠITELJA OBRADE PODATAKA

Kako bi se Uredba na lakši način implementirala u poduzeća, institucije i ustanove i kako ne bi došlo do nejasnoća u procesu implementacije, potrebno je definirati nove odgovornosti:

- voditelj obrade
- izvršitelj obrade.

Voditelj obrade je, sukladno članku 4. stavku 7. iz Opće uredbe o zaštiti podataka „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno sa drugima utvrđuje svrhe i sredstva obrade osobnih podataka“.[10]

Izvršitelj obrade je, sukladno članku 4. stavku 8. Opće uredbe o zaštiti podataka, „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade“.[11]

Ne postoji ograničenje tko može biti voditelj i izvršitelj obrade, pa tako voditelj i izvršitelj mogu biti fizičke osobe koje su unutar poduzeća zadužene na provedbu zaštite osobnih podataka prema Uredbi, ali i trgovačko društvo koje je angažirano kao vanjski suradnik za usklađenje. Voditelji obrade najčešće su trgovačka društva koja obrađuju podatke svojih radnika i klijenata, banke koje obrađuju podatke svojih stranaka, obrazovne ustanove koje obrađuju podatke svojih učenika, nastavnika, zdravstvene ustanove koje obrađuju podatke svojih pacijenata. Voditelji obrade mogu biti i fizičke osobe, a najčešće su to iznajmljivači koji iznajmljuju apartmane svojim gostima. Voditelji obrade dužni su voditi u pisanom i elektroničkom obliku evidencije obrade podataka. Svaka evidencija mora sadržavati podatke o voditelju obrade, svrhu obrade podataka, opis kategorije ispitanika te kategoriju osobnih podataka koja se prikuplja. Poduzeće koje posluje izvan EU potrebno je u evidenciji sadržavati sve primatelje koji su u zemlji, ali isto tako i izvan EU. Potrebno je navesti i rokove

[10] https://www.iusinfo.hr/Appendix/DDOKU_HR/DDHR20181007N112_14_1.pdf 12.04.2020.
[11] https://www.iusinfo.hr/Appendix/DDOKU_HR/DDHR20181007N112_14_1.pdf 12.04.2020.

za brisanje pojedinih kategorija te opisati organizacijske mjere koje su provedene u svrhu zaštite osobnih podataka.

Najčešći primjer izvršitelja obrade su IT poduzeća, ona služe kao potpora svakoj organizaciji s informacijskom prilagodbom te na taj način pristupaju svim podacima koje poduzeće ima u svojoj bazi podataka. Slijedi knjigovodstveni servis koji obrađuje podatke o plaćama radnika za svoje klijente, isto tako izvršitelji obrade mogu biti i zaštitarska poduzeća koja su ovlaštena za obavljanje privatne zaštite.

Ako voditelj obrade odluči kako će koristiti izvršitelja obrade, potrebno je u pisanom obliku sklopiti ugovor o međusobnoj suradnji. Ugovor je potrebno sklopiti u pisanom obliku u kojem su navedena sva prava, odgovornosti i obveze obje strane. Izvršitelj obrade mora se obavezati na zaštitu i povjerljivost obrade osobnih podataka, koje voditelj može u svako vrijeme provjeriti. Kako bi izvršitelj obrade mogao obrađivati dane osobne podatke, dužan je uskladiti svoje poslovanje s Općom uredbom o zaštiti podataka. U situacijama u kojima se koristi izvršitelj obrade njegova dužnost je provoditi i ostale mjere zaštite kako bi osigurao da se provedba obrade provodi u skladu s Uredbom.

Treća strana definirana je člankom 4. stavkom 10. Uredbe – to je svaka pravna ili fizička osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade koji su ovlašteni za obradu osobnih podataka pod izravnom nadležnošću voditelja ili izvršitelja obrade.

Pojam zajedničkih voditelja obrade odnosi se na dva ili više voditelja koji su neophodni u definiranju svrhe i načinu obrade osobnih podataka.[12]

Najčešći primjer iz prakse zajedničkih voditelja obrade možemo vidjeti kod rezerviranja putovanja preko *web*-stranica. Pretpostavimo da su za osnivanje *web*-stranice koja se bavi prodajom aranžmana za ljetovanje bile potrebne tri strane: agencija koja ima ponude ljetovanja, zrakoplovna kompanija kao prijevoznik i hotel koji nudi uslugu smještaja na ljetovanju. Prilikom dogovora ta tri poduzeća da osnuju zajedničku *web*-stranicu oni su odredili koje će osobne podatke koristiti prilikom rezervacije, tko će moći vidjeti koje osobne podatke, kako će dijeliti informacije koje se mogu iskoristiti u marketinške svrhe te su u tom slučaju oni definirani kao zajednički voditelji obrade.

[12] https://azop.hr/osnovne-informacije-za-organizacije/ 19.12.2020.

4. ULOGA I NADLEŽNOST SLUŽBENIKA ZA ZAŠTITU OSOBNIH PODATAKA

Službenik za zaštitu podataka (u daljnjem tekstu službenik) nova je funkcija koja se pojavljuje stupanjem na snagu važeće Uredbe.

Prema članku 37. stavak 1. Uredbe[13]

1. Voditelj obrade i izvršitelj obrade imenuju službenika za zaštitu osobnih podataka u svakom slučaju u kojem:

a) obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske nadležnosti

b) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrhe iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri ili

c) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka na temelju članka 9. i osobnih podataka u vezi s kaznenim osudama i kažnjavanim djelima iz članka 10.

Osoba koja nosi tu ulogu ne mora nužno biti zaposlenik poduzeća, može biti i vanjski suradnik. Jedna od bitnih karakteristika službenika je da je upućen u pravo i prakse u području zaštite podataka što uključuje dobro poznavanje i primjenu Uredbe. Osoba koja se imenuje službenikom za zaštitu osobnih podataka mora imati i stručno znanje i kompetencije iz informacijske sigurnosti. Službenik je dužan i pravodobno informirati i savjetovati voditelja i izvršitelja obrade o mogućem kršenju uredbe te ih savjetovati i informirati kako ispravno postupiti u određenim situacijama, on je izravno odgovoran upravi organizacije. Ostale zadaće koje može obavljati službenik su podizanje kolektivne svijesti i osposobljavanja sudionika procesa obrade osobnih podataka, pružanje savjeta vezanih za primjenu odredbe te suradnju s nadzornim tijelima oko nejasnoća prilikom obrade osobnih podataka i obavljanja konzultacija prilikom sumnje na kršenje pravila zaštite osobnih podataka. Službenika za zaštitu osobnih podataka potrebno je prijaviti Agenciji za zaštitu osobnih podataka. Kako bi službenik na

[13] https://www.iusinfo.hr/Appendix/DDOKU_HR/DDHR20181007N112_14_1.pdf 12.03.2021.

primjeren način obavljao svoje zadaće, voditelj i izvršitelj obrade dužni su mu osigurati pristup svim potrebnim informacijama. On je slobodan pristupiti svim informacijskim sustavima kojima društvo prikuplja, obrađuje i pohranjuje osobne podatke. Vrlo je bitna i potpora koju službenik dobiva od voditelja i izvršitelja u smislu sredstava potrebnih za izvršavanje svojih zadaća. Službenik za obavljanje svojeg posla ne smije primati nikakve upute za izvršavanje svojih zadataka, ne smije ga se razriješiti dužnosti ili kazniti zbog izvršavanja svojih zadaća. Službenik je osoba koja može u poduzeću biti zaposlena na ugovor o djelu i ne smije tijekom obavljanja posla biti u sukobu interesa. Obvezan je u svojem djelovanju pridržavati se načela tajnosti i povjerljivosti u vezi s obavljanjem poslova iz svoje nadležnosti. Službenik je kontakt-osoba za sva pitanja u vezi zaštite osobnih podataka te jedini koji je u konstantnoj suradnji s Agencijom za zaštitu osobnih podataka.

Prema priručniku za službenike za zaštitu osobnih podataka iz 2018. godine još uvijek ne postoji sustav kojim bi se funkcija službenika definirala kao radno mjesto i kojim bi bilo definirano potrebno stručno znanje koje službenik mora posjedovati. Stručno znanje koje službenik mora dokazati prilikom odabira ovisi o području djelatnosti kojim se poduzeće bavi. Korisno je i poznavanje poslovnog sektora u kojem je imenovan za stručnjaka, što znači da netko tko je imenovan stručnjakom u javnom tijelu mora dobro poznavati upravna pravila i postupke koje provodi navedena organizacija. Vrlo je bitno da službenik bude i informatički obrazovan kako bi mogao pomoći prilikom razvoja i implementacije informatičkog sustava za potrebe prilagođavanja s Uredbom. Formalna edukacija još uvijek ne postoji, znanje se stječe pohađanjem tečajeva i seminara koji su ciljano usmjereni na osiguravanje stručnosti oko Uredbe i davanja smjernica o zadaćama dodijeljenim službeniku.[14]

[14] https://azop.hr/wp-content/uploads/2020/12/prirucnik-_za_dpo-t4data-hrv.pdf, str. 141/268. 05.05.2020.

5. OSNOVNA NAČELA OBRADE PODATAKA I PRAVA ISPITANIKA

Sukladno Uredbi definirana su načela obrade podataka kao i prava ispitanika u cilju preciznijih i jasnijih obveza prema pravnim i fizičkim osobama u obradi osobnih podataka, kao i njihova obveza u odnosu na prava ispitanika.

Koristeći bilo koji od navedenih načina obrade podataka, omogućeno nam je prikupljanje veće količine podataka, čime sve podatke činimo dostupnijima i izloženijima nego inače. Korisnici se u današnje vrijeme s pravom brinu za izloženost podataka i privatnost te je postalo obavezno na pravi način informirati ispitanike o načinu korištenja njihovih podataka te načinu postupanja s podacima nakon obrade. Zaštita osobnih podataka je važna da bi svaka osoba mogla očuvati vlastitu privatnost.

Kako bi se obrada podataka odvijala u skladu s Uredbom, u članku 5. stavku 1. i 2. Opće uredbe o zaštiti podataka navedena su načela obrade osobnih podataka.[15]

1. Osobni podaci moraju biti:

a) zakonito, pošteno i transparentno obrađivani, s obzirom na ispitanika („zakonitosti, poštenosti i transparentnosti“)

b) prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja, ili u statističke svrhe sukladno s člankom 89. Stavkom 1. ne smatra se neusklađeno s prvotnom svrhom („ograničavanje svrhe“)

c) primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe koje se obrađuje („smanjenje količine podataka“)

d) točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguranja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuje, bez odlaganja izbrišu ili isprave („točnost“)

[15] https://www.iusinfo.hr/Appendix/DDOKU_HR/DDHR20181007N112_14_1.pdf 12.03.2021.

e) čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhu znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1., što podliježe primjeni tehničkih i organizacijskih mjera propisanih ovom uredbom radi zaštite prava i slobode ispitanika („ograničavanje pohrane“)

f) obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade, te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera („cjelovitost i povjerljivost“)

2. Voditelj obrade odgovoran je za usklađenost sa stavkom 1. te je mora biti u mogućnosti dokazati („pouzdanost“).

Kada kažemo da podatke obrađujemo prema načelu zakonitosti, točnosti i transparentnosti, podrazumijeva se da će se podaci koji su prikupljeni obrađivati samo u skladu s pravnim temeljima za koje su prikupljeni, a načelo poštenosti i transparentnosti zahtijeva da ispitanik čiji se podaci obrađuju može od voditelja obrade u svakom trenutku zahtijevati dodatne informacije o postupku i posljedicama korištenja njegovih podataka, koje mu je voditelj dužan bez odgađanja učiniti dostupnim. Ograničavanje svrhe znači da podaci koji se prikupe za određene svrhe ne mogu se i ne smiju se koristiti na ni jedan način koji nije u skladu s tom svrhom, osim u iznimnim situacijama u kojima je to uredbom dozvoljeno. Kako bi se smanjio rizik od neovlaštene upotrebe osobnih podataka, ali i omogućilo informacijskim sustavima da lakše procesuiraju osobne podatke, podatke je potrebno ograničiti na ono što je zaista potrebno. Svi podaci koji se prikupljaju moraju biti točni, a da bi točnost mogla biti ispunjena, potrebna je i ažurnost u pregledavanju osobnih podataka. Prilikom ažuriranja ispravljaju se netočni podaci, a sve ostale podatke koji više ne služe svrsi potrebno je bez odgađanja obrisati i ukloniti. Kako ne bi došlo do nepotrebnog popunjavanja prostora za pohranu, podaci se moraju čuvati samo onoliko dugo koliko traje svrha radi koje su prikupljeni, a ostale podatke je potrebno ukloniti. Podaci koji se prikupljaju od ispitanika moraju odgovarati načelu cjelovitosti i povjerljivosti što znači da se podaci moraju čuvati od neovlaštenog ili

nezakonitog pristupa i obrade od strane osoba koje nisu ovlaštene za pristupanje osobnim podacima.

Pouzdanost je navedena u članku Uredbe kao zasebno načelo za koje je odgovoran voditelj obrade te u svakom trenutku on mora biti spreman dokazati da su osobni podaci kojima raspolaže i koji se nalaze u njegovom posjedu usklađeni s načelom i s Uredbom.

Usklađivanje s načelima obrade osobnih podataka nužno je i čini najvažniji dio Uredbe, a kršenje navedenih načela kažnjava se najvećim mogućim kaznama. Pretpostavlja se da će se kršenjem jednog od načela obrade dogoditi lančana reakcija koja će uzročno-posljedično dovesti do kršenja i ostalih načela obrade podataka.

Tvrtke koje su stupanjem na snagu Uredbe dobile pravo obrađivati osobne podatke dobile su i nove obaveze koje utječu na funkcionalne zahtjeve koji moraju biti ispunjeni prilikom korištenja osobnih podataka koje su skupile od ispitanika. Sva prava koja se odnose na funkcionalne zahtjeve potrebno je javno objaviti kako bi bila dostupne svima. Bitno je da svi ispitanici koji su u nekom trenu dali privolu za obrađivanje osobnih podataka znaju kakva prava imaju te na koji način mogu iskoristiti koje pravo.

Funkcionalni zahtjevi koji moraju biti ispunjeni prilikom obrade osobnih podataka su:

- Pravo na pristup – svaki ispitanik ima pravo od voditelja obrade zahtijevati pristup osobnim podacima koji se odnose na njega, također njegovo je pravo dobiti informacije na kojim mjestima se njegovi podaci obrađuju, u koju svrhu te koriste li se u razmjeni među zemljama. To pravo bilo je propisano i u ranijoj važećoj Direktivi 95/46/EZ, no u Uredbi je obrađeno na detaljniji način. Prilikom razmišljanja o pravu na pristup ne nalazimo neke velike prepreke tako dugo dok ne počnemo razmišljati na koji način se sve podaci prikupljaju i gdje se sve zaista nalaze naši osobni podaci.

  Kao primjer možemo uzeti poduzeće koje je svrstano u skupinu velikih poduzeća, u kojem prilikom zapošljavanja potpisujemo ugovor o radu, koji oni kopiraju i pohranjuju u nekoliko arhiva i računalima zaposlenika raznih odjela. Prilikom ulaska u poduzeće vjerojatno je da smo snimljeni nadzornim kamerama iz sigurnosnih razloga koje se isto tako čuvaju na nekoliko servera. Kada počinjemo tako razmišljati, pravo na pristup informacijama ne izgleda kao jednostavan zahtjev jer je potrebno obraditi

velik broj podataka da bi se na traženi zahtjev odgovorilo u što kraćem vremenu, a da smo sigurni da nam ništa od podataka nije promaklo.

- Pravo na zaborav – ispitanik ima pravo tražiti brisanje osobnih podataka koji se odnose na njega bez navođenja objašnjenja, dok voditelj obrade bez nepotrebnog odgađanja mora obrisati takve podatke ako oni nisu više nužni u svrhu obrade, prilikom traženja tog prava povlači se privola dana za korištenje osobnih podataka te se svako daljnje korištenje podataka može smatrati nezakonitom radnjom. Navedeni zahtjev stvara mnogo problema u današnjim informacijskim sustavima. Kako pravo na zaborav navodi da se osobni podaci moraju bez pogovora ukloniti, informacijska služba mora ukloniti sve podatke sa svih sigurnosnih kopija koje postoje u poduzeću. Dodatne komplikacije nastaju ako su podaci proslijeđeni izvršitelju obrade koji se ne nalazi u istom poduzeću. Ako ispitanik zatraži ispunjenje tog prava, a neki drugi pravni akt nam brani uništavanje dokumentacije, voditelj obrade odbit će izvršavanje tog prava, ali će na drugi način zaštititi osobne podatke ispitanika. Kao primjer možemo navesti radnika koji je prestao raditi kod poslodavca i kod otkaza traži pravo na zaborav svih svojih podataka. Poslodavac će odbiti izvršenje takvog prava jer mu drugi zakon o čuvanju dokumentacije nalaže da se isplatne liste radnika čuvaju trajno. Prilikom takve situacije poslodavac neće obrisati sve osobne podatke, ali će ih šifriranjem ili nekim drugim načinom maskirati kako treća osoba koja dođe do tih podataka ne bi znala o kome se radi.

- Pravo na prenosivost podataka – svi podaci koje je ispitanik pružio voditelju obrade mogu se zatražiti u strojno čitljivom formatu te se mogu prenijeti drugom voditelju obrade bez ometanja od strane voditelja kojem su osobni podaci prvi put pruženi. Prilikom prijenosa podataka na takav način potrebno je podatke šifrirati i zaštititi zaporkom kako bi ispitanik koji je zatražio navedeno pravo bio siguran da se podaci dijele s osobom na koju se odnose, a ne nekoj trećoj. Isto tako pravo na prenosivost može se odbiti ako ne postoji informatički siguran način da se ta prenosivost obavi. Kao primjer prava na prijenos možemo navesti promjenu poslovne banke korisnika koji mijenja poslovnu banku u kojoj ima otvoreni račun pa banke zbog uštede vremena podijele podatke od korisnika u elektroničkom obliku.

- Izvješćivanje o povredi osobnih podataka – podrazumijeva kršenje koje dovodi do slučajnog ili nezakonitog gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađeni, u slučaju sumnje na kršenje sigurnosti voditelj obrade je dužan prijaviti nadležnom nadzornom tijelu unutar 72 sata. Najčešća povreda nad podacima nastaje u poduzećima koja nisu na adekvatan način zaštitila svoje sustave i datoteke iz ranijeg vremena pa se osobnim podacima može pristupiti na jednostavan način. Agencija za zaštitu osobnih podataka objavila je obrazac izvješća o povredi osobnih podataka koje voditelj i izvršitelj obrade mogu koristiti u svom radu.

- Transparentnost – voditelj obrade mora obavijestiti ispitanika o svojem identitetu i kontakt-podacima te razlozima obrade podataka, načinima primanja, pohrane i mogućnostima povlačenja danih podataka. Što je transparentnost veća, povećava se povjerenje ispitanika te smanjuju upiti ispitanika.

- Pravo na ispravak – ispitanik ima pravo u svakom trenutku dopuniti nepotpune osobne podatke koji se odnose na njega. Podaci se kontinuirano mijenjanju: adresa stanovanja, bankovni račun, telefonski broj, ime i prezime…, sve su to primjeri podataka koji su bitni u našem životu i koji nas na neki način određuju pa je tako i pravo na ispravak podataka jedno od bitnijih kako bi podaci koje smo dali na obradu bili ažurirani.

- Pravo na prigovor – ispitanik u bilo kojem trenutku može uložiti prigovor na obradu osobnih podataka ako se ona temelji na izvršavanju službenih ovlasti voditelja obrade i legitimnog interesa voditelja obrade. Tada je voditelj dužan dokazati da su njegovi razlozi legitimni, inače mora prestati obrađivati osobne podatke. Do trenutka prigovora pravo na obradu osobnih podataka je legitimno.

6. ORGANIZACIJSKE I TEHNIČKE MJERE ZA USKLAĐIVANJE S OPĆOM UREDBOM O ZAŠTITI PODATAKA

Prema Općoj uredbi o zaštiti podataka, primjena Uredbe je obavezna za sve pravne i fizičke osobe koje u svom poslovanju obrađuju osobne podatke građana Europske unije.

„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.“[16]

Jednostavnije rečeno, moraju se uskladiti s Uredbom sve fizičke i pravne osobe koje se bave obradom podataka koji potječu s područja Europske unije. U tu grupu se uvrštavaju razne udruge, nevladine organizacije i javna tijela, male i velike tvrtke.

Međutim, postoje i oni koji nisu obvezni u svoje poslovanje uvesti Uredbu, ali takvih je malo. Kako bi se izbjegla uskladba s Uredbom, moraju se zadovoljiti dva uvjeta:

- osobne podatke mora se obrađivati samo povremeno
- ne obrađivati posebne kategorije osobnih podataka.[17]

Kako bi se Opća uredba o zaštiti podataka mogla implementirati u poduzeće, prvi korak je analiza stanja tog poduzeća. Kako bi se usklađivanje moglo provesti bez većih problema, potrebno je poznavati procese i sustave koji djeluju unutar organizacije te na koji način i gdje se podaci pohranjuju unutar organizacije. Nakon prvotne analize morali bismo dobiti odgovore na neka osnovna pitanja kao što su s kojim podacima se organizacija susreće, na koji način ih koristi i gdje se oni pohranjuju, na koje dijelove organizacije se promjena i usklađivanje s Uredbom najviše odnosi te na koje poslovne procese implementacija ima najveći utjecaj. Kako bi implementacija Uredbe bila što lakša za sve djelatnike unutar

[16] Članak 18. Uredba EU 2016/679 Europskog parlamenta i Vijeća. 12.04.2020.

[17] https://gdprinformer.com/hr/vodic-kroz-gdpr 26. 3. 2020.

organizacije i kako bi je svi što bolje razumjeli, potrebno je organizirati podatke koji se smatraju osobnim podacima. Organiziranjem osobnih podataka možemo lakše identificirati načine na koji se ti podaci kreću unutar organizacije.

Nakon što je odrađena kompletna analiza poslovnih i informacijskih sustava, nužno je ustvrditi na kojim se mjestima unutar poduzeća obrađuju i pohranjuju osobni podaci te se može pristupiti analizi rizika.

Kako stoji navedeno u članku 35. stavku 1. Uredbe, definirana je procjena učinka na zaštitu podataka:

„Ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka. Jedna procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike.“[18]

Kako bi tvrtkama bilo olakšano analiziranje, identifikacija i umanjenje rizika zaštite podataka, primjenjuje se DPIA (engl. Data Protection Impact Assessment) proces. Proces DPIA jedan je od ključnih obaveza i odgovornosti u djelokrugu Uredbe. Prilikom analize rizika u nekom poduzeću moramo biti svjesni da rizik nije moguće eliminirati, ali ga je potrebno smanjiti da bi njegova razina bila prihvatljiva u okviru onoga što smo si zadali da želimo postići.

Kako bi lakše pristupili analizi rizika na stranicama ICO-a[19] (engl. Information Commissioner s Office), nalazi se primjer analize koji možemo primijeniti na svakom poduzeću da bismo lakše prilagodili poslovanje zahtjevima GDPR-a.

Primjer analize rizika:

Analiza rizika postavlja sljedeće zahtjeve na razmatranje:

- svijest

[18] https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=EN, 25. 3.2021.

[19] https://ico.org.uk/for-organisations/accountability-framework/risks-and-data-protection-impact-assessments-dpias/ 19.12.2020.

- informacije koje posjedujemo
- komuniciranje podataka o privatnosti
- prava pojedinaca
- zahtjevi za pristup
- pravna osnova za obradu osobnih podataka
- privola
- djeca
- povreda podataka
- dizajn zaštite podataka i procjena učinka na zaštitu podataka
- službenik za prijenos podataka.

Svaki navedeni zahtjev potrebno je objasniti, smjestiti unutar organizacije i odrediti kako ga još poboljšati.

- Svijest – potrebno je kod ključnih ljudi u organizaciji osvijestiti da Uredba stupa na snagu i da bi mogla imati značajan utjecaj na resurse poduzeća – u organizaciji su određeni prvi datumi sastanka čelnih ljudi i odabira ključnih korisnika koji će sudjelovati u procesu usklađivanja s Uredbom – potrebno je još proučiti Uredbu i zahtjeve koje donosi, odlučiti o okvirnim rokovima i resursima koji su potrebni u projektu usklađivanja organizacije s Uredbom.
- Informacije koje posjedujemo – proučavamo osobne podatke koje posjedujemo, dokumentiramo ih i određujemo kako i kome ih prosljeđujemo. Izrađen je predložak aktivnosti obrade u kojem će se bilježiti svi osobni podaci, mjesto pohrane i rokovi čuvanja tih podataka – svaki odjel u poduzeću mora popuniti predložak aktivnosti obrade, potrebno je pregledati procedure i procese te razmotriti situacije u kojima dolazi do višestrukih prijetnji.

- Komuniciranje podataka o privatnosti – potrebno je donijeti plan za donošenje potrebnih izmjena. Kao organizacija imamo obavijest da prikupljamo osobne podatke, ali nemamo jasno navedenu svrhu prikupljanja – potrebno je doraditi i osigurati bolje obavijesti u skladu sa zahtjevima koje propisuje Uredba.

- Prava pojedinaca – potrebno je osigurati sva prava koja navodi Uredba. U poduzećima većina sustava ima implementirane funkcionalnosti koje omogućavaju zahtjevi Uredbe – potrebno je ponovno pregledati podatke koji su dostupni korisnicima kako bismo bili sigurni da u potpunosti pokrivaju zahtjeve za pristup podacima.

- Zahtjev za pristup – potrebno je ažuriranje procedura i planiranje kako ćemo obrađivati zaprimljene zahtjeve u novim okvirima kako bi se izbjeglo plaćanje kazni i utvrditi točne rokove za rješavanje zahtjeva. Postoje procedure u kojima je definirani proces odgovaranja tvrtke na zahtjeve ispitanika – potrebno je osigurati da su svi zaposlenici svjesni promjena koje su vezane za zahtjev za pristup podacima.

- Pravna osnova za obradu osobnih podataka – potrebno je definirati pravnu osnovu za prikupljanje i određivanje dokumentacije i osobnih podataka. Trenutno se u poduzeću koriste osnovne privole korisnika – potrebno je ponovno proučiti usklađenost postupaka sa zakonskim okvirima.

- Privola – treba provjeriti sve načine na koji tražimo, dobivamo i bilježimo privole, Uredba nas upućuje da moramo imati dokaz da je korisnik dao privolu. Slijedi pregledavanje pravne osnove za obradu osobnih podataka i prepreka procjene učinka na privatnost – valja pregledati politike i procedure koje se koriste te pregledati metode koje se koriste.

- Djeca – Opća uredba o zaštiti podataka donosi posebnu zaštitu osobnih podataka koji se odnose na djecu, posebno zbog korištenja djece u komercijalne i internetske usluge. Poduzeće obrađuje podatke o djeci za potrebe stipendiranja djece zaposlenika i dodjele prigodnih nagrada – provjeriti jesu li prikupljeni podaci zaštićeni i da se obrađuju u skladu sa zakonom.

- Povreda podataka – potrebno je osigurati sve potrebne postupke za istraživanje, otkrivanje i prijavljivanje kršenja osobnih podataka, izvještavanje o značajnim incidentima kršenja podataka nadzornim tijelima; ako je kršenje Uredbe rezultirano

rizikom za pojedince, potrebno je obavijestiti sve oštećene vlasnike podataka. Postoji procedura koja se bavi povredama nad podacima – treba provjeriti jesu li postojeći procesi i procedure u potpunosti usklađeni s Uredbom, dodatno educirati zaposlenike o načinu rukovanja s osobnim podacima klijenata koje obrađuje, potrebno je osigurati da se uklone sve nepotrebne kopije osobnih podataka s računala i svih ostalih uređaja.

- Dizajn zaštite podataka i procjena učinka na zaštitu podataka – svi novi sustavi moraju sadržavati privatnost i zaštitu podataka u okviru svoje specifikacije. Svi poslovni sustavi koje tvrtka ima moraju imati minimalno ugrađenu kontrolu pristupa podacima putem odgovarajućih korisničkih rola – potrebno je podignuti svijest za provođenje procjene učinka na zaštitu podataka.

- Službenik za zaštitu podataka – Uredba određuje da je potrebno odrediti službenika za zaštitu podataka koji ima stručno iskustvo i znanje o zakonima zaštite podataka kako bi mogao obavještavati i savjetovati sve zaposlenike o njihovim obavezama i pravima, kako bi pratio usklađenost s Uredbom i drugim zakonima o zaštiti podataka; on je također prva točka kontakta s nadzornim tijelom – službenik je već određen unutar poduzeća te redovito izvješćuje menadžment tvrtke i potrebno mu je omogućiti sve resurse koji su potrebni.

- Međunarodni prijenos podataka – ako poduzeće posluje međunarodno, treba provjeriti pod koje nadzorno tijelo pripada – u Hrvatskoj, nadzorna agencija kojoj odgovaramo je AZOP. Potrebno je pregledati sve dostupne informacije o agenciji koje su na snazi u zemlji u kojoj poslujemo te uskladiti svoje propise s nadzornim tijelima.

Nakon što smo proveli potrebne analize u poduzeću te smo utvrdili zatečeno stanje, možemo se pripremiti na integraciju Uredbe u poduzeće. Kako bismo imali podlogu za integriranje Uredbe, potrebno je pripremiti sve potrebne obrasce i dokumente na koje se možemo osloniti prilikom provedbe u poduzeću.

Obrasci koji su potrebni:

1. Pravilnik o primjeni Uredbe – svako poduzeće donosi pravilnik o primjeni Uredbe koji je prilagođen njihovom djelokrugu poslovanja te je takav pravilnik potrebno

objaviti na svojim stranicama kako bi bio javno dostupan, a u njemu se moraju navesti sve informacije o svrsi prikupljanja osobnih podataka, kontakt-osobe koje su zadužene za prilagodbu s Uredbom i koje je moguće kontaktirati u vezi bilo kakvih pitanja vezanih za obradu i prikupljanje osobnih podataka.

2. Evidencija aktivnosti obrade – sve tvrtke koje imaju više od 250 zaposlenih dužne su voditi evidenciju obrade, koja mora sadržavati podatke o razlogu prikupljanja i obrade podataka, opise podataka koji se obrađuju, vremenskom roku obrade i mjerama koje su provedene da bi se zaštitili podaci koji su prikupljeni.

3. Privola za obradu osobnih podataka – dokument koji se sastavlja kako bismo ispitaniku pružili izjavu kojom ga se upoznaje sa svrhom u koju će se njegovi osobni podaci koristiti, u kojoj je naveden način na koji tu privolu može povući, privola mora biti dobrovoljna te ispitanik mora imati mogućnost i odbiti davanje privole. Na privoli je potrebno navesti podatke voditelja obrade kako bi ispitanik imao informaciju kome se može obratiti u slučaju bilo kakvih nejasnoća. Prikupljanje privole kasnije mora biti moguće dokazati da je prikupljena na zakonit način.

4. Odluka o odabiru službenika za zaštitu podataka – odluka koju donosi voditelj obrade podataka u kojoj su navedeni svi podaci o osobi koja će se odabrati na poziciji službenika za zaštitu podatka ako je takva odluka potrebna, navedenu odluku potrebno je dostaviti Agenciji za zaštitu osobnih podataka.

5. Izvješće o odabiru službenika – dokument poduzeća u kojem su definirane uloge voditelja obrade, izvršitelja obrade i svih ostalih službenika koji rade na primjeni Uredbe ako je to potrebno.

6. Izvješće o aktivnostima službenika – izvješće se sastoji od podataka na koji način službenici prikupljaju osobne podatke, od koga su ih prikupili, u koje svrhe, način na koji su ih obradili, mjesto na kojem su ih obradili, kome su bili potrebni u poduzeću, po kojem zakonu su ih prikupili, koje su uspostavljene kontrolne mjere te koja su prava ispitanika koji su dali navedene podatke.

7. Izvješće o povredi osobnih podataka – ako se dogodi povreda, potrebno je sastaviti izvješće u kojem je opisano što se dogodilo, kako se dogodilo i kako je sanirana šteta

koja je nastala. Unutar 72 sata potrebno je o tome obavijestiti nadzorno tijelo koje će postupiti u skladu s člankom 55. Opće uredbe o zaštiti podataka.

8. Obavijesti ispitanika o povredi – dokument koji je obvezan dostaviti ispitaniku ako se dogodila povreda u smislu neovlaštenog pristupa njegovim osobnim podacima. Potrebno ga je obavijestiti o načinu na koji se povreda dogodila, kako smo sanirali štetu te je li o tome obaviještena nadzorna agencija.

9. Odluka o proceduri upravljanja zamolbama i životopisima u svrhu zaposlenja – interna odluka poduzeća u kojoj je objašnjena procedura prikupljanja zamolba i način na koji se navedene zamolbe kasnije sortiraju, čuvaju i uklanjaju ako ne postoji razlog njihova čuvanja.

10. Interni pravilnici o postupanju s osobnim podacima – pravilnici koji će biti doneseni s ciljem revidiranja do tada korištene politike i izjave o privatnosti, pravilnici koji će regulirati ili pobliže objasniti kako se neke mjere provode u praksi i sl.

Kako bi sva dokumentacija bila na ispravan način tumačena, a i kako bi se Uredba na pravilan način implementirala u poduzeće, jednako je bitna i edukacija svih zaposlenih. Kako bismo na pravilan način educirali zaposlenika, najbolje je održati prezentaciju sa svim temeljitim informacijama koji se odnose na njih. Na prezentaciji je potrebno osigurati i vrijeme za postavljanje pitanja kako bi se razjasnile sve moguće nedoumice koje postoje. Prije dogovorene prezentacije možemo putem *e-maila* svim zaposlenicima proslijediti materijale koji će pratiti prezentaciju kako bi se svi mogli pripremiti te kako bi se olakšalo njezino slušanje i praćenje. Na održanoj prezentaciji potrebno je potaknuti zaposlene na vlastito istraživanje kako bi se smanjila nepredvidivosti kod primjene novih zakona, a i kako bi zaposleni znali kome i kada se mogu obratiti u slučaju povrede njihovih prava.

Nakon implementacije Uredbe u poduzeće potrebno je s vremena na vrijeme provesti testiranje cijelog sustava. Prilikom testiranja vidjet ćemo jesu li svi zaposlenici educirani te primjenjuju li na pravilan način Uredbu. Postoji li propust zbog kojeg bi mogli snositi neke kazne. Moguće je vidjeti i probleme koje prilikom procjene rizika nismo zapazili ili su nam promakli. Isto tako možemo zatražiti pomoć konzultantskih organizacija za podršku prilikom

implementacije te za rješavanje nejasnih situacija koje su nama nove, a oni su ih imali prilike rješavati u drugim slučajevima.

U današnje vrijeme često zaboravljamo koliko je važna fizička kontrola pristupa podacima, a ne samo softverska zaštita. Postoji više načina kontrole pristupa podacima. Svaki poslovni sustav uvodi svoju kontrolu pristupa na način za koji on smatra da je najbolji za njegovo poslovanje. Poslužitelji se tako zaključavaju u zasebnu prostoriju kojoj pristup imaju samo određeni djelatnici, isto tako moguće je kreirati dopuštenja segmentima aplikacije samo određenim grupama korisnika.

Zadaća svakog poduzeća je definirati poslovne zadatke za svakog pojedinog radnika te definirati razinu podataka kojima svaki radnik ima pravo pristupa. Ne može se dogoditi da svi zaposlenici imaju pristup svim podacima jer je to jedan od najvećih sigurnosnih rizika u poduzeću. Zbog česte fluktuacije zaposlenih u poduzeću radnici koriste pristup podacima tako da ih odnose sa sobom prilikom napuštanja radnog mjesta, a to je jedna od najvećih povreda nad podacima. Isto tako potrebno je ograničiti kopiranje podataka na razne direktorije (medije za pohranu) jer tako gubimo kontrolu nad podacima i povećavamo mogućnosti povrede koju je kasnije teško odrediti. Preporučuje se enkripcija tvrdih diskova nad podacima (USB-a, laptopa i dr.)

Prvi korak prema kontroli i pristupu podacima je zaključavanje računala zaporkom nakon nekoliko minuta neaktivnosti, time se sprječava pristup računalu i podacima kada korisnik nije aktivan. Prilikom prijenosa podataka s računala na računalo svakako bi trebalo izbjegavati kopiranje podataka na razne prijenosne uređaje jer se tako gubi kontrola nad količinom podataka i mjestima njihove pohrane.

U današnje vrijeme kada svaki radnik ima pametan uređaj preko kojeg pristupa svojoj elektroničkoj pošti kako bi mogao komunicirati s poslovnim partnerima, može doći do velike povrede u dijeljenju podataka. Prilikom korištenja službene *e-mail* adrese imamo pristup svim privicima kao što su poslovni akti, poslovna dokumentacija o zaposlenicima i slično, pa lako dolazi do propusta u sigurnosti. Iz navedenog razloga potrebno je zaštititi uređaje s pinom s kojim se otključava zaslon te osigurati da se podaci prilikom krađe uređaja ili u slučaju gubitka mogu obrisati s drugog uređaja.

Kako bi se podaci zaštitili u što većem obujmu, Uredba preporučuje anonimizaciju, pseudonimizaciju i minimizaciju podataka. Prema Općoj uredbi o zaštiti podataka, ako se proces anonimizacije provede na pravilan način, prikupljeni podaci više nisu informacije koje bi mogle poslužiti za prepoznavanje određene osobe te se kao takve imaju pravo koristiti, obrađivati i objavljivati bez privole vlasnika podataka. Razlika između anonimizacije i pseudonimizacije je ta da se kod pseudonimizacije ne uklanjaju svi identifikatori iz podataka nego se smanjuje način na koji su ti podaci povezani s određenim osobama.

Kod maskiranja podataka skup podataka o fizičkim osobama procesira se na način kako originalne vrijednosti ne bi bile prepoznatljive. Maskirane podatke nije moguće ponovno identificirati pa oni prestaju biti pod uredbom GDPR-a pa ih je tako moguće koristiti i upotrebljavati u sve svrhe.

7. ULOGA AGENCIJE ZA ZAŠTITU OSOBNIH PODATAKA KAO NADZORNOG TIJELA U RH

Prema članku 51. Uredbe „svaka država članica osigurava jedno ili više neovisnih tijela javne vlasti odgovornih za praćenje primjene ove Uredbe kako bi se zaštitila temeljna prava i slobode pojedinca u pogledu obrade i olakšao slobodni protok osobnih podataka unutar Unije“.[20]

Kako se usklađenje s Uredbom ne bi zloupotrebljavalo te kako bi se provodilo na što ispravniji način, nadzorna tijela mogu izdati neke od mjera kojima mogu sankcionira tvrtke koje se ne drže propisa.

Mjere su[21]:

- upozorenje
- opomena
- zabrana obrade
- novčane kazne.

Agencija za zaštitu osobnih podataka (u daljnjem tekstu AZOP) u Hrvatskoj ima ulogu nadzora u obradi osobnih podataka te joj je zakonom propisan ustroj, financiranje, ovlasti i dužnosti te poslovi i funkcije koje smije obavljati. Zakonom su definirani svi glavni pojmovi kojima agencija barata te je također propisano na koji način se evidencije moraju prijaviti AZOP-u i kako se evidentiraju promjene te kako se zbirke podataka moraju voditi. AZOP provodi nadzor nad postupanjem s podacima koji su prikupljeni. Agencija također može utvrditi kršenje zakona. Glavna zadaća AZOP-a je podizanje svijesti o zaštiti osobnih podataka kao i važnost zaštite osobnih podataka te predlaganje mjera za stručno usavršavanje službenika uz koje bi provedba zakona bila jednostavnija i lakša za prihvaćanje svim obveznicima primjene zakona. AZOP prati uređenje zaštite osobnih podataka u drugim

[20] https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=EN 12.04.2020.

[21] https://gdprinformer.com/hr/vodic-kroz-gdpr 13.03.2021.

zemljama, nadzire iznošenje osobnih podataka iz Hrvatske, također izrađuje letke kojima se informiraju ispitanici o njihovim pravima i obvezama. AZOP provodi radionice i seminare na kojima se iznose preporuke za unapređenje zaštite osobnih podataka, daje se mišljenje o specifičnim slučajevima ili scenarijima na koje se dolazi u poslovanju te se predlažu poboljšanja za organizacijske i tehničke mjere zaštite.

Ako dođe do nadzora od strane AZOP-a, dokumentacija koja je obavezna i koja će se u najviše slučajeva tražiti na uvid je sljedeća: dokument na kojem je navedena fizička osoba ovlaštena za zastupanje tvrtke, pravilnik o obradi osobnih podataka ili politike o privatnosti, obavijesti koje se pružaju ispitanicima o njihovim pravima, dokumentacija iz koje je vidljiva ovlast zaposlenika ili vanjskih suradnika, evidencije aktivnosti obrade, izjave o povjerljivosti, ugovor s izvršiteljem obrade ako postoji izvršitelj obrade i, najvažnije, dokumentacija koja se odnosi na mjere organizacijske i tehničke zaštite.

Nadzorno tijelo u Hrvatskoj AZOP mora djelovati potpuno neovisno, a država je ta koje mora osigurati resurse – kako ljudske, tako tehničke i financijske, prostor te potrebnu infrastrukturu kako bi agencija mogla obavljati svoje zadaće. Agencija je u svojem radu samostalna i neovisna te za svoj rad odgovara Hrvatskome saboru. Jedna od zadaća AZOP-a je osvješćivanje javnosti o rizicima, pravima, pravilima i mjerama te mora pružiti ispitanicima informacije o njihovim pravima, rješavati pritužbe te surađivati s ostalim nadzornim tijelima država članica EU. Kako je AZOP i savjetodavno tijelo, oni savjetuju Hrvatski sabor, Vladu i druge institucije javne vlasti po pitanju administrativnih mjera koje se odnose na obradu i postupanje s podacima. Izdaju mišljenja i odobravaju nacrte kodeksa ponašanja te donose standardne klauzule o zaštiti podataka.

Prilikom određivanja kazni, upozorenja, zabrana te opomena nadzorno tijelo dužno je poštovati međunarodne i hrvatske zakone koji definiraju navedeno područje.

Zakonski okvir koji se odnosi na zaštitu osobnih podataka u Hrvatskoj obuhvaća sljedeće sustave propisa[22]:

- Zakon o provedbi Opće uredbe o zaštiti podataka – NN 42/18

[22] https://azop.hr/zakonodavni-okvir/zakonodavstvo/nacionalno-zakonodavstvo 13.02.2021.

- Ustav Republike Hrvatske, Narodne novine, broj 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 05/14
- Zakon o potvrđivanju konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, Narodne novine – međunarodni ugovori 4/05
- Zakon o potvrđivanju izmjena i dopuna konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka, ETS br. 108, koje europskim zajednicama omogućavaju pristupanje, Narodne novine – Međunarodni ugovori 12/05
- Kazneni zakon, Narodne novine 68/18
- Konvencija za zaštitu ljudskih prava i temeljnih sloboda (Međunarodni ugovori 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10
- Direktiva EU parlamenta i Vijeća o obradi osobnih podataka i zaštiti privatnosti na području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)
- Direktiva EU parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela za zaštitu podataka
- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga čl. 30 (NN 64/18).

Agencija je dužna pokrenuti postupak kaznene ili prekršajne odgovornosti prema nadležnim tijelima ako uoči nesukladnosti u radu i obradi s osobnim podacima.

Ako se greške odnose na neke administrativne pogreške u vođenju evidencije, obavještavanju ispitanika o povredama podataka ili komunikaciji s nadzornim tijelom, kazna za prekršaje može biti najviše 10 milijuna eura ili 2 % ukupnog prometa za prethodnu godinu, odnosno uzima se veći iznos. Za teška kršenja odredbe za zaštitu podataka predviđene su kazne od 20 milijuna eura ili 4 % ukupnog godišnjeg prometa za prethodnu godinu. AZOP u svojem djelokrugu poslovanja ima mogućnosti provoditi revizije i istrage o primjeni zaštite osobnih

podataka te može ishoditi pristup svim osobnim podacima i informacijama koje su joj nužne za obavljanje revizije. Ako utvrdi nepravilnosti koje mogu dovesti do kaznenih djela, ima mogućnost zapečatiti sustave pohrane i obavijestiti nadležnu policijsku postaju ili državno odvjetništvo o saznanjima.

Što se tiče nadzora izvan Europske unije, oformljena je komisija koja je ovlaštena utvrditi pridržavaju li se sve članice Europske unije, a i države izvan EU svih stavaka uredbe i imaju li odgovarajuću razinu zaštite osobnih podataka. AZOP prati uređenje zaštite osobnih podataka u inozemstvu i surađuje s tijelima za zaštitu država članica Europske unije.

Ako zemlja koja nije u Europskoj uniji ima odgovarajuću razinu zaštite osobnih podataka, Europska unija može izdati odluku o primjerenosti. Pomoću takve odluke omogućava se lakši prijenos osobnih podataka izvan EU s odgovarajućom razinom zaštite osobnih podataka bez dodatnih zaštitnih mjera, odnosno prijenos u zemlju koja ima odluku o primjerenosti izjednačuje se s prijenosom podataka unutar EU. Da bi se odluka usvojila, mora ju usvojiti Europska komisija, a i odobriti predstavnici zemalja Europske unije. Isto tako, traži se mišljenje Europskog odbora za zaštitu osobnih podataka. Zemlje koje su do sada prepoznate kao zemlje sa zadovoljavajućom razinom zaštite su: „Andora, Argentina, Kanada, Farski otoci, Izrael, otok Man, Japan, Jersey, Novi Zeland, Švicarska i Urugvaj[23]“.

Agencija je dužna svake godine podnositi Hrvatskom saboru izvješće o radu koje mora sadržavati podatke o praćenju provedbe Uredbe i mora biti u skladu sa zakonom koji je propisan sa sadržajem godišnjeg izvješća. Navedeno izvješće se na zahtjev Europskog odbora za zaštitu osobnih podataka dostavlja njima na uvid.

[23] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_hr#documents 19.12.2020.

8. ISTRAŽIVANJE O IMPLEMENTACIJI OPĆE UREDBE O ZAŠTITI PODATAKA (GDPR) U JAVNIM I PRIVATNIM PODUZEĆIMA

CILJ ISTRAŽIVANJA

Cilj istraživanja je istražiti anketnim upitnikom na koji način i u kojoj mjeri je implementacija Opće uredbe o zaštiti podataka u javnim i privatnim organizacijama provedena. Kako bi istražili implementaciju postavili smo si četiri ključna pitanja na koja želimo dobiti odgovor:

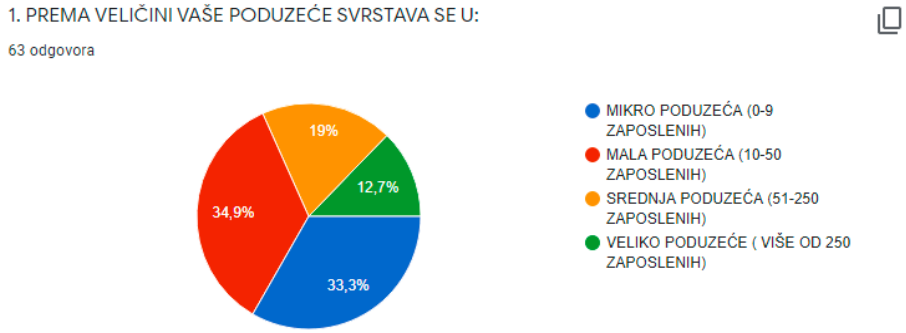
- Na koji način su organizacije prilagodile svoje poslovanje
- Jesu li upoznate s uredbom
- Primjenjuju li uredbu u poslovanju
- Jesu li njihovi ispitanici upoznati s pravima na način kako Uredba predviđa

U istraživanju su sudjelovala 63 ispitana poduzeća s područja sjeverozapadne Hrvatske. Poduzeća koja su se odazvala na ispunjavanje ankete su iz privatnog i javnog sektora.

METODOLOGIJA ISTRAŽIVANJA

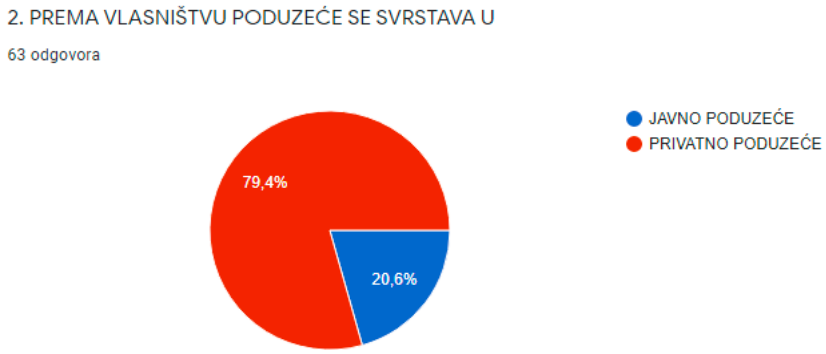
Metoda provođenja ovog istraživanja je anketni upitnik. Anketa je provedena putem Googleova obrasca s unaprijed ponuđenim odgovorima kako bi se olakšalo odgovaranje te smanjilo vrijeme potrebno za ispunjavanje ankete. Ciljana skupina ispitanika su javne i privatne organizacije na području sjeverozapadne Hrvatske. Anketa je započela 22. veljače i trajala do 28. veljače 2021. godine. Anketa se provodila preko Google obrasca te je nakon popunjavanja ankete i dobivanja zadovoljavajučeg broja odgovora ista importirana u Excel. Nakon importiranja podataka i obrade svih grafova sljedi tumačenje dobivenih informacija.

REZULTATI ISTRAŽIVANJA



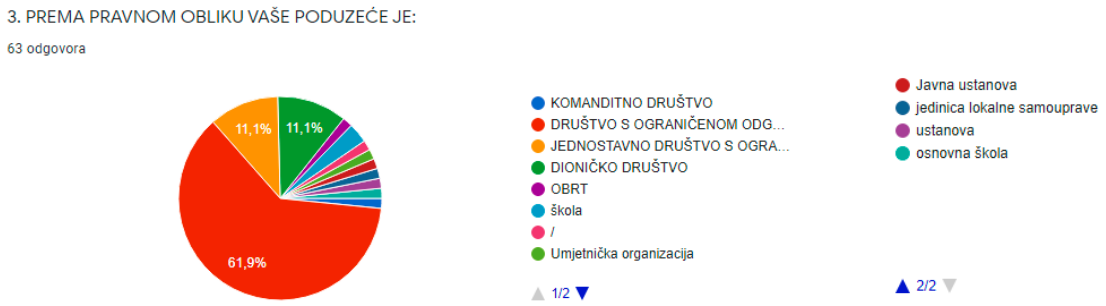
Grafikon 1 – Veličina poduzeća

Na početku ankete postavili smo pitanje o veličini poduzeća kako bismo vidjeli koji poduzetnici su se u najvećoj mjeri odazvali anketi. Najveći postotak odgovora došao je od malih poduzetnika: 34,9 %, zatim slijede mikro poduzeća: 33,3 %, nakon toga srednja poduzeća: 19 % i na kraju s najmanjim odazivom je bilo velikih poduzeća samo 12,7 %.



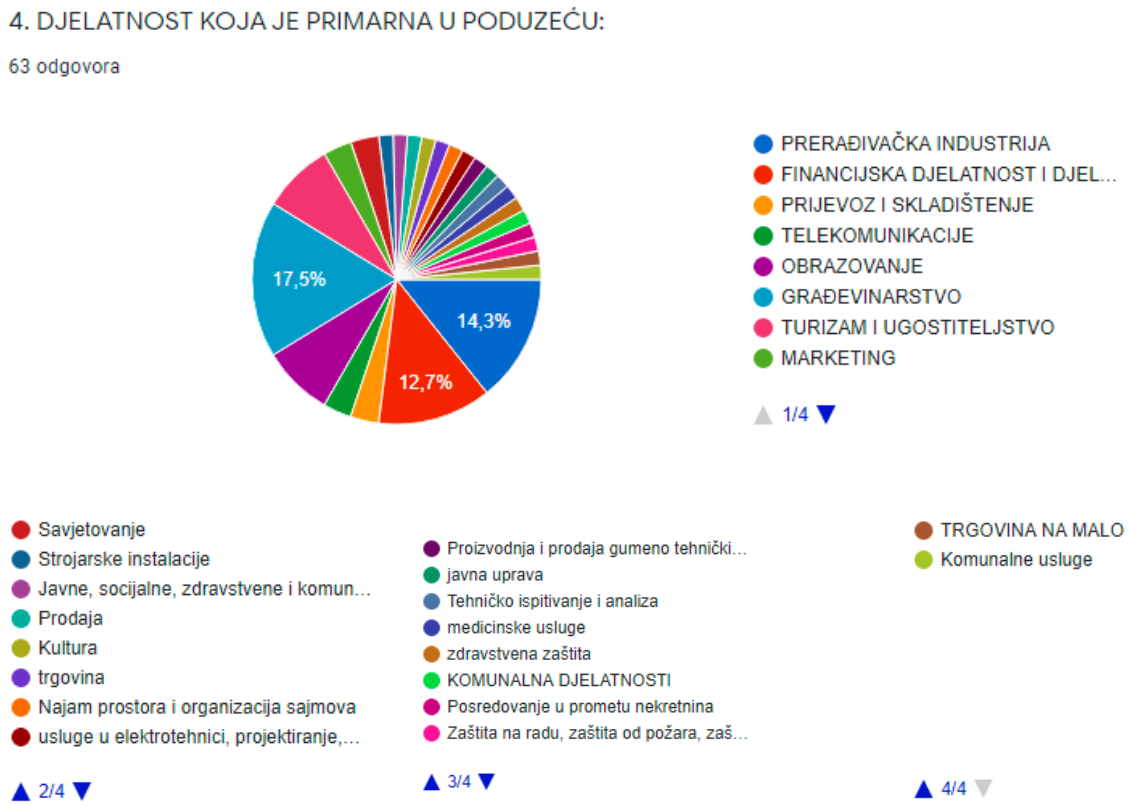
Grafikon 2 – Vlasništvo

U drugom pitanju prema vlasništvu saznali smo da je većina ispitanika bila s privatnog sektora: 79,4 %, a ostatak iz javnog sektora: 20,6 % .



Grafikon 3 – Pravni oblik

Prema pravnom obliku poduzeća 61,9 % njih je dioničko društvo s ograničenom odgovornošću, zatim je 11,1 % njih dioničko društvo i jednostavno društvo s ograničenom odgovornošću. 4,8 % od ukupnih odgovora su bile škole, dok su u 1,6 % odgovori stigli od obrta, lokalnih samouprava, javnih ustanova, umjetničkih organizacija i komanditnih društava.

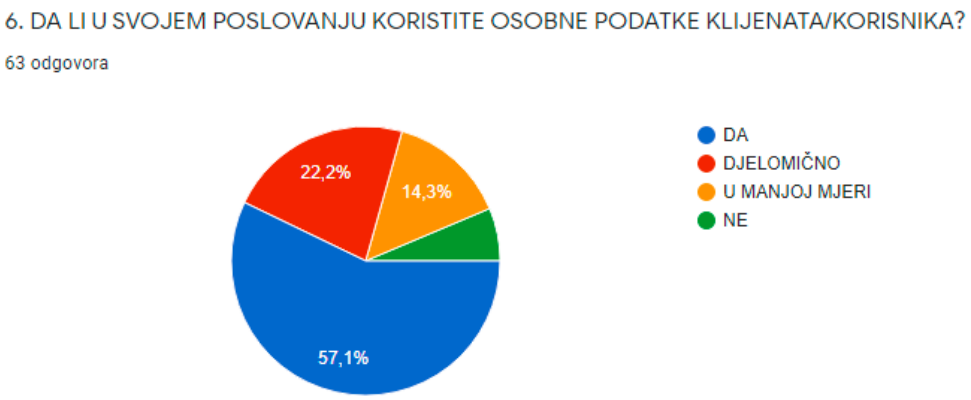


Grafikon 4 - Djelatnost

Na četvrtom pitanju tražili smo da se ispitanici izjasne koja djelatnost je pretežita u poduzeću: 17,5 % anketiranih je bilo iz građevine, 14,3 % iz prerađivačke industrije, 12,7 % iz financijske djelatnosti i djelatnosti osiguranja, 7,9 % odgovora je bilo iz područja obrazovanja i turizma i ugostiteljstva, 4,8 % odgovora je bilo iz zdravstvene djelatnosti, ispitanici koji imaju djelatnosti prijevoza i skladištenja, telekomunikacije, marketinga i savjetovanja te komunalnu djelatnost kao primarnu čine 3,2 % anketiranih dok je 1,6 % ispitanika bilo s područja prodaje, javne uprave, tehničkog ispitivanja, elektrotehnike, najma prostora i organiziranja sajmova, zaštite na radu, strojarskih instalacija, kulture, posredovanja u prodaji nekretnina i proizvodnje i prodaje gumeno-tehničkih proizvoda.

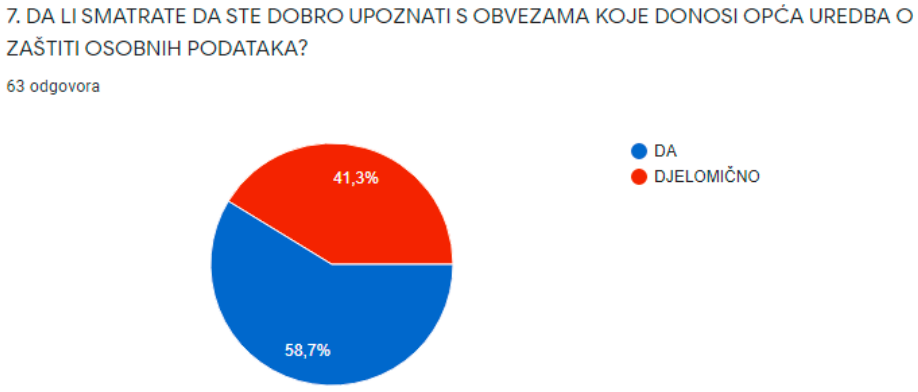
Grafikon 5 – Pravni temelj

Kako bismo saznali imaju li ispitanici uopće temelje za implementaciju Opće uredbe o zaštiti podataka, pitali smo ih znaju li na koji pravni temelj se oslanjaju na što je 92,1 % njih odgovorilo potvrdno, dok je njih 7,9 % odgovorilo da ne znaju što je temelj prilikom obrada osobnih podataka.



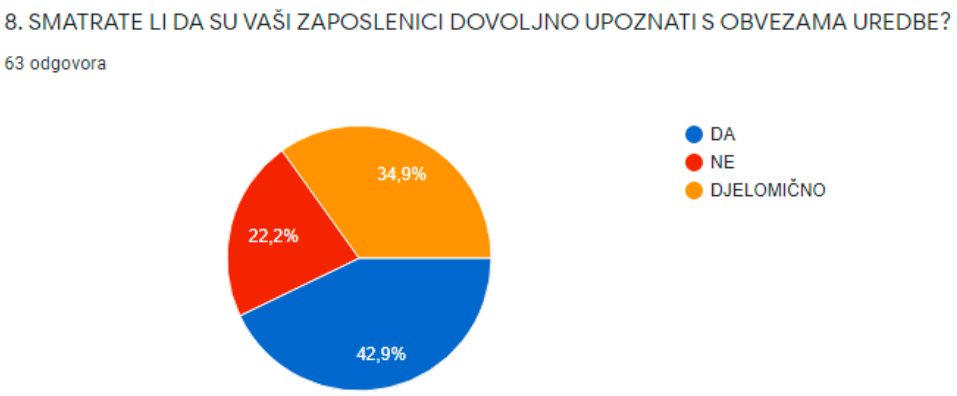
Grafikon 6 – Korištenje GDPR-a

Osobne podatke klijenata u svojem poslovanju koristi 57,1 % ispitanih, njih 22,2 % djelomično ih koristi dok je njih 14,3 % odgovorilo da koriste osobne podatke u manjoj mjeri, dok je 6,3 posto ispitanih negiralo da u poslovanju koriste osobne podatke što je vjerojatno povezano sa činjenicom da nisu dovoljno upoznati s Uredbom te ne shvaćaju na pravilan način što sve obuhvaća obrada osobnih podataka.



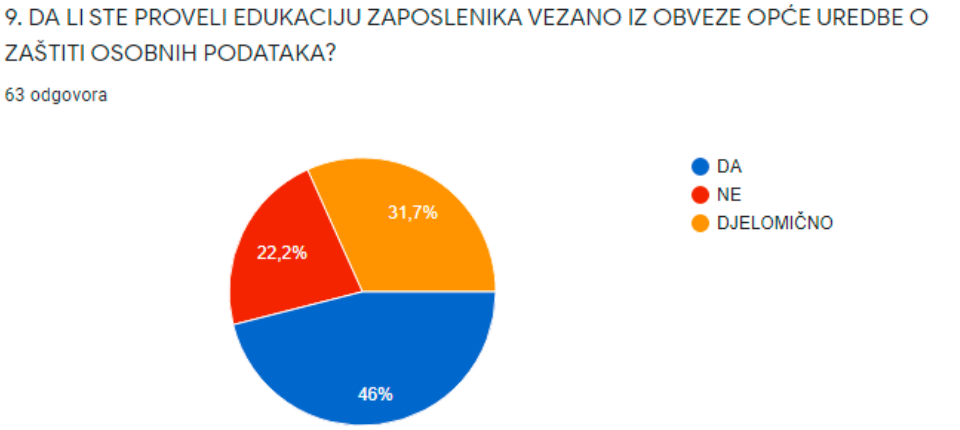
Grafikon 7 – Upoznatost s Uredbom

Odgovori na ovo pitanje nadovezuju se s prethodnim jer vidimo da je 58,7 % ispitanika odgovorilo da je dobro upoznato s time što Uredba nosi, a vidimo da je na prethodnom pitanju skoro isti broj ispitanika odgovorio da koriste osobne podatke. Možemo zaključiti da ostatak od 41,3 % su oni koji su se na pitanje broj 6. izjasnili s ne, u manjoj mjeri i djelomično jer nisu na dobar način upoznati s Uredbom i svim njezinim stavkama.



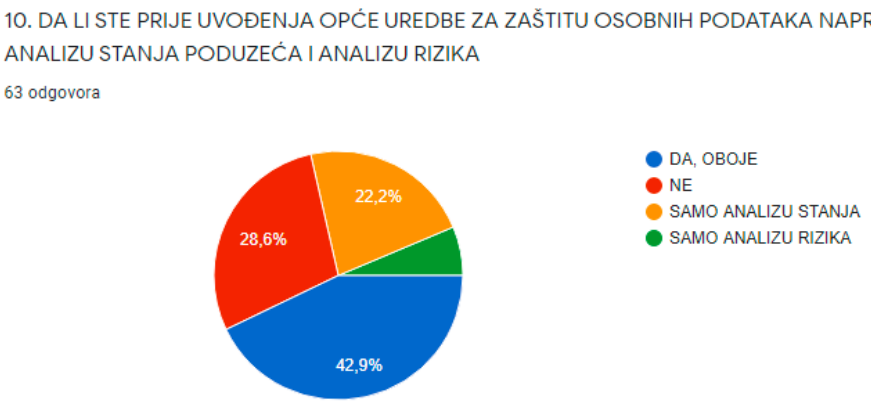
Grafikon 8 – Zaposlenici

Na pitanje jesu li zaposlenici ispitanih poduzeća upoznati s Uredbom, 42,9 % odgovorilo je da su dovoljno upoznati, njih 34,9 % smatra da su zaposlenici djelomično upoznati s Uredbom i svime što ona nosi, dok 22,2 % ispitanih odgovorilo da njihovi zaposlenici nisu upoznati s obvezama i pravima iz Uredbe.



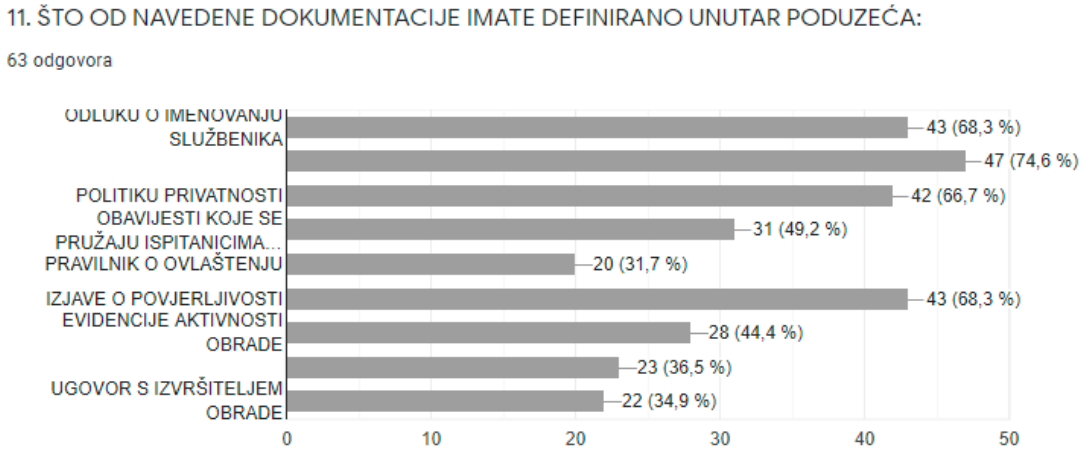
Grafikon 9 – Educiranost zaposlenika

Edukaciju svojih zaposlenika nije provelo 22,2 % ispitanih što možemo povezati s pitanjem broj 8. gdje je isti postotak poduzetnika izjavio da misle da zaposlenici nisu upoznati s obvezama iz Uredbe, 31,7 % ispitanih je provelo u određenoj mjeri edukaciju svojih zaposlenih, dok je 46,0 % ispitanih provelo nekakve edukacije na temu Opće uredbe o zaštiti podataka.



Grafikon 10 – Analiza poduzeća

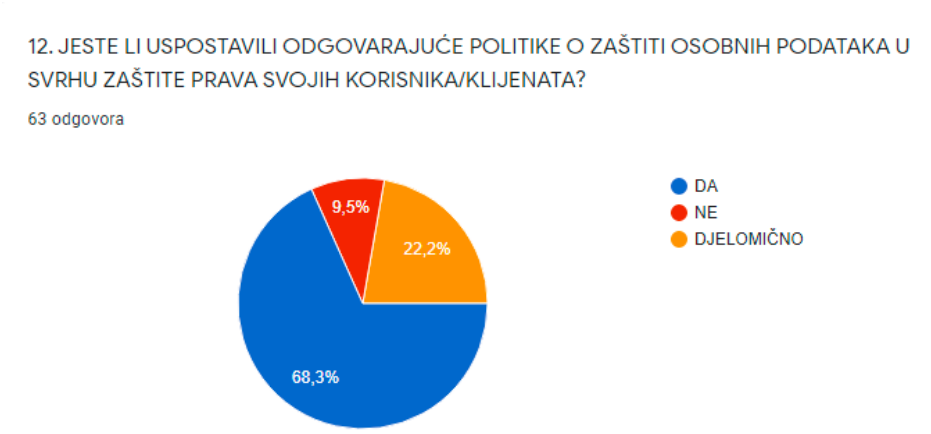
Da bi provjerili stanje u svojem poduzeću i vidjeli na što sve moraju obratiti pozornost prilikom uvođenja i implementacije Uredbe, 42,9 % ispitanih provelo je analizu stanja i analizu rizika u svojoj firmi, 28,6 % ispitanih nije provelo ni jednu analizu, 22,2 % provelo je samo analizu stanja, a samo 6,3 % provelo je samo analizu rizika.



Grafikon 11 – Dokumentacija

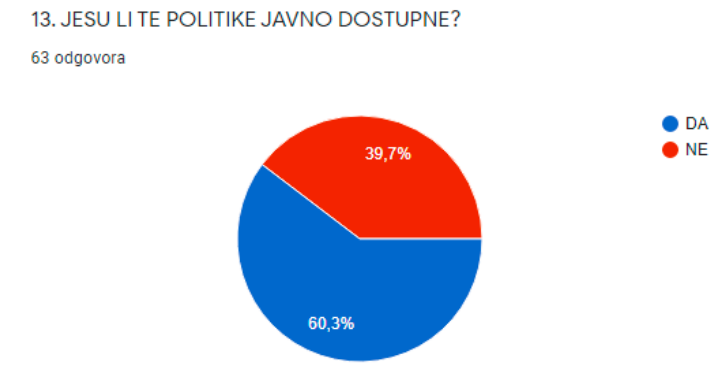
Jedanaestim pitanjem htjeli smo utvrditi u kojoj mjeri su ispitana poduzeća izradila potrebnu dokumentaciju te imaju li sve što je potrebno. Više od 50 % ispitanih ima izrađenu odluku o imenovanju službenika, pravilnik o zaštiti osobnih podataka, politiku privatnosti i izjavu o povjerljivosti. Obavijesti koje se pružaju ispitanicima i evidencije o aktivnosti ima između 40

i 50 posto ispitanih, dok manje od 40 % ima izrađene pravilnike o ovlaštenju, dokumente koji prikazuju načine prikupljanja osobnih podataka i ugovor s izvršiteljima obrade.



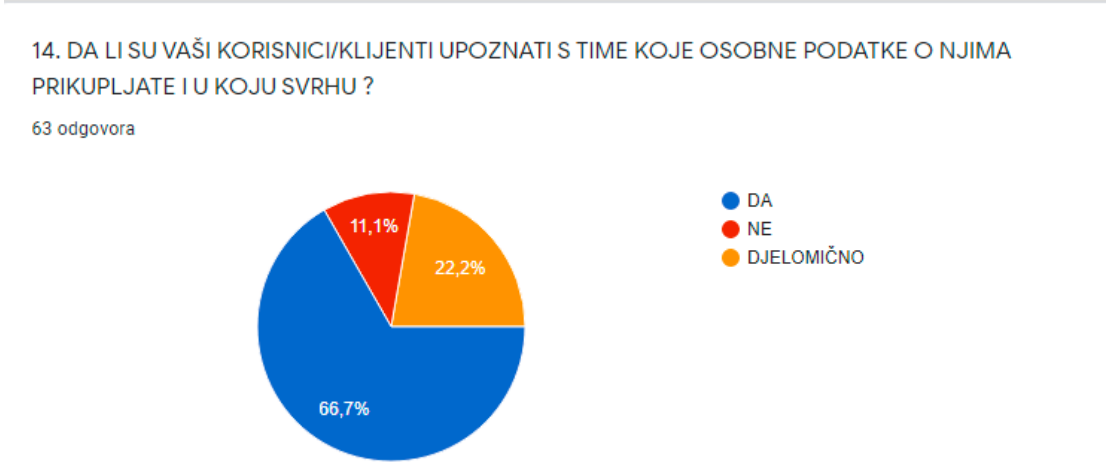
Grafikon 12 – Politika GDPR-a

Kako bi zaštitili prava svojih korisnika i klijenata, njih 68,3 % izradilo je ogovarajuće politike koje traži Uredba, njih 22,2 % ima djelomično izrađene politike, dok njih 9,5 % smatra da politike nisu bitne te ih nisu ni izradili.



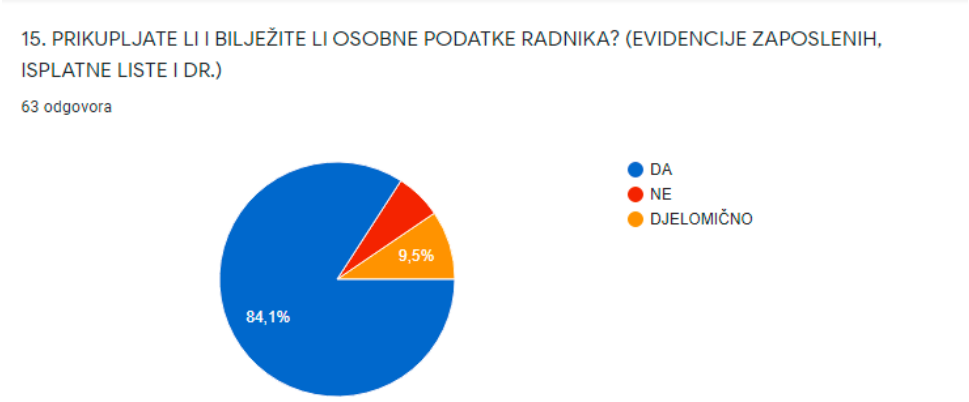
Grafikon 13 – Dostupnost politika

Na pitanje jesu li politike o zaštiti osobnih podataka javno dostupne, 60,3 % ispitanih odgovorilo je potvrdno dok ostalih 39,7 % smatra da nije potrebno javno objavljivati.



Grafikon 14 – Prikupljanje osobnih podataka

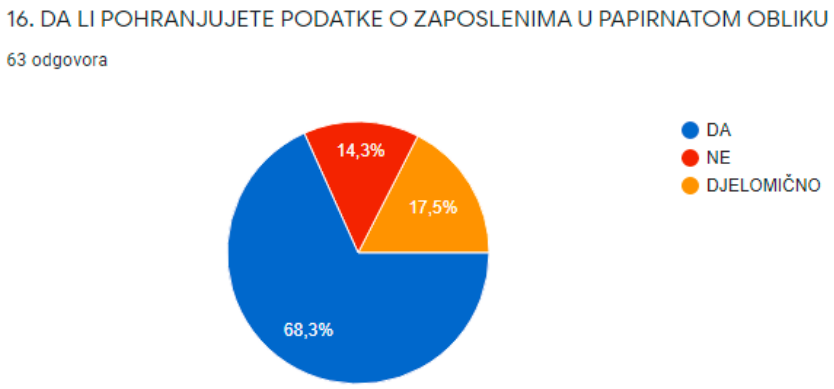
Od ukupnog broja ispitanih kod njih 66,7 % ne moramo se brinuti hoćemo li biti upoznati koje osobne podatke prikupljaju i u koju svrhu, kod njih 22,2 % korisnici su djelomično upoznati s prikupljanjem podataka i svrhe prikupljanja, dok kod njih 11,1 % korisnici nisu uopće upoznati s podacima koji se prikupljaju i u koju svrhu se ti podaci koriste što pokazuje da poduzetnici i dalje nisu shvatili svoje obveze iz Uredbe.



Grafikon 15 – Prikupljanje podataka zaposlenika

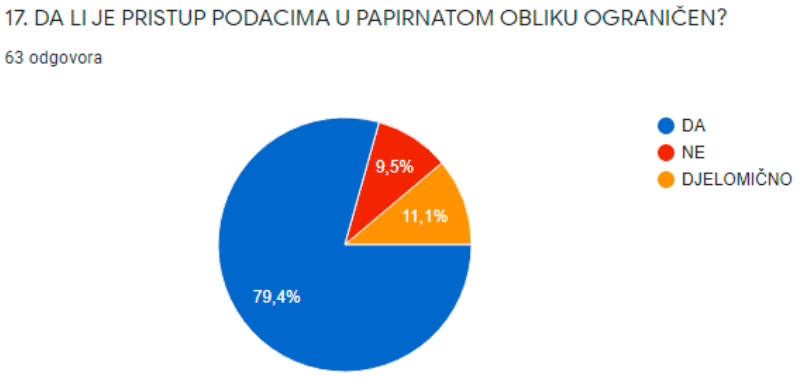
Na pitanje bilježe li i čuvaju osobne podatke svojih zaposlenih, njih 84 % odgovorilo je da čuva, 9,5 % radi to djelomično, dok 6,3 % ispitanih poduzetnika ne bilježi osobne podatke svojih zaposlenih. Tvrtke koje su se na ovom pitanju izjasnile da ne bilježe podatke svojih zaposlenih u nekoj mjeri krše neke druge zakone jer je svima poznato da se dokumentacija kao što su plaće zaposlenih po Zakonu o računovodstvu mora čuvati trajno, te bi bilo dobro

detaljnije ispitati u kojem smislu su navedeni ispitanici mislili da ne čuvaju osobne podatke zaposlenih.



Grafikon 16 – Pohranjivanje podataka

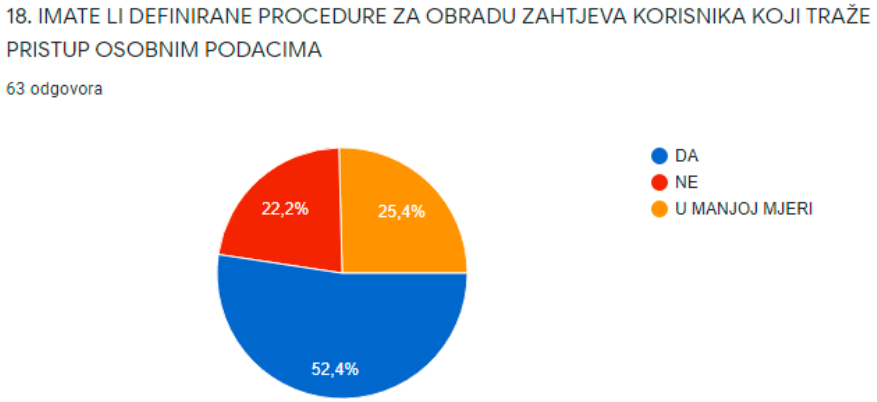
Podatke o zaposlenima ne pohranjuje u papirnatom obliku 14,3 %, njih 17,5% ima podatke pohranjene djelomično što podrazumijeva papirnati i neki od elektroničkih oblika, dok njih 68,3 % pohranjuje podatke o zaposlenima u papirnatom obliku.



Grafikon 17 – Ograničenost pristupa

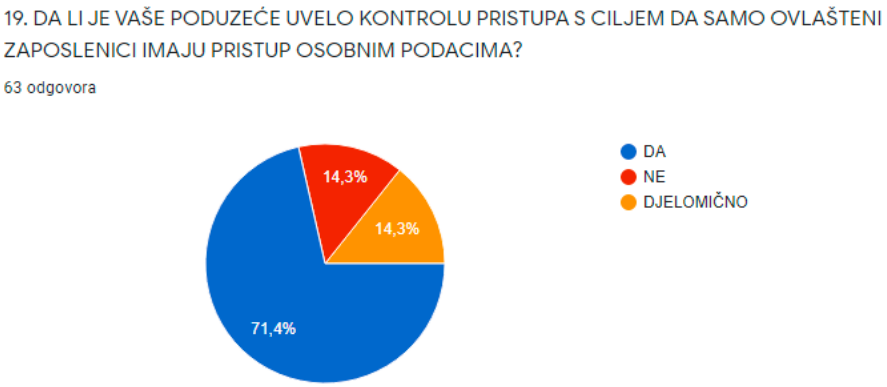
U šesnaestom pitanju ispitali smo čuvaju li podatke o zaposlenima u papirnatom obliku, u pitanju broj sedamnaest zanimalo nas je čuva li se dokumentacija u papirnatom obliku i je li takva dokumentacija na pravilan način zbrinuta, odnosno imaju li pristup takvim podacima samo ovlaštene osobe. Ograničeni pristup takvoj dokumentaciji ima 79,4 % anketiranih, njih

11,1 % ima djelomično ograničen pristup, dok kod njih 9,5 % pristup takvoj dokumentaciji uopće nije ograničen što znači da svi zaposleni imaju pristup.



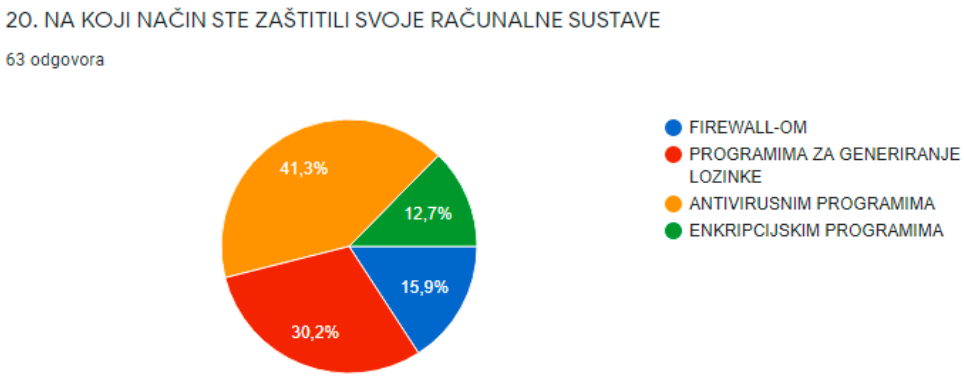
Grafikon 18 – Procedure pristupa

Ako netko od korisnika ili zaposlenih zatraži pristup svojim osobnih podacima, samo njih 52,4 % ima na pravilan način definirane procedure kako izvršiti takav zahtjev, njih 25,4 % ima u manjoj mjeri definirane procedure, dok njih 22,2 % nema uopće propisane procedure za obradu zahtjeva korisnika.



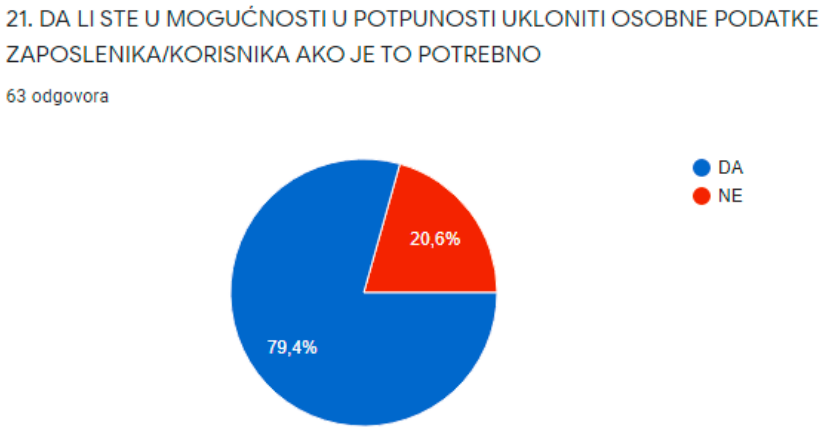
Grafikon 19 – Kontrola pristupa

Kako bi kontroliralo pristup osobnim podacima 71,4 % anketiranih ograničilo je pristup podacima samo zaposlenicima koji imaju ovlaštenje za pristup, 14,3 % posto kontrolira djelomično pristup ili uopće ne kontrolira pristup osobnim podacima u poduzeću.



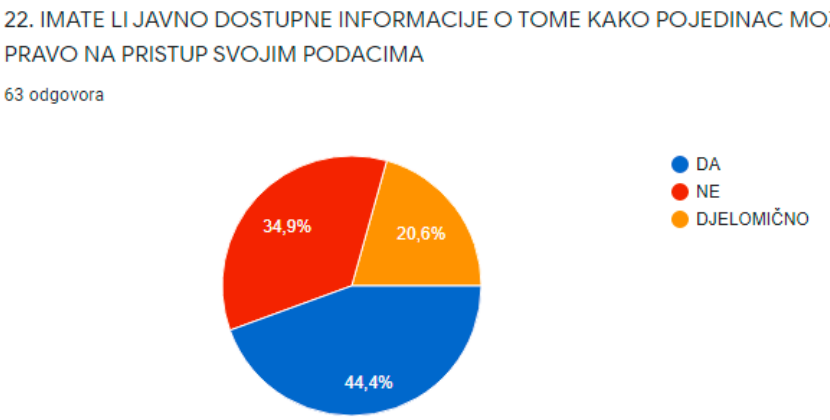
Grafikon 20 – Zaštita osobnih podataka

Svoje računalne sustave 41,3 % anketiranih zaštitilo je antivirusnim programima, njih 30,2 % koristi programe za generiranje lozinke da bi otežali pristup osobnim podacima koji se čuvaju u elektroničkom obliku, 15,9 % postavilo je *firewall* na svoje računalo, dok je samo 12,7 % anketiranih svoje podatke zaštitilo nekim od enkripcijskih programa.



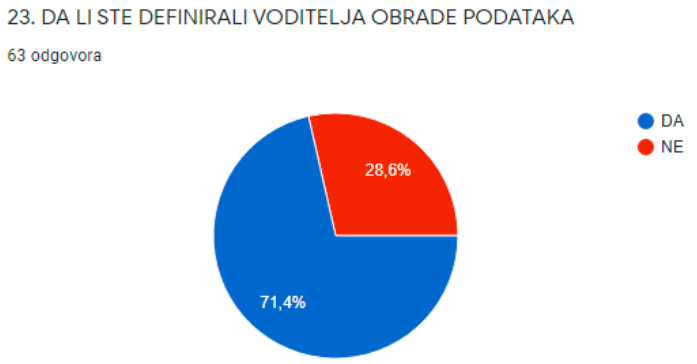
Grafikon 21 – Uklanjanje osobnih podataka

Ako korisnik ili zaposlenik zatraži uklanjanje osobnih podataka, što je jedno od prava i obveza prema Općoj uredbi o zaštiti podataka, njih 79,4 % moglo bi ukloniti osobne podatke dok njih 20,6 % nije u mogućnosti ukloniti osobne podatke korisnika na način na koji to zahtijeva Uredba.



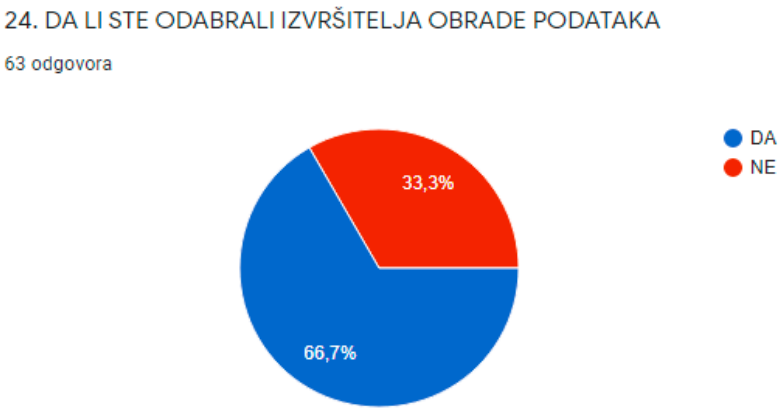
Grafikon 22 – Pravo na pristup

Kako bi korisnik ili zaposlenik imao informaciju o svojim pravima i načinu na koji to može ostvariti, 44,4 % anketiranih ima javno dostupne informacije, njih 34,9 % nema uopće dostupne informacije o tome kako ostvariti pristup svojim podacima dok 20,6 % ispitanih ima djelomično dostupne informacije kako ostvariti pristup svojim osobnim podacima.



Grafikon 23 – Voditelj obrade

Od ukupno ispitanih 71,4 % poduzeća definiralo je voditelja obrade osobnih podataka, dok njih 28,6 % nije odredilo voditelja obrade.

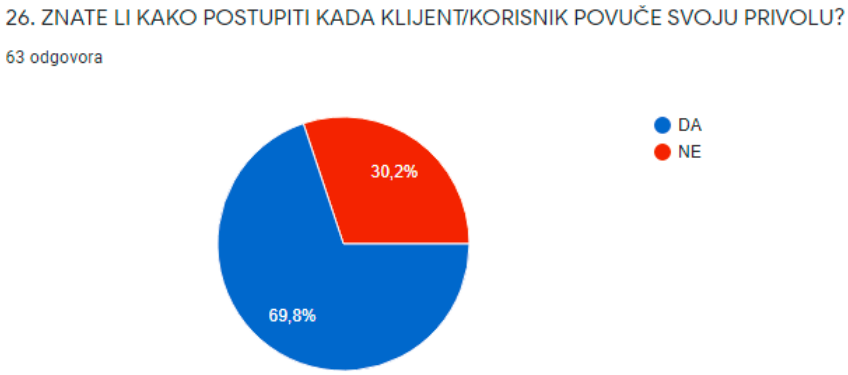


Grafikon 24 – Izvršitelj obrade

Izvršitelja obrade u svojem poduzeću odabralo je 66,7 % ispitanih poduzeća dok njih 33,3 % nije imenovalo izvršitelja obrade. Pitanje o izvršitelju i voditelju obrade još je jedan pokazatelj da se poduzeća nisu na pravilan način uskladila s Općom uredbom o zaštiti podataka te da postoji još puno mjesta za unapređenje i edukaciju kroz koju bi tvrtke shvatile na koji način moraju postupati te koje su njihove obveze.

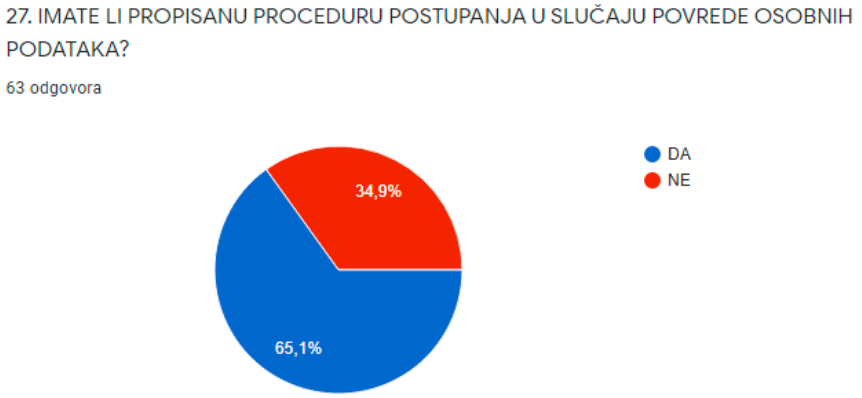
Grafikon 25 – Službenik za zaštitu osobnih podataka

Ako je pravno određeno da poduzeće mora imati službenika, njih 54 % imenovalo je tog službenika, dok njih 46 % nije imenovalo službenika za zaštitu osobnih podataka.



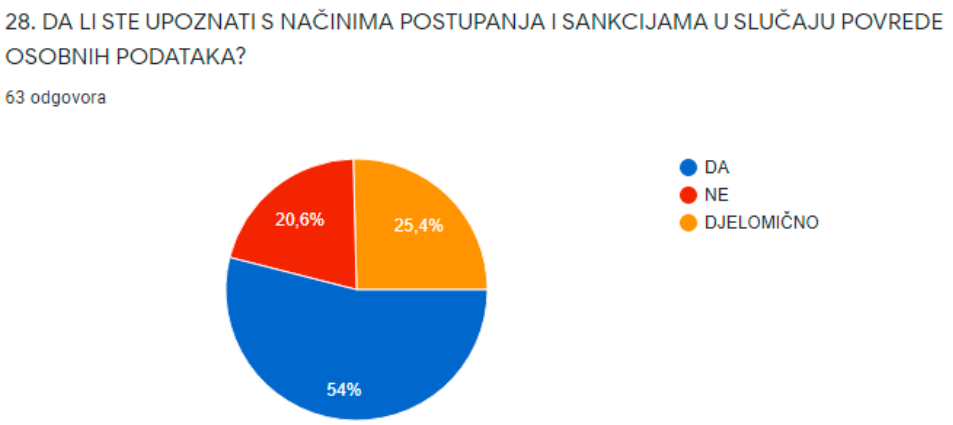
Grafikon 26 – Postupak povlačenja privole

Kako postupiti kada klijent ili korisnik povuče privolu danu za obradu i korištenje osobnih podataka? 69,8 % ispitanih zna način kako postupiti i koje korake poduzeti da bi se takvi osobni podaci osigurali i prestali koristiti, dok njih 30,2 % ne zna kako ukloniti osobne podatke kada korisnik povuče privolu.



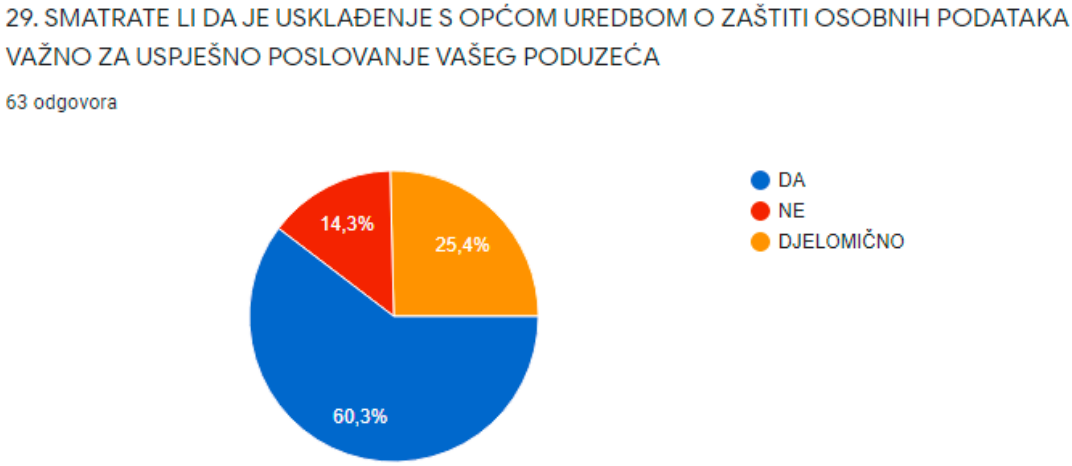
Grafikon 27 – Procedure u slučaju povrede

Kako reagirati ako se dogodi povreda kod postupanja s osobnim podacima? 65,1 % anketiranih ima propisane procedure za takve situacije, dok njih 34,9 % nema procedure postupanja u slučaju povrede osobnih podataka.



Grafikon 28 – Sankcije kod povrede osobnih podataka

Ako nadzorna agencija utvrdi povredu Opće uredbe o zaštiti podataka, 54 % ispitanih zna koje postupke i sankcije mogu očekivati, 25,4 % ispitanih je djelomično upoznato sa sankcijama koje ih očekuju dok njih 20,6 % nije upoznato uopće sa sankcijama i načinom postupanja u slučaju povrede.



Grafikon 29 – Uspješnost u poslovanju

Pitanje *Smatrate li da je usklađenost s Općom uredbom o zaštiti podataka važna za uspješno poslovanje?* najbolje pokazuje stanje i način razmišljanja poduzetnika kad je u pitanju Uredba. Njih 60,3 % smatra da je usklađenje s Uredbom bitno za uspješno poslovanje svoje tvrtke, 25,4 % smatra da im usklađenost s Uredbom samo djelomično pomaže kod uspješnosti u poslovanju, dok njih 14,3 % smatra kako usklađenje s Uredbom nema nikakvog utjecaja na uspješnost poslovanja njihovog poduzeća.

Rezultati ankete koju smo proveli na području sjeverozapadne Hrvatske, u poduzećima iz javnog i privatnog sektora ne može poslužiti kao reprezentativan primjerak da bi se izvukli neki generalni zaključci. Međutim, dobivene rezultate ankete možemo koristiti kao preliminarne kao podlogu za neko veće istraživanje i donošenje zaključaka o trendu. Na Anketu je odgovorilo ukupno šezdeset tri ispitanika.

Podacima kojima raspolažemo nakon provedene analize došli smo do zaključka da su s Općom uredbom o zaštiti podataka upoznata skoro sva poduzeća koja su sudjelovala u anketi. Manji broj poduzeća nije upoznat s pravnim temeljima kojim ih Uredba obvezuje. Polovica ispitanih poduzeća nije upoznata s vrstama osobnih podataka koje definira Uredba te zbog toga smatraju da ne koriste osobne podatke u svojem poslovanju. Također, velik broj ispitanih svjestan je da nisu u dovoljnoj mjeri upoznati sa svim odredbama i da nisu na pravilan način educirali svoje zaposlene o pravima i obvezama koje nosi primjena Opće uredbe o zaštiti podataka. Prilikom uvođenja Uredbe preporučeno je provesti analizu stanja i analizu rizika kako bi se utvrdili rizici vezano za obradu podataka u poduzeću i kako bi se revidirali uočeni nedostaci. Nešto više od polovice ispitanika svjesno je važnosti provođenja analiza dok ostali smatraju da to i nije toliko bitno. Dvije trećine ispitanih poduzeća imaju napisane politike o zaštiti osobnih podataka te su i te politike javno dostupne kako bi svi zainteresirani znali na koji način će se postupati s njihovim osobnim podacima ako dođe do kršenje pravila o obradi podataka. Trećina poduzeća pohranjuje osobne podatke svojih zaposlenih u papirnatom obliku te ti podaci nisu adekvatno zaštićeni, i do njih se može nesmetano doći te tako dovesti poduzeće u nepotrebne reputacijske i normativne probleme. Skoro četvrtina ispitanih nije u mogućnosti ukloniti sve osobne podatke ako korisnik povuče svoju privolu, niti su uspostavili procedure koje će se provoditi prilikom povlačenja privole. Načina postupanja i sankcija koje slijede ako dođe do povrede osobnih podataka prilikom njihove obrade svjesna je tek polovina ispitanih. I, kao zaključak možemo reći da jedan dio poslodavaca ne smatra bitnim usklađenje s Općom uredbom o zaštiti podataka. U glavnom svi su čuli za Uredbu i upoznati su s njom u određenoj mjeri, ali prema rezultatima ankete tome ne pridaju veliki značaj jer se do sada nisu susreli s nadzorom AZOP-a do kojeg dolazi u koliko se dogodi gubitak, krađa ili nezakonita obrada podataka po prijavi ispitanika. Zaključno, još uvijek ima mnogo mjesta za napredak i poboljšanje stanja koje se može ostvariti s više edukacije AZOP-a te informiranja poslodavaca i zaposlenika o njihovoj osobnoj odgovornosti za stanje u području obrade osobnih podataka.

9. ZAKLJUČAK

Opća uredba o zaštiti podataka u Hrvatskoj je postala obavezna za primjenu od 25. svibnja 2018. godine za sve fizičke i pravne osobe u Europskoj uniji koje obrađuju osobne podatke građana EU u komercijalne ili profesionalne svrhe. Pravila koja nameće Opća uredba o zaštiti podataka prilikom stupanja na snagu nisu jednostavna i lako primjenjiva te su ih se obvezni pridržavati i sve druge organizacije izvan EU koje u svojem poslovanju obrađuju osobne podatke građana EU.

Zbog brzog razvoja interneta i digitalizacije poslovanja EU je kroz donošenje Uredbe o zaštiti podataka ostvarila cilj prije svega glede normativnog jačanja u zaštiti privatnost građana EU od prekomjerne obrade osobnih podataka, osiguravanja zakonitosti i transparentnosti u obradi podataka kao i pravu ispitanika na informiranost. Uloga voditelja obrade, izvršitelja obrade i službenika za zaštitu podataka dodatno je naglašena u Uredbi čime se jasnije definira i njihova odgovornost za zakonitu i transparentnu obradu osobnih podataka. Uloga AZOP-a kao regulatornog tijela je zakonom određen u smislu savjetodavne, nadzorne i korektivne uloge. AZOP poduzima niz aktivnosti u području edukacije pravnih i fizičkih osoba, informiranja i davanja stručnih mišljenja na upite građana i pravnih osoba preko svojih stranica, ali i izricanjem opomena, upozorenja te financijskih kazni kada su u pitanju teža kršenja odredbi iz Uredbe.

Fizičke osobe obrtnici koje zapošljavaju mali broj ljudi te nemaju velik broj poslovnih partnera lakše će se i brže prilagoditi Uredbi i, što je najbitnije, bez značajnijih troškova. Velika poduzeća će svoju prilagodbu morati provoditi duže vrijeme i vjerojatno s uključivanjem vanjskih suradnika koji donose i određene troškove.

Prilikom provođenja ankete na području sjeverozapadne Hrvatske uočeno je kako većina poslodavaca ima osnovne informacije o Uredbi i na neki način ju implementirala u svoje poslovanje. No, potrebno je još dodatne edukacije i upoznavanja poslodavaca s Uredbom jer jedan dio nije informiran o njihovoj osobnoj odgovornosti kao voditelja obrade.

Na kraju svega možemo donijeti zaključak da je usklađenje s Uredbom svakodnevna aktivnost, no za njezinu punu primjenu u praksi morat će proteći još određeno vrijeme kako bi svi subjekti u procesu spoznali kako ulaganje u zaštitu osobnih podataka nije trošak već investicija koja osigurava konkurentsku prednost i opstanak organizacije na tržištu.

10. LITERATURA

1. Agencija za zaštitu osobnih podataka: Vodič kroz Opću uredbu o zaštiti podataka (GDPR), Zagreb, dostupno na: https://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka - 26.03.2020.
2. Bisnode, brošura, Zaštita osobnih podataka, GDPR: Opća uredba o zaštiti osobnih podataka - utjecaj na poduzeća, Zagreb, 2018. – 12.03.2021.
3. Edukacija službenika za zaštitu osobnih podataka u privatnom sektoru - https://digitalnakomora.hr/e-ucenje/baza-znanja/1652 - 13.03.2021.
4. Godišnje izvješće o radu Agencije o zaštiti osobnih podataka za razdoblje od 01.01.-31.12.2018. godine https://azop.hr/wp-content/uploads/2020/12/izvjesce_azop_2018.pdf - 05.05.2020.
5. https://ec.europa.eu/croatia/what_is_digital_transformation_changing_hr 13.03.2021.
6. https://www.bisnode.hr/znanja-misli/nase-misli-znanje/kako-pripremiti-svoje-poduzece-za-opcu-uredbu-o-zastiti-podataka-gdpr/ 15.02.2021.
7. Information Commissioner s Office https://ico.org.uk/for-organisations/accountability-framework/risks-and-data-protection-impact-assessments-dpias/ -19.12.2020.
8. kako uskladiti poslovanje s općom uredbom o zaštiti osobnih podataka (GDPR) - https://digitalnakomora.hr/e-ucenje/baza-znanja/1624 - 12.03.2021.
9. Kazneni zakon RH (NN 125/11, 144/12, 56/15, 61/15) - https://www.zakon.hr/z/98/Kazneni-zakon - 13.02.2021.
10. Krakar, Z., Rotim Tomić, S., Žgela, M., Arbanas, K., Kišasond, T.,: Korporativna informacijska sigurnost, Fakultet organizacije i informatike, Varaždin, Zavod za informatičku djelatnost Hrvatske, Zagreb, 2014.
11. Luetić, A.,: Business intelligence i upravljanje opskrbnim lancem, Despot Infinitus, Zagreb, 2018.
12. Nacionalna razvojna strategija 2030 - https://hrvatska2030.hr/ 23.03.2021
13. Prijedlog zakona o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka https://www.sabor.hr/fgs.axd?id=4742 02.03.2020.

14. Priručnik za službenika za zaštitu osobnih podataka https://azop.hr/wp-content/uploads/2020/12/prirucnik-_za_dpo-t4data-hrv.pdf - 13.03.2021.
15. Spremić, M.,: Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Ekonomski fakultet u Zagrebu, Zagreb, 2017.
16. 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) https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=EN-12.04.2020.
17. Ustav Republike Hrvatske (2010) Zaštita ljudskih prava i temeljnih sloboda pročišćeni tekst, Narodne novine broj 05/14 - https://www.zakon.hr/z/94/Ustav-Republike-Hrvatske - 13.02.2021.
18. Vijeće Europe (1981) Konvencija 108, Konvencija 108 za zaštitu osoba glede automatizirane obrade osobnih podataka https://www.gdpr-2018.hr/33/konvencija-108-vijeca-europe-zakon-o-potvr-ivanju-konvencije-za-zastitu-osoba-glede-automatizirane-obrade-osobnih-podataka-i-dodatnog-protokola-uz-konvenciju-mu-br-04-05-uniqueidRCViWTptZHJmO-O7Qf9pYHRkOiBH6bJi/ -19.12.2020.
19. Zakon o pravu na pristup informacijama . (NN 25/13, 85/15) https://www.zakon.hr/z/126/Zakon-o-pravu-na-pristup-informacijama -27.02.2021.
20. Zakon o provedbi opće uredbe o zaštiti podataka (NN 42/2018)
21. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12) https://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka – 19.12.2020.

11. POPIS GRAFOVA

12. ANKETNI UPITNIK

Zaštita osobnih podataka u javnim i privatnim poduzećima

Ljubazno vas molim da popunite kratki upitnik. Rezultati ankete bit će anonimni i te će se koristiti prilikom izrade diplomskog rada na temu „obveze pravnih i fizičkih osoba u zaštiti osobnih podataka“

Molim vas da na pitanja odgovorite iskreno kako bi vaši odgovori pridonijeli što realnijim rezultatima istraživanja

1. Prema veličini vaše poduzeće svrstava se u :
   - Mikro poduzeća (0-9 zaposlenih)
   - Mala poduzeća (10-50 zaposlenih)
   - Srednja poduzeća (51-250 zaposlenih)
   - Veliko poduzeće (više od 250 zaposlenih)

2. Prema vlasništvu poduzeće se svrstava u:
   - Javno poduzeće
   - Privatno poduzeće

3. Prema pravnom obliku vaše poduzeće je:
   - Komanditno društvo
   - Društvo s ograničenom odgovornošću
   - Dioničko društvo
   - Jednostavno društvo s ograničenom odgovornošću
   - Obrt
   - Drugo

4. Djelatnost koja je primarna u poduzeću
   - Prerađivačka industrija

- Financijska djelatnost i djelatnosti osiguranja
- Prijevoz i skladištenje
- Telekomunikacije
- Obrazovanje
- Građevinarstvo
- Turizam i ugostiteljstvo
- Marketing
- Drugo:

5. Znate li na koji pravni temelj se oslanjate prilikom obrade osobnih podataka?
   - Da
   - Ne
   - Ne znam

6. Da li u svojem poslovanju koristite osobne podatke klijenata/korisnika?
   - Da
   - Djelomično
   - U manjoj mjeri
   - Uopće ne

7. Da li smatrate da ste dobro upoznati s obvezama koje donosi opća uredba o zaštiti osobnih podataka?
   - Da
   - Ne
   - Djelomično

8. Smatrate li da su vaši zaposlenici dovoljno upoznati s obvezama uredbe?
   - Da
   - Ne
   - Djelomično

9. Da li ste proveli edukaciju zaposlenika vezano iz obveze opće uredbe o zaštiti osobnih podataka?
    - Da
    - Ne
    - Djelomično

10. Da li ste prije uvođenja opće uredbe za zaštitu osobnih podataka napravili analizu stanja poduzeća i analizu rizika
    - Da
    - Ne
    - Samo analizu stanja
    - Samo analizu rizika

11. Što od navedene dokumentacije imate definirano unutar poduzeća:
    - Odluku o imenovanju službenika
    - Pravilnik o zaštiti osobnih podataka
    - Politiku privatnosti
    - Obavijesti koje se pružaju ispitanicima o njihovim pravima
    - Pravilnik o ovlaštenju
    - Izjave o povjerljivosti
    - Evidencije aktivnosti obrade
    - Dokumente koji prikazuju načine prikupljanja određenih podataka
    - Ugovor s izvršiteljem obrade

12. Jeste li uspostavili odgovarajuće politike o zaštiti osobnih podataka u svrhu zaštite prava svojih korisnika/klijenata?
    - Da
    - Ne
    - Djelomično

13. Jesu li te politike javno dostupne?
    - Da

- Ne
- Ne znam

14. Da li su vaši korisnici/klijenti upoznati s time koje osobne podatke o njima prikupljate i u koju svrhu
    - Da
    - Ne
    - Djelomično

15. Prikupljate li i bilježite li osobne podatke radnika? (evidencije zaposlenih, isplatne liste i dr.)
    - Da
    - Djelomično
    - U manjoj mjeri
    - Ne

16. Da li pohranjujete podatke o zaposlenima u papirnatom obliku
    - Da
    - Ne
    - Djelomično

17. Da li je pristup podacima u papirnatom obliku ograničen
    - Da
    - Ne
    - Djelomično

18. Imate li definirane procedure za obradu zahtjeva korisnika koji traže pristup osobnim podacima
    - Da
    - Ne
    - U manjoj mjeri

19. Da li je vaše poduzeće uvelo kontrolu pristupa s ciljem da samo ovlašteni zaposlenici imaju pristup osobnim podacima?
    - Da
    - Ne
    - Djelomično

20. Na koji način ste zaštitili svoje računalne sustave
    - Firewall-om
    - Programima za generiranje lozinke
    - Antivirusne programima
    - Enkripcijske programima

21. Da li ste u mogućnosti u potpunosti ukloniti osobne podatke zaposlenika/korisnika ako je to potrebno
    - Da
    - Ne

22. Imate li javno dostupne informacije o tome kako pojedinac može ostvariti pravo na pristup svojim podacima
    - Da
    - Ne
    - Djelomično

23. Da li ste definirali voditelja obrade podataka
    - Da
    - Ne

24. Da li ste odabrali izvršitelja obrade podataka
    - Da
    - Ne

25. Da li imate odabranog službenika za zaštitu podataka (ako ste obavezni)
    - Da
    - Ne

26. Znate li kako postupiti kada klijent/korisnik povuče svoju privolu?
    - Da
    - Ne

27. Imate li propisanu proceduru postupanja u slučaju povrede osobnih podataka?
    - Da
    - Ne

28. Da li ste upoznati s načinima postupanja i sankcijama u slučaju povrede osobnih podataka?
    - Da
    - Ne
    - Djelomično

29. Smatrate li da je usklađenje s općom uredbom o zaštiti podataka važno za uspješno poslovanje vašeg poduzeća
    - Da
    - Ne
    - Djelomično

Sveučilište
Sjever

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, DOLORES MEŽNARIĆ *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica ~~završnog~~/diplomskog (*obrisati nepotrebno*) rada pod naslovom OBVEZE PRAVNIH I FIZIČKIH OSOBA U ZAŠTITI OSOBNIH PODATAKA *(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, DOLORES MEŽNARIĆ *(ime i prezime)* neopozivo izjavljujem da sam suglasan/na s javnom objavom ~~završnog~~/diplomskog (*obrisati nepotrebno*) rada pod naslovom OBVEZE PRAVNIH I FIZIČKIH OSOBA U ZAŠTITI OSOBNIH PODATAKA *(upisati naslov)* čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)

_____
(vlastoručni potpis)