UNIVERZITET U SARAJEVU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

SISTEMATSKI PREGLED LITERATURE O PROPISIMA O PRIVATNOSTI PODATAKA

Sarajevo, januar 2025.godine AMILA HADŽIĆ

U skladu sa članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalistički studij na Univerzitetu u Sarajevu, daje se

IZJAVA O AUTENTIČNOSTI RADA

Ja, Amila Hadžić, studentica drugog (II) ciklusa studija, broj index-a 5829-73812 na programu Menadžment, smjer Menadžment i informacione tehnologije, izjavljujem da sam završni rad na temu:

SISTEMATSKI PREGLED LITERATURE O PROPISIMA O PRIVATNOSTI PODATAKA

pod mentorstvom prof. dr. Amra Kapo izradila samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Rad ne sadrži prethodno objavljene ili neobjavljene materijale drugih autora, osim onih koji su priznati navođenjem literature i drugih izvora informacija uključujući i alate umjetne inteligencije.

Ovom izjavom potvrđujem da sam za potrebe arhiviranja predao/predala elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija (ime, prezime, datum i mjesto rođenja, datum odbrane rada, naslov rada) na web stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu sa članom 34. 45. i 46. Zakona o autorskom i srodnim pravima (Službeni glasnik BiH, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, 13.01.2025. godine Potpis studenta/studentice:

SAŽETAK

Ovaj rad prikazuje sistematski pregled literature popisa o privatnosti podataka, gdje su osnovni ciljevi istražiti izazove sa kojima se organizacije susreću prilikom implementiranja novih propisa, u kojoj mjeri su potrošači zabrinuti za svoje lične podatke i koja su njihova prava, te kako su novi propisi utjecali na poslovne modele kompanija.

Konstantna upotreba tehnologije i globalna povezanost doveli su do velikih promjena u načinu na koji se lični podaci koriste, te je kao rezultat toga nastala potreba za kreiranjem novih zakonskih regulativa s ciljem osiguranja zaštite ličnih podataka i omogućavanja korisnicima veći nadzor nad vlastitim podacima i na samom kraju poticanje organizacija da obezbijede odgovoran pristup prilikom prikupljanja i obrade podataka.

Neki od primjera propisa su Opšta uredba o privatnosti podataka (GDPR) u Evropskoj uniji i Zakon o privatnosti potrošača u Kaliforniji (CCPA) u Sjedinjenim Američkim Državama. Ovi propisi su kreirani kako bi organizacijama pružili smjernice za organizovanje poslovnih procesa u cilju zaštite privatnosti i prava potrošača, te da pomognu u očuvanju povjerenja među potrošačima i organizacijama.

Usklađivanje sa ovim propisima donosi i mnogo izazova za organizacije. One se suočavaju sa problemima prilikom razumijevanja i primjene novih propisa, te sa uvođenjem novih sistema i poslovnih modela koji sa sobom donose i nove neplanske troškove, a sve u cilju ispunjavanja zakonskih uslova.

Također, uloga potrošača je veoma važna pa su samim tim organizacije prisiljene da se prilagode očekivanjima potrošča i zahtijevima tržišta koji se konstantno mijenjaju. Potrošači zahtijevaju veću transparentnost i kontrolu nad njihovim podacima i procesima prikupljanja i obrade podataka, što značajno utiče na poslovne prakse i strategije organizacija.

Sve ove navedene komponente predstavljaju jednu cjelinu koju je potrebno ispoštovati kako bi se omogućila zaštita privatnosti podataka, jer je to ključni faktor za izgradnju povjerenja između potrošača i organizacija. Organizacije koje poštuju propise i koje uspješno upravljaju privatnošću podataka, te reaguje na promjene i zahtijeve potrošača poboljšavaju svoju reputaciju i ostvaruju konkurentsku prednost u današnjem veoma zahtijevnom digitalnom tržištu.

Ključne riječi: privatnost, zaštita, propisi, GDPR, CCPA,izazovi, zakon, potrošači

ABSTRACT

This paper presents a systematic review of the literature on data privacy, with the primary objectives of exploring the challenges organizations face when implementing new regulations, understanding the extent to which consumers are concerned about their personal data and their rights, and assessing how new regulations have impacted business models.

The constant use of technology and global connectivity have led to significant changes in how personal data is utilized, resulting in the need to create new legal regulations aimed at ensuring the protection of personal data, providing users with greater control over their data, and ultimately encouraging organizations to adopt a responsible approach to data collection and processing.

Examples of such regulations include the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These regulations are designed to provide organizations with guidelines for organizing business processes to protect consumer privacy and rights, and to help maintain trust between consumers and organizations.

Compliance with these regulations presents many challenges for organizations. They face difficulties in understanding and implementing new regulations, as well as in introducing new systems and business models that incur unforeseen costs, all in an effort to meet legal requirements.

Furthermore, the role of consumers is extremely important, forcing organizations to adapt to ever-changing consumer expectations and market demands. Consumers are demanding greater transparency and control over their data and the processes of data collection and processing, significantly affecting organizations' business practices and strategies.

All these components represent a cohesive whole that must be respected to ensure data privacy protection, as it is a key factor in building trust between consumers and organizations. Organizations that comply with regulations and effectively manage data privacy while responding to consumer changes and demands enhance their reputation and achieve a competitive advantage in today's highly demanding digital market.

Keywords: privacy, protection, regulations, GDPR, CCPA, challenges, law, consumers

SADRŽAJ

POPIS SLIKA

POPIS TABELA

POPIS SKRAĆENICA

EU- Evropska unija

GDPR- General Data Protection Regulation

CCPA- California Consumer Privacy Act

FADP- Federal Act on Data Protection

LGPD- Brazilian General Data Protection Law

AI- Artificial intelligence

SAD- Sjedinjene Američke Države

SLR- Systematic Literature Review

PIPL- Personal Information Protection Law

1.UVOD

1.1. Objašnjenje teme

Ovaj rad istražuje propise o privatnosti podataka, fokusirajući se na ključne teme kao što su zaštita privatnosti, upravljanje i obrada podataka, povjerenje korisnika, vrste propisa itd. Pored navedenog u radu ću se najviše bazirati na propisima o privatnosti podataka GDPR (General Data Protection Regulation)- Opšta uredba o zaštiti podataka Evropske Unije, zbog toga što se ona odnosi na Evropsku uniju i na sve zemlje koje su van EU, a koriste podatke stanovnika EU. Uredba je nastala 2016. godine, a počinje se primjenjivati od 2018- te godine, pa su samim tim i podaci, analize kao i naučno istraživački radovi relativno novi, što nam omogućava relevantan pregled uticaja ove uredbe na privatnost podataka korisnika i kompanija, kao i njihove stavove o tome.

Prepoznavanje privatnosti kao temeljnog prava u digitalnom dobu je veoma bitno kako za organizacije, tako i za same korisnike. Zloupotreba ličnih podataka podrazumijeva krađu identiteta, rizike od zlostavljanja, povrede privatnosti tj. pristup povjerljivim informacijama od strane neovlaštenih osoba. Privatnost se može definisati kao zahtjev pojedinca, grupe ili organizacije da budu obaviješteni kada, kako i u kojoj mjeri se informacije o njima dijele sa drugima (Sanchez, 2022).

Privatnost i zaštita podataka postali su jedan od najvažnijih problema u digitalnom svijetu. Kako bi regulisali načine na koji se podaci mogu prikupljati, kreirani su mnogi propisi o zaštiti podataka koji zapravo predstavljaju pravila za organizovanje poslovnog okruženja. Cilj ovih propisa jeste da kreiraju prava i dužnosti za korisnike i kompanije, koja se trebaju primjenjivati svaki put kada se vrši obrada ličnih podataka, kao i zaštita naših ličnih podataka od onih kojima su dostupni podaci, te onima koji se bave prikupljanjem i obradom naših podataka (Alves, *et al.*, 2020).

Organizacije sve više sarađuju sa trećim stranama kao što su dobavljači i poslovni partneri kako bi prikupili i analizirali podatke koje će koristiti za poboljšano donošenje odluka i poboljšanje poslovanja. Dijeljenje podataka preovladava u svim organizacijama bez obzira na njihove resurse i tehnologiju, te donosi mnoge prednosti organizacijama, dok sa druge strane predstavlja određene rizike za privatnost pojedinaca koji koriste njihove usluge. Narušena povjerljivost podataka, insajderski napadi, te zloupotreba podataka od strane organizacije ukazuje na opravdanost ove zabrinutosti. Ove aktivnosti dijeljenja informacija i podataka izazivaju brigu o privatnosti, jer mnoge organizacije iskorištavaju podatke u marketinške svrhe kako bi na što lakši način došli do novih klijenata (Ghorashi, *et al.*, 2023).

Mnoge organizacije prikupljaju podatke kako bi analizirali ponašanje, stavove i navike korisnika. Ti podaci utiču na poslovanje preduzeća i određuju smjer daljeg razvoja organizacije. Sa razvojem interneta razmjena podataka i informacija se znatno povećala, pa su samim tim i podaci postali dostupni mnogima (Pantelic, *et al.*, 2022).

Upotreba tehnologije i interneta postala je bitan dio svakodnevnog života ljudi. To uključuje korištenje e-pošte, online kupovine, online pretraživanja, društvenih mreža itd., a sve to rezultiralo je stvaranjem značajne količine ličnih podataka koji se prikupljaju, koriste, dijele, pohranjuju od strane organizacija, vlade i nekih trećih strana. Organizacije koriste prikupljene podatke za razvoj strateških pristupa, uključujući razvoj proizvoda koje nude, analizu iskustva potrošača, te za identifikaciju budućih tržišnih trendova (Lonzetta i Hayajneh, 2021).

Lični podaci pojedinaca su postali veoma važan faktor u modernom društvu i današnjem načinu poslovanja. To je jedna veoma bitna tema, ali u isto vrijeme i dosta problematična, s obzirom na to da je veoma teško napraviti balans između zaštite privatnosti podataka i očuvanja interesa kompanija, koje su spremne učiniti sve kako bi unaprijedili i povećali obim svog poslovanja, a da prilikom toga ne obraćaju baš puno pažnje na svoje klijente i na njihovu privatnost koja može biti ozbiljno ugrožena (Frey & Presidente, 2024).

Propise o privatnosti podataka uvele su vlade kako bi zaštitile privatnost pojedinaca dopuštajući im da ostvaruju određena prava prilikom dijeljenja njihovih informacija. Ovi propisi uveli su veliku promjenu u načinu na koji organizacije dijele podatke. Zahtijevi za dobivanje pristanka prije prikupljanja podataka, kao i organizacijska transparentnost u dijeljenju podataka, potaknuli su organizacije da ponovo procjene svoje prakse prikupljanja podataka i privatnosti. Organizacije moraju naglasiti svrhu u koju će se podaci koristiti, kao i ko će sve imati pristup podacima, te kako će ti podaci biti zaštićeni. Propisi poput GDPR-a imaju određena ključna načela koja je potrebno ispoštovati, a to su: zakonita obrada podataka, ograničenje upotrebe, tačnost, cjelovitost i povjerljivost itd. Nepoštivanje ovih načela može rezultirati značajnim novčanim kaznama i pravnim posljedicama (Ghorashi, *et al.*, 2023).

Veoma je teško istaknuti se u današnjem konkurentskom okruženju, pa je samim tim kvalitet usluge postao ključna strategija za organizacije, a kako bi je ostvarili potrebno je da prikupljaju podatke o klijentima i na taj način kreiraju svoju ponudu. Organizacije koriste različite podatke kako bi spoznale koje su to potrebe kupaca i na koji način mogu pružiti određene pogodnosti svojim kupcima. Podaci o klijentima se čuvaju u bazama podataka koje često znaju biti meta zlonamjernih hakera. Napad na takve baze može dovesti do velikih novčanih gubitaka kompanije i može ugroziti privatnost milionima ljudi, te dovesti do toga da kljenti izgube povjerenje u kompaniju. Kako bi se to spriječilo organizacije su morale dosta da rade kako bi unaprijedile svoje sisteme i zaštitile privatnost podataka svojih klijenata, te kako bi prilagodile svoje poslovanje sa već utvrđenim propisima o privatnosti podataka (Al-Abdullah, *et al.*, 2020).

Dijeljenje podataka je veoma rasprostranjena praksa koja poboljšava organizacijsku učinkovitost i performanse, ali sa sobom donosi i brojne izazove, naročito u vezi sa privatnosti. Politike privatnosti su ključne za organizacije jer osiguravaju usklađenost sa propisima o privatnosti i zaštiti podataka klijenata. Ove politike služe kao pravni dokumenti koji pružaju informacije pojedincima o tome kako se njihovi lični podaci prikupljaju,

obrađuju i dijele. Politike privatnosti igraju ključnu ulogu u zaštiti privatnosti kupaca, ali također mogu predstavljati i izazove zbog toga što su često veoma duge i nerazumljive za obične korisnike, pa ih zbog toga mnogi izbjegavaju i ne posvećuju im dovoljno pažnje (Ghorashi, *et al.*, 2023).

Regulacija privatnosti je pojam koji se odnosi na "pravo na privatnost" pojedinca, grupe ili organizacije. Propisi o privatnosti su važni za države kako bi osigurale da svi njeni ljudi i organizacije rade u sigurnom okruženju bez prijetnji od vanjskih faktora koji bi mogli prouzrokovati krađu, oštećenje, neovlašteni pristup podacima, kao i određene manipulacije. Organizacije moraju uzeti u obzir sve pravne i etičke aspekte prilikom korištenja podataka za obavljanje poslovnih aktivnosti (Albahar i Thanoon, 2022).

U januaru 2012. godine Europska komisija je objavila prijedlog za reviziju postojećeg zakona o zaštiti podataka. Cilj je bio ispraviti i unaprijediti postojeću Direktivu o zaštiti podataka (95/46/EC) uz upotrebu interneta i digitalnih usluga. Nova opšta uredba o zaštiti podataka se prvenstveno odnosi na zemlje članice EU, ali i na sve ostale zemlje koje obrađuju lične podatke građana EU, bez obzira na državu u kojoj se organizacija nalazi. Ukoliko se ne budu pridržavali datog zakona uslijedit će kazne u vrijednosti od 4 % od ukupnog prihoda organizacije. Također trebaju imenovati službenike za zaštitu podataka DPO (Data Protection Officer), koji će u slučaju povrede podataka obavijestiti i vlasnike podataka i određene službe koje su zadužene za to (Labadie i Legner, 2023).

Propisi o privatnosti podataka kao što je GDPR jasno definiše pravila koja organizacije koje prikupljaju podatke moraju ispoštovati. Ovi propisi također omogućavaju državnim institucijama da sankcionišu organizacije koje zanemaruju propise, a u isto vrijeme povećavaju povjerenje pojedinaca, jer oni sada mogu očekivati da će organizacije prikupljati i obrađivati njihove podatke u skladu sa novim propisima (Bauer, *et al.*, 2022).

Labadie i Legner (2023) kao prednost provođenja propisa navode konkurentsku prednost koje kompanije ostvaruju u odnosu na one koji nisu izvršili provođenje, dok nepridržavanje novih propisa može imati značajan negativni uticaj na kompaniju koji može biti direktni (npr. novčane kazne) i indirektni (npr. gubitak ugleda), kao i nemogućnost kompanije da ostvari dobit, što znatno utiče na performance kompanije.

Dijeljenje podataka postala je veoma važna praksa u poslovnom svijetu koja pomaže organizacijama prilikom donošenja i provođenja poslovnih odluka. Razmjena podataka je široko priznata praksa koja značajno utiče na učinkovitost i performanse organizacije, dok sa druge strane može predstavljati i izazove naročito u vezi sa problemima privatnosti (Ghorashi, *et al.*, 2023).

Mnoge kompanije kao izazove sa kojima se susreću prilikom usklađivanja sa ovim propisima navode da je kontekst propisa nejasan, da su opširno napisani i da sve to zahtijeva njihovo dešifriranje. Organizacije moraju uložiti dosta napora kako bi ih razumijeli. Mnogi

propisi nalažu sigurnosne kontrole kao što su enkripcija, anonimnost podataka, upravljanje pristupom i identitetom itd (Lonzetta i Hayajneh, 2021).

U našem okruženju gdje vlada konstantni tehnološki napredak, zaštita osjetljivih podataka postala je sve veći izazov. Povrede podataka predstavljaju ogromnu i konstantno prisutnu prijetnju, izlažući kompanije rizicima i ostavljajući velike posljedice na samo poslovanje. Uticaj povrede podataka sa sobom nosi i mnoge posljedice, poput finansijskih gubitaka, narušenog ugleda kompanije, te pravnih posljedica (Miryala i Gupta, 2022).

Uvođenje GDPR-a sa sobom donosi i brojne izazove za kompanije. Uslovi koji su potrebni kako bi se dobilo odobrenje od vlasnika podataka postali su znatno strožiji, gdje kompanije trebaju tačno definisati politike privatnosti i omogućiti da one budu jasne i konkretne i što kraće. Zbog svega toga potrebno je izdvojiti dosta vremena i resursa kako bi se sve to ispunilo. Ovi propisi također dozvoljavaju korisnicima da povuku svoju dozvolu tj. pristanak ukoliko smatraju da njihovi podaci nisu zaštićeni i da se koriste u pogrešne svrhe (Politou, *et al.*, 2018).

Jantti (2020) navodi neke od izazova koji se javljaju prilikom usklađivanja, poput potrebe za većim ulaganjem u komunikaciju i informisanje od strane GDPR timova koji će bolje upoznati kompanije sa novim propisima i dati im detaljnije upute kako da sve zakone sprovodu u djelo i kako da prilagode svoje poslovanje, zatim potrebno je izvršiti detaljnu anlizu postojećeg stanja unutar kompanije i uložiti sva potrebna sredstva da bi proces prilagođavanja bio što lakši. Također, veoma je važno obezbijediti obuke za svoje zaposlenike na vrijeme kako bi oni mogli obavljati svoj posao, a u isto vrijeme ispoštovati sva pravila koja nalažu ovi propisi.

1.2. Svrha istraživanja

Svrha ovog istraživanja jeste analizirati koji sve međunarodni propisi o privatnosti podataka postoje, koja je njihova uloga i šta organizacije trebaju uraditi kako bi što efikasnije implementirali ove propise i poboljšali svoje poslovanje. Također, veoma je bitno istražiti i načine na koji se podaci prikupljaju i obrađuju, te procjenu učinkovitosti ovih propisa u savremenom digitalnom svijetu. Očekuje se da će pregled i analiza dosadašnjih naučno istraživačkih radova i studija pomoći prilikom identifikacije snaga i slabosti trenutačnih propisa, te da će nas upoznati sa izazovima sa kojima se organizacije susreću prilikom njihovog provođenja. Pored ovoga potrebno je istražiti i probleme sa privatnošću koji se svakodnevno pojavljuju, te istaći potencijalne mjere zaštite privatnosti korisnika.

1.3. Ciljevi istraživanja

Osnovni ciljevi ovog istraživanja su :

- Definisati ključne teme i aspekte privatnosti podataka,

- Identificirati izazove sa kojima se organizacije susreću prilikom sprovođenja propisa o privatnosti podataka,
- Definisati prava građana i mjere zaštite njihovih podataka,
- Analizirati kako se propisi o privatnosti podataka odnose na nove tehnologije i trendove,
- Analizirati uticaj propisa o privatnosti podataka na poslovne modele i propise kompanija.

1.4. Istraživačka pitanja

Na osnovu prikazanog problema i predmeta istraživanja, definisana su sljedeća istraživačka pitanja:

- Koje su ključne teme i aspekti privatnosti podataka ?
- Sa kojim izazovima se organizacije susreću prilikom sprovođenja propisa o privatnosti podataka ?
- Koja su prava građana i mjere zaštite njihovih podataka ?
- Kako se propisi o privatnosti podataka odnose na nove tehnologije i trendove ?
- Da li implementacija propisa o privatnosti podataka utiče na poslovne modele i propise kompanija ?

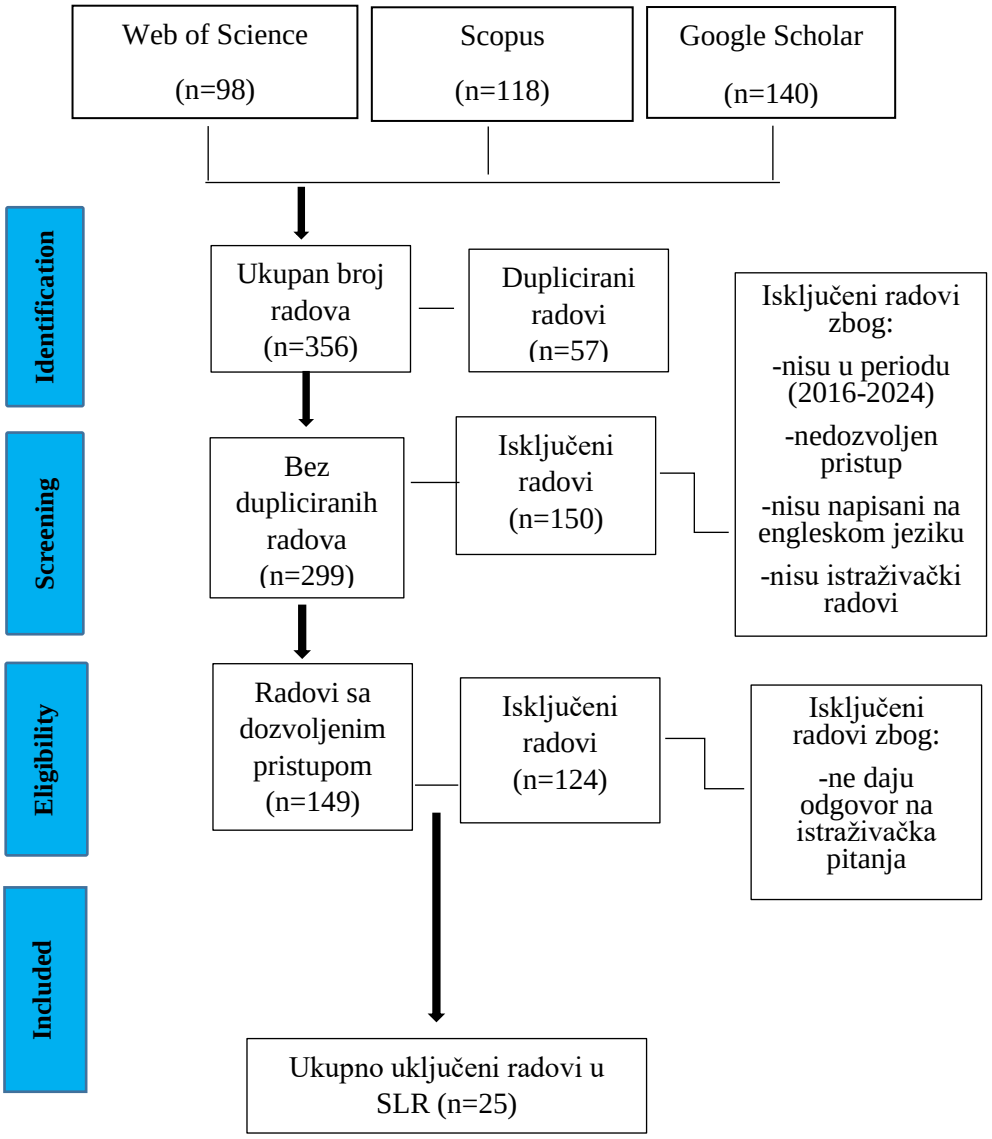
1.5. Metodologija istraživanja

Sistematski pregled literature jeste dobro isplanirani pregled postojeće literature koji će dati odgovore na specifična istraživačka pitanja koristeći različite naučno istraživačke radove za identificiranje, odabir i kritičku procjenu razultata studija uključenih u pregled literature (Rother, 2007).

Sistematski pregled literature kao metodologija podrazumijeva proces prikupljanja, uređivanja i procjene postojeće literature, gdje se prikupljanje odnosi na identifikaciju i pribavljanje literature, uređivanje podrazumijeva organizovanje i analiziranje date literature i na kraju procjena odnosno ocjenjivanje i kreiranje izvještaja o literaturi (Paul, *et al.*, 2021).

Sistematski pregled literature predstavlja način za objedinjavanje naučnih dokaza i istraživanja kao odgovor na određeno istraživačko pitanje na transparentan način, a nastoji uključiti sve objavljene dokaze o datoj temi kao i ocjenu kvaliteta tih dokaza. Glavni cilj jeste smanjiti rizik za pristrasnost te povećati transparentnost u svakoj fazi postupka. Faze koje je potrebno ispoštovati prilikom pisanja sistematskog pregleda literature jesu: definisati istraživačka pitanja, locirati postojeće studije vezane za datu temu, odabrati studije koji ispunjavaju naše kriterije, procjena kvaliteta studija, izdvajanje značajnih podataka, analiziranje i predstavljanje rezultata kao i tumačenje dobivenih rezultata (Lame, 2019).

Slika 1. SLR prizma



Izvor: Kreacija autora

1.6. Struktura rada

Ovaj rad je strukturiran konceptom uvoda u kojem je predstavljeno obrazloženje teme i svrha istraživanja kao i glavni ciljevi istraživanja i istraživačka pitanja na osnovu kojih će biti izvedeni i zaključci rada. Nakon toga je definisana i metodologija istraživanja korištena prilikom izrade rada, te struktura rada. Nakon uvoda slijedi prikaz teorijskog okvira koji će se sastojati od određenih poglavlja i potpoglavlja, a koji će definisati pojam privatnosti i podataka, propise o privatnosti i zaštiti podataka, vrste propisa, pojam GDPR-a (General Data Protection Regulation) itd. Zatim slijedi pregled literature na osnovu dodašnjih

provedenih istraživanja. Kako bi bila osigurana kvalitetna pretraga literature, bit će korištena Web of Science baza podataka, Scopus, Google Scholar itd. Na samom kraju bit će predstavljen zaključak i diskusija zajedno sa pregledom korištene literature i referencama.

2. TEORIJSKI OKVIR

2.1. Pojam podatka, privatnosti i sigurnosti

Tehnološki napredak i nove aplikacije poput senzora, pametnih mobilnih uređaja, društvenih mreža, internet stvari itd., omogućili su prikupljanje, pohranjivanje i obradu velike količine podataka. Ovakav scenarij povećava prijetnje sigurnosti i privatnosti prilikom upravljanja podacima. Oštećenje i zloupotreba podataka ne utječe samo na pojednice ili organizacije, već može imati negativan utjecaj na cijele društvene sektore. Problem sigurnosti i privatnosti podataka nije novi problem, on datira još od 70-tih godina, ali sa konstantnim razvojem i upotrebom tehnologije ovaj problem postaje sve veći (Bertino i Ferrari, 2017).

Zaštita podataka zahtijeva osiguranje tri glavna sigurnosna svojstva a to su povjerljivost podataka, cjelovitost i dostupnost (CIA). Povjerljivost (Confidentiality) se odnosi na zaštitu podataka od neovlaštenog pristupa, integritet (integrity) se bavi zaštitom podataka od neovlaštenih izmjena. Također integritet se odnosi na pouzdanost podataka, te osigurava da podatke mogu mijenjati samo ovlaštene osobe i da se podaci mijenjaju bez grešaka, da budu ažurirani i da potiču iz pouzdanih izvora, te dostupnost (availability) je svojstvo koje osigurava da su podaci dostupni ovlaštenim korisnicima. Ispunjavanje ovih zahtijeva predstavlja izazov, jer su se povećali napadi na podatke zbog sve većih aktivnosti prikupljanja podataka iz različitih izvora (Bertino i Ferrari, 2017).

Za jednu od najčešće korištenih definicija privatnosti podataka zaslužan je Allan Westin koji je privatnost podataka definisao kao "zahtijev pojedinca, grupe ili institucije da sami odluče kada, kako i u kojoj mjeri se informacije o njima prenose drugima". Pojam privatnost podataka i povjerljivost podataka mnogi smatraju istim, međutim postoje određene razlike između ova dva pojma. Istina je da privatnost podataka zahtijeva osiguranje povjerljivosti podataka, jer ako podaci nisu zaštićeni od neovlaštenog pristupa, privatnost ne može biti osigurana. Privatnost također ima i dodatnih problema koji podrazumijevaju poštivanje određenih zahtijeva iz zakonskih propisa kao i individualnih postavki privatnosti (Bertino i Ferrari, 2017).

Privatnost podataka i informacija je privilegija da imate određenu kontrolu nad načinom na koji se lični podaci prikupljaju, obrađuju i koriste. To je zapravo sposobnost pojedinca ili grupe da spriječi da njihovi lični podaci budu dostupni osobama ili kompanijama koje prethodno nisu dobili odobrenje od njih. Sigurnost možemo definisati kao praksu odbrane podataka i informacija korištenjem tehnologija, softvera, te različitih procesa od neovlaštenog pristupa, izmjena, dijeljenja i uništavanja. Sigurnost podataka predstavlja ključnu ulogu prilikom usklađivanja sa propisima i prilikom poslovnog upravljanja, štiteći

podatke od oštećenja, krađe, neovlaštenih izmjena i pristupa. Razlika između privatnosti i sigurnosti je u tome što je privatnost usmjerena na definisanje pravila kako bi se osiguralo da se podaci prikupljaju, dijele i koriste na odgovarajuće načine, dok se sigurnost više koncentriše na zaštitu podataka od zlonamjernih napada i zloupotrebe ukradenih podataka za ostvarivanje određenog profita (Jain, *et al.*, 2016).

S obzirom na to da se podaci pohranjuju u sve većim količinama na globalnom nivou, hakerima je postalo sve lakše da iskorištavaju ranjivost i nedostatke vezane za cyber sigurnost kompanija. Ukoliko kompanije na vrijeme ne preduzmu odgovarajuće mjere zaštite, zlonamjerni hakeri mogu neovlašteno pristupiti njihovim IT sistemima i bazama podataka, dijeliti, mijenjati i brisati podatke pojedinaca, te samim tim omogućiti krađe identiteta i stvoriti velike probleme. Također, sve prethodno navedeno može ugroziti poslovanje kompanija, stvoriti troškove u vidu novčanih kazni od pokrenutih tužbi prema kompanijama, te naštetiti njihovom ugledu (Netwrix, 2023).

Pored toga što pojedinci i organizacije mogu poduzeti mjere kako bi zaštitili lične podatke, mnoge vlade širom svijeta su kreirale propise o zaštiti privatnosti, na osnovu kojih zahtijevaju od kompanija da izvrše usklađenost svojih poslovnih procesa sa ovim propisima ukoliko žele prikupljati i upravljati ličnim podacima ljudi (BuiltIn, 2023).

BuiltIn (2023) navodi ono što korisnici mogu samostalno uraditi kako bi zaštitili svoje podatke:

- Kreirati jake, jedinstvene lozinke – lozinke su prva linija odbrane ličnih podataka,
- Koristiti dvofaktorsku provjeru autentičnosti – omogućiti autentifikaciju u dva koraka za svoje online račune, kao npr. slanje koda za pristup na mobilni telefon,
- Redovno ažurirati softver i aplikacije koje koriste,
- Biti oprezni prilikom dijeljenja podataka- istražiti koliko su sigurne web stranice koje traže njihove podatke,
- Izbjegavati davanje ličnih podataka aplikacijama vještačke inteligencije,
- Detaljno pročitati politike privatnosti i šta one podrazumijevaju,
- Pratiti svoje online račune – ukoliko primijete neke sumnjive promjene, reagovati na vrijeme.

Sigurnost podataka se također odnosi i na mjere zaštite digitalne privatnosti kako bi se spriječio neovlašteni pristup računarima, bazama podataka, web stranicama i sl. Sigurnost podataka podrazumijeva uvođenje sigurnosnih mjera poput enkripcije, autentifikacije, kontrole pristupa, firewall itd., koji će pomoći u zaštiti kako pohranjenih tako i podataka koji se šalju ili primaju (Atlan, 2023).

Privatnost podataka podrazumijeva i usklađenost sa zakonima i propisima poput Opšte uredbe o zaštiti podataka (GDPR) u Evropskoj Uniji i Kalifornijski zakon o privatnosti potrošača (CCPA) u SAD-u. Ovi zakoni propisuju kako organizacije trebaju dobiti odobrenje od pojedinaca prije prikupljanja, upotrebe i obrade njihovih ličnih podataka.

Također govore o tome kako i na koji način organizacije trebaju pohranjivati i osigurati te podatke, te koja sve prava imaju vlasnici podataka (Atlan, 2023).

Generiranje podataka može se podijeliti na aktivno generiranje i pasivno generiranje podataka. Aktivno generiranje podataka podrazumijeva da će vlasnik podataka svoje podatke dati trećim stranama, dok se pasivno generiranje podataka odnosi na podatke prikupljene online aktivnostima korisnika, dok vlasnik podataka nije upućen da treća strana prikuplja te podatke (Jain, *et al.*, 2016).

Rizik kršenja privatnosti podataka usljed generiranja podataka se može minimizirati na sljedeće načine:

- Ograničenje pristupa – ukoliko vlasnik podataka smatra da podaci mogu otkriti osjetljive informacije koje se ne bi smjele dijeliti, ima pravo odbiti dati takve podatake.
- Krivotvorenje podataka – u nekim slučajevima je nemoguće spriječiti pristup osjetljivim podacima, pa zbog toga vlasnici podataka vrše izmjene podataka, tačnije unose nepotpune, netačne ili iskrivljene informacije uz pomoć raznih softvera i alata koji ih omogućavaju skrivanje internetskog identiteta (Jain, *et al.*, 2016).

U prošlosti su organizacije prikupljale što je više moguće podataka, a da pritom nisu vodile računa o privatnosti podataka što je trebalo biti prioritet. Usvajanje GDPR-a je prisililo veliki broj organizacija da razmotre rješenja za osiguranje usklađenosti sa propisima o privatnosti podataka. Ukoliko kompanije nastoje izvršiti usklađenost sa propisima poput GDPR-a, potrebno je da kreiraju nove sisteme koji će omogućiti snažnu zaštitu privatnosti podataka, za razliku od postojećih koji su općenito kreirani za lak pristup podacima. Te propise je još teže ispuniti onda kada se podaci međusobno dijele sa organizacijskim jedinicama ili sa nekim trećim stranama, ali se regulatorni zahtijevi trebaju primjenjivati čak i u tim slučajevima (Wang, *et al.*, 2019).

Wang *et al*. (2019) navode pet načela privatnosti podataka:

1. Transparentnost i revizija – vlasnik podataka treba biti upoznat sa tim ko ima njegove podatke, kako se oni obrađuju i za šta se koriste.
2. Saglasnost – vlasnik podataka treba dati pristanak za prikupljanje i obradu njegovih ličnih podataka.
3. Kontrola obrade – vlasnik podataka treba imati kontrolu nad vrstama obrade za koje se koriste njegovi podaci.
4. Prenosivost podataka – vlasnik podataka bi trebao dobiti kopiju svih podataka koji se na njega odnose, ukoliko to zatraži.
5. Garancija protiv ponovne identifikacije – rezultati obrade ne bi trebali dopustiti ponovnu identifikaciju bilo kojeg pojedinačnog subjekta i podataka.

2.2. Privatnost vs sigurnost

Podaci su veoma važan dio današnjeg digitalnog svijeta, zbog toga je veoma važno zaštititi podatke što je više moguće. Pored zaposlenika, podaci su najvrijednija imovina jedne kompanije. Samim tim ukoliko kompanije ne obezbijedi sigurnosne mjere s ciljem zaštite podataka, njene baze podataka bi mogle biti u opasnosti od provale. Istraživanja pokazuju da oko 60% malih i srednjih preduzeća čiji su podaci hakirani, propadne nakon šest mjeseci. Odgovornost svake kompanije jeste da zaštiti podatke koje su u njenom posjedu, a to podrazumijeva zaštitu podataka i privatnosti svojih kupaca, zaposlenika, poslovnih partnera i svih ostalih kontakata. Zakoni o privatnosti podataka nisu isti u svim zemljama, ali većina zakona zahtijeva zaštitu od neovlaštenih pristupa i otkrivanja ličnih podataka (Blesch, 2024).

Iako je sigurnost podataka najvažnija komponenta privatnosti podataka tj. ne možemo imati privatnost bez sigurnosti, obrnuto nije uvijek tako. Sistem može biti veoma siguran odnosno teško mu je pristupiti bez autorizacije ili ga je teško hakirati, ali ipak ne poštuje propise privatnosti ukoliko prikuplja, obrađuje i dijeli podatke na neprikladan način ili na način kojim se ne poštuju prava vlasnika podataka. Privatnost podataka se odnosi na pravilno upravljanje podacima, pravilnu upotrebu, zadržavanje i brisanje podataka, dok sigurnost podataka čine pravila, sredstva i metode za zaštitu ličnih podataka (Atlan, 2023).

Kod privatnosti podataka ključnu ulogu predstavljaju kontrole. One omogućavaju korisnicima da ustanove ko ima pravo na pristup njihovim podacima i u koju svrhu će se ti podaci koristiti. Dozvole korisnika omogućavaju pojedincima da kontrolišu sve procese koji su povezani sa njihovim ličnim podacima (Dataversity, 2024).

Bez sigurnosti podataka, neovlaštene kompanije ili pojedinci mogu dobiti pristup ličnim podacima a samim tim dovesti i do kršenja privatnosti, što može dovesti do krađe identiteta, finansijskih prevara, oštećenja ugleda pojedinaca i kompanija sa kojima su prethodno dijelili svoje podatke. Nedostatak sigurnosti može negativno uticati na kompanije, stvoriti nepovjerenje među potrošačima, dovesti do gubitka i narušiti ugled kompanije (Atlan, 2023).

Sigurnost i privatnost podataka zahtijevaju stalni nadzor i prakse upravljanja rizicima. Do povrede podataka najčešće dolazi zbog slabih sigurnosnih mjera, a neadekvatne kontrole vezane za privatnost mogu uticati na otkrivanje osjetljivih informacija, čak i u slučajevima kada su kreirane snažne sigurnosne mjere. Osnovni cilj privatnosti podataka jeste da se uspostavi kontrola i potrebni protokoli za zaštitu ličnih i osjetljivih podataka, dok je cilj sigurnosti da se spriječe cyber napadi i povrede podataka (Dataversity, 2024).

2.3. Ključni koraci za prikupljanje podataka

Podaci značajno mijenjaju način na koji kompanije posluju. Podaci mogu pomoći kompanijama prilikom poboljšanja kvaliteta rada, predviđanja trendova, sprječavanje rizika, uštede vremena, donošenja boljih odluka, povećanja profita itd.

Emeritus (2022) navodi da je prije samog početka prikupljanja podataka potrebno:

- Definisati vlastite ciljeve – precizno definisati ciljeve koji će predstavljati glavne smjernice prilikom istraživanja,
- Odabrati prave metode – odlučiti koje metode prikupljanja će nam najviše biti od koristi (ankete, upitnik, intervju, posmatranje itd.),
- Prikupiti podatke – uz upotrebu odgovarajućih metoda izvršiti prikupljanje podataka,
- Provjeriti prikupljene podatke – provjeriti kvalitet prikupljenih podataka kako bi se osigurala pouzdanost istraživanja,
- Analiza prikupljenih podataka – koristiti odgovarajuće statističke programe kako bi se došlo do pouzdanih rezultata,
- Tumačenje dobivenih rezultata – kreiranje zaključaka uz adekvatne dokaze,
- Kreiranje konačnih izvještaja – predstaviti rezultate vlastitih istraživanja publici putem izvještaja, prezentacija.

Baig (2023) ističe da se najčešće prikupljaju sljedeće vrste podataka:

- Podaci o online ponašanju – gdje se prati ponašanje korisnika, koliko su vremena proveli na određenim web stranicama, šta najviše istražuju, na koju stranicu su najviše puta klikuli,
- Iskustva na društvenim mrežama – kako i na koji način korisnici govore o proizvodu, usluzi, brendu na platformama društvenih mreža,
- Online recenzije – anonimne informacije koje korisnici daju o brendu, proizvodu koji su koristili i na taj način utiču na razmišljana novih potencijalnih korisnika,
- Razne vrste B2B podataka – gdje se korisnici mogu informisati o kompaniji, oglasima za posao, poslovanju neke kompanije itd.,
- Popisi kontakata za stvaranje novih potencijalnih klijenata,
- Informacije o cijenama proizvoda sa web stranica.

2.4. Metode zaštite podataka

Svaka organizacija mora provesti plan za sigurnost podataka svojih korisnika, te ga stalno ažurirati u skladu sa potrebama. Taj plan treba da sadrži popis svih kategorija podataka koje organizacija prikuplja, obrađuje i pohranjuje. Za svaku kategoriju podataka sigurnosne politike i procedure trebaju biti jasno definisane. Sigurnost podataka bi trebalo biti jedan od najvažnijih elemenata prilikom kreiranja strateškog plana organizacije, jer neovlašteni pristup i korištenje podataka se može veoma negativno odraziti na samo poslovanje kompanije (Blakeley i Matsuura, 2013).

U dobu u kojem pohranjivanje i dijeljenje podataka raste velikom brzinom, značaj kreiranja snažne strategije kako bi se zaštitili podaci je veoma važna. Zaštita podataka podrazumijeva strateške i proceduralne korake koje je potrebno preduzeti kako bi se omogućila zaštita privatnosti, te dostupnost i integritet osjetljivih podataka (Cloudian, 2024).

Imperva (2024) navodi tri osnovna fokusa za većinu strategija za zaštitu podataka:

- Sigurnost podataka - potreba za zaštitom podataka od slučajnog ili zlonamjernog oštećenja,
- Dostupnost podataka – sposobnost brzog oporavka podataka u slučaju gubitka, oštećenja ili prirodne nepogode,
- Kontrola pristupa – ograničiti pristup podacima samo onima koji imaju ovlaštenje za to, a ne bilo kojim drugim osobama.

Povreda podataka kompanije može dovesti do ozbiljnih posljedica, uključujući finansijski gubitak, pravne posljedice, te lošu reputaciju za kompaniju. Ključnu ulogu u zaštiti podataka kompanije imaju zaposlenici, jer su oni često prva odbrana od cyber prijetnji, samim tim moraju veoma dobro poznavati prakse privatnosti i sigurnosti, te ih upotrijebiti kada za to postoji potreba. Svaka organizacija bi trebala implementirati program privatnosti i sigurnosti podataka koji bi trebao uključivati redovne procjene rizika, politike i postupke, te planove odgovora u slučaju incidenata. Također, potrebno je redovno stvarati sigurnosne kopije podataka, te kreirati strategije za oporavak podataka u slučaju njihovog gubitka ili povrede (Chojnowska, 2023).

TitanFile (2023) navodi metode zaštite podataka:

- Enkripcija – podrazumijeva pretvaranje osjetljivih podataka i informacija u kodirani oblik, te ih na taj način čine nečitljivim svima koji nemaju odgovarajući " ključ za dešifriranje". Samo ovlaštene osobe mogu dekodirati i pročitati podatke. Najznačajnija prednost enkripcije jeste ta što omogućava visoku razinu sigurnosti, čak i slučajevima kada dođe do povrede podataka. Ukoliko se šifrirani podaci ukradu ili im pristupi neovlaštena osoba, oni će biti nečitljivi i samim tim beskorisni. Pored ovoga enkripcija pomaže organizacijama prilikom usklađivanja sa propisima o privatnosti podataka. Enkripcija se mora pravilno implementirati kako bi bila efikasna, jer ukoliko se " ključ za dešifriranje" izgubi ili ukrade, šifrirani podaci bit će nedostupni čak i legitimnom vlasniku,
- Sigurnosno kopiranje i oporavak podataka – Jedan od najvažnijih aspekata zaštite podataka jeste redovno kopiranje podataka koje osigurava očuvanje podataka u slučaju oštećenja ili gubitka. Stvaranjem kopija, organizacije mogu brzo opraviti svoje podatke, te neometano nastaviti sa svojim poslovanjem. Najznačajnija prednost sigurnosnog kopiranja podataka jeste u tome što organizacije mogu veoma brzo da povrate podatke, smanjujući vrijeme prekinutog rada i smanjujući rizik od trajnog gubitka podataka,
- Kontrola pristupa podacima – podrazumijeva ograničavanje pristupa povjerljivim podacima samo ovlaštenim korisnicima. Ograničavanje se postiže kreiranjem i upotrebom lozinki, kao i višefaktorskim provjerama autentičnosti. Najznačajnija prednost kontrole pristupa jeste u tome što pomaže kompanijama da prate i nadziru ko ima pristup podacima, te ko je izvršio određene radnje, čime se nastoji smanjiti

rizik od unutrašnjih prijetnji. Sistemi koji vrše kontrolu pristupa podacima trebaju se često testirati i ažurirati, kako bi se omogućilo ispravno funkcionisanje i zaštita ličnih podataka od neovlaštenih pristupa,

- Sigurnost mreže – čiji je osnovni zadatak zaštita podataka, informacija i imovine sačuvanih na računarskim mrežama od krađa, neovlaštenih pristupa ili eventualnih oštećenja. To se postiže korištenjem vatrozida (firewall) koji odlučuje da li će dopustitit ili blokirati pristup mreži i pohranjenim podacima, na osnovu definisanog skupa sigurnosnih pravila, te enkripcije koja služi za zaštitu ličnih podataka koji se prenose preko mreže. Sigurnost mreže pomaže organizacijama prilikom upravljanja rizikom, te omogućava ispunjavanje regulatornih zahtijeva,
- Fizička sigurnost - podrazumijeva mjere koje se koriste kako bi se osigurali fizički uređaji i objekti koji služe za pohranjivanje ličnih podataka. Potrebno je zaštititi ormare koji se koriste za skladištenje, trezore kroz implementaciju sistema za kontrolu pristupa pomoću biometrijske autentifikacije, posebnih kartica i sl. Pored toga veoma je važno zaštititi računare, mobilne telefone sigurnosnim lozinkama jer su oni veoma osjetljivi na krađu.

Kako bi na što bolji način izvršili zaštitu podataka, od organizacije se zahtijeva da upotrijebi tri vrste resusa:

- Ljudski resursi – koji imaju značajnu ulogu u zaštiti podataka kao npr. službenik za zaštitu podataka, kontakt osoba za prava u vezi sa podacima,
- Tehnološki resursi- koji uključuju fizičku IT imovinu poput hardvera, softvera, baze podataka koji omogućavaju sisteme za obradu podataka,
- Nematerijalni resursi- koji predstavljaju znanje i iskustvo u vezi sa zaštitom podataka kao npr. okviri, standardi, modeli procesa (Wang, *et al.*, 2019).

2.5. Izazovi prilikom poslovanja i zaštite podataka

Kompanije se susreću sa mnogim izazovima prilikom obavljanja poslovnih procesa, samim tim što moraju velike napore uložiti kako bi na što bolji način zaštitili privatnost svojih korisnika i omogućili im da se osjećaju sigurno. TechTarget (2024) navode neke od izazova:

- Povjerenje potrošača – veoma je važno steći povjerenje svojih potrošača kako bi kompanije neometno mogle nastaviti sa svojim poslovanjem. Prilikom prikupljanja podataka o svojim klijentima, kompanije moraju biti transparentne te tražiti dozvolu za obavljanje bilo kakve radnje u koju su uključeni podaci njihovih klijenata. Kompanije mogu preduzeti sljedeće korake kako bi izgradili povjerenje među svojim potrošačima:
  - Provjeriti da li su ugovori o pristanku davanja saglasnosti za korištenje podataka napisani jasno i konkretno kako bi bili razumljivi prosječnom korisniku,

    - Angažovati marketinške i prodajne timove i stručnjake kako bi se naglasile poruke o zaštiti,
    - Ponuditi mogućnost korisnicima da povuku svoje odobrenje za korištenje i obradu podataka,
    - Omogućiti korisnicima potpuni pregled njihovih podataka koji su dostupni kompaniji itd.
- Poštivanje zakona i propisa – preduzeća moraju konstantno pratiti izmjene koje se dešavaju u zakonima i propisima o zaštiti podataka, te prilagoditi svoje poslovanje,
- Upravljanje podacima - je veoma složeni proces koji zahtijeva stalna ulaganja u nove sisteme koji će omogućiti konstantno ažuriranje i izmjene vezne za očuvanje privatnosti podataka,
- Tehnološke promjene – konstantne promjene tehnologije koje se dešavaju sa sobom donose i brojne izazove. Sa napretkom tehnologije, zaštita podataka postaje sve složenija.
- Operacije sa podacima – prikupljanje ličnih podataka je u stalnom porastu kojem se ne nazire kraj. Podaci se stalno prikupljaju, dijele i obrađuju, pa su samim tim često i meta cyber napada. Kako bi lakše upravljali podacima, kompanije se trebaju bazirati samo na prikupljanje i zadržavanje neophodnih podataka koji su ključni za vođenje poslovanja.
- Upotreba vještačke inteligencije - vještačka inteligencija predvodi trenutnu digitalnu revoluciju. Hakeri sve više koriste vještačku inteligenciju kako bi pokrenuli napade na određene kompanije i njihove baze podataka.

2.5.1. Zašto je zaštita podataka važna ?

Zaštita ličnih podatka korisnika je etička odgovornost svake organizacije. Kompanije se moraju pridržavati zakona i propisa o privatnosti podataka, ugovornim obavezama kako bi ispunili očekivanja svojih klijenta, a također kako ne bi bili sankcionisani. S obzirom na sve veću dostupnost i količinu digitalnih podataka, korisnici trebaju što više pažnje posvetiti kontroli nad podacima i informacijama koje dijele sa organizacijama. Određene prakse upravljanja podacima su ključne kako bi se osiguralo da su lične i povjerljive informacije sigurno pohranjenje i da njima mogu pristupiti samo ovlaštene osobe. Uvođenjem snažnih sigurnosnih mjera i šifriranja može se značajno smanjiti rizik od potencijalnih cyber prijetnji kao i neovlaštenog pristupa ličnim podacima. Usklađenost poslovanja sa zakonima o zaštiti podataka poput GDPR-a ili CCPA su veoma važni kako bi se izbjegle visoke kazne, te kako bi se održalo povjerenje klijenata u kompaniju i njeno poslovanje (DataGuard, 2024).

NextDLP (2024) navode razloge zbog kojih je zaštita podataka važna:

- Slučajno brisanje podataka- slučajnom ljudskom greškom se često dešava da veoma bitni podaci budu izbrisani, pa zbog toga kompanije moraju na vrijeme obezbijediti

sigurnosne kopije podataka kako bi ih što prije vratili i kako ne bi ugrozili poslovanje i poslovne procese.

- Zlonamjerno brisanje podataka – podaci se mogu namjerno izbrisati ili oštetiti kako bi se nanijela šteta kompaniji. Zlonamjerni hakeri mogu pristupiti bazi podataka i ugroziti određene vrijedne resurse ili nasumično brisati podatke.
- Ransomware napadi – su zapravo zlonamjerni softveri koji traže novac od žrtve kako ne bi objavili, obrisali, podijelili ili zabranili pristup privatnim podacima.
- Prirodne katastrofe – koje mogu ugroziti cjelokupno poslovanje organizacije, ukoliko one nemaju unaprijed pripremljen plan oporavka podataka koji bi omogućili neometano obavljanje poslovnih aktivnosti.
- Neovlašteni pristup i korištenje privatnih podataka- unutrašnji ili vanjski akteri mogu neovlašteno pristupiti bazama podataka i iskoristiti ih za vlastitu korist, što može ugroziti poslovanje i sve subjekte čiji su podaci zloupotrebljeni .

2.6. Vrste propisa o privatnosti podataka

2.6.1. General Data Protection Regulation (GDPR)

Sa napretkom tehnologije i interneta, Evropska unija je prepoznala potrebu za kreiranjem nečega što će poboljšati poslovanje kompanija, a na prvom mjestu zaštititi prava ljudi koji dijele svoje lične podatke sa njima i omogućiti im da se osjećaju sigurno i da iza sebe imaju zakone koji će štiti njihove interese u slučaju nekih neovlaštenih pristupa i radnji u vezi sa njihovim podacima (GDPR, 2020).

GDPR je najstrožiji zakon o zaštiti privatnosti i sigurnosti na svijetu. Bez obzira na to što je ovaj zakon kreirala i usvojila Evropska unija, on se odnosi i na sve organizacije van EU koje prikupljaju i ciljaju podatke građana EU. Ovaj propis nameće stroge kazne za one koji krše standarde privatnosti i sigurnosti, a vrijednost kazni iznosi i do nekoliko desetina miliona eura ili 4% globalnog prihoda (u zavisnosti koji od tih iznosa je veći), a pored toga vlasnici čiji su podaci iskorišteni imaju pravo tražiti naknadu štete (Wolford, 2020).

Ovim zakonom Evropska unija želi istaći svoj čvrsti stav vezan za privatnosti i sigurnost podataka u vremenu kada sve više ljudi dijeli svoje podatke sa kompanijama i web stranicama, a njihove zloupotrebe i povrede su postale svakodnevna pojava (GDPR, 2020).

Opšta uredba Evropske unije o zaštiti podataka (GDPR) se počinje primjenjivati od 25. maja 2018. godine, te zamjenjuje Zakon o zaštiti podataka direktiva 95/46/EC koji je do tada bio na snazi. GDPR potiče kompanije da više pažnje posvećuju podacima i da imaju plan prikupljanja, korištenja i uništavanja podataka (Hoofnagle, *et al.*, 2019).

Nakon uvođenja GDPR-a mnoge kompanije su izmijenile i prilagodile svoje prakse u vezi sa podacima i po prvi put primijenile profesionalan pristup prilikom rukovanja ličnim podacima. Također, GDPR zahtijeva zaštitu i praćenje podataka, te kompanije koje koriste i

dijele lične podatke sa drugima, moraju provjeriti one koji pružaju usluge i nametnuti im određena ograničenja prilikom upotrebe podataka. Ovaj propis će značajno pomoći kompanijama da budu više zaštićene od čestih cyber napada, da osiguraju vlastiti brend, da poboljšaju svoje odnose sa klijentima, te da poboljšaju svoj položaj na tržištu s obzirom na veliku konkurenciju (Hoofnagle, *et al.*, 2019).

Bez obzira na veličinu ili opis posla kojim se kompanija bavi, sve dok vrši transakcije vezano za lične podatke klijenata iz Evropske unije, to se smatra kao obrada podataka građana EU. To podrazumijeva aktivnosti poput pristupa podacima o adresama za naplatu ili dostavu kupaca unutar EU, podaci vezani za online bankarstvo, obavljene online transakcije putem e-trgovine itd. Kompanije su često u zabludi jer nisu sigurne da li se neki podaci i informacije smatraju ličnim podacima, pa je zbog toga potrebno uložiti napore kako bi se to ustanovilo (Trendmicro, 2024).

Za kompanije se može reći da nisu izvršile usklađivanje sa GDPR-om onda kada se ne pridržavaju ili zanemaruju zakone koji su definisani propisima o privatnosti podataka. Tu neusklađenost mogu ustanoviti nadzorna tijela, vlastitom inicijativnom ili nakon pritužbe od strane klijenta kompanije. Nadzorno tijelo koje formira svaka država unutar EU za sebe, treba obratiti pažnju na pristiglu pritužbu, te istražiti da li je ona istinita. Pored toga nadzorno tijelo ima i ovlaštenja da izrekne novčanu kaznu za svaku kompaniju koja nije poslovala u skladu sa propisima (Trendmicro, 2024).

Nakon što istraži procese prikupljanja i obrade podataka unutar jedne kompanije, te utvrdi da postoji prekršaj, nadzorno tijelo analizira sljedeće kriterije kako bi utvrdili iznos kazne:

- Broj osoba čiji su podaci korišteni, nivo štete koja im je nanijeta, te svrhu za koju su podaci iskorišteni,
- Da li je kršenje propisa urađeno namjerno ili zbog nemarnosti zaposlenika kompanije,
- Šta je kompanija uradila kako bi ublažila propust i nanesenu štetu,
- Vrstu podataka koji su ugroženi,
- Da li je kompanija provela neke preventivne mjere prije samog događaja,
- Poslovanje kompanije u prošlosti,
- Da li su izricane slične kazne i da li su se ovi postupci ponavljali više puta,
- Da li je kompanija imala bilo kakvu korist, direktnu ili indirektnu od povrede privatnosti svojih klijenata (Trendmicro, 2024).

Ukoliko nadzorno tijelo utvrdi da je kršenje propisa beznačajno, u tom slučaju kompanijama se mogu izreći upozorenja, te zatražiti od njih da svoje poslovne modele prilagode propisima o privatnosti podataka. S druge strane ako se utvrdi da je kompanija više puta prekšila propise na isti način, kako bi ostvarila neku korist, nadzorna tijela će propisati najtežu kaznu (Trendmicro, 2024).

Smatrajući zaštitu ličnih podataka osnovnim pravom svake osobe, GDPR nalaže da će lični podaci biti:

- Obrađeni zakonito, pošteno i transparentno
- Prikupljeni za tačno određene svrhe,
- Tačni i precizni,
- Čuvani ne duže nego što je neophodno,
- Obrađeni sa integritetom i povjerljivošću (Zaeem i Barber , 2020).

Primarna svrha GDPR-a je definisanje zakona o zaštiti podataka za sve zemlje članice širom Evropske unije. Namjera GDPR-a jeste:

- Povećanje privatnosti i prava na podatke za stanovnike EU,
- Pomoć stanovnicima EU da razumiju upotrebu ličnih podataka,
- Rješavanje problema izvoza ličnih podataka izvan EU,
- Regulatornim tijelima dati veće ovlasti za poduzimanje mjera protiv organizacija koje krše novu uredbu o zaštiti podataka,
- Zahtijevanje da svaki novi poslovni proces koji koristi lične podatke mora ispoštovati stroga pravila koja nalaže novi propis o zaštiti podataka (Buckley, *et al.*, 2021).

GDPR (2020) navode slučajeve u kojima je dozvoljena zakonita obrada ličnih podataka. Podaci se ne smiju prikupljati, pohranjivati ili dijeliti sa drugima osim u slučajevima:

- Kada je ispitanik dao jasan i nedvosmislen pristanak za prikupljanje i obradu podataka,
- Ukoliko je obrada podataka neophodna za pripremu i sklapanje ugovora (kako bi se provjerila istinitost podataka),
- Ispunjavanja zakonske obaveze (npr. primljen nalog od suda),
- Potrebe za obradom podataka kako bi se spasio nečiji život,
- Kada je obrada neophodna za obavljanje radnji od javnog interesa ili za obavljanje određene službene dužnosti.

GDPR (2020) navodi da ovaj propis daje dozvolu vlasnicima podataka da imaju lakši pristup podacima koje kompanije imaju o njima. Pored ovoga vlasnici podataka imaju sljedeća prava:

- Pravo na informisanost,
- Pravo na pristup podacima u svakom trenutku,
- Pravo na ispravak i brisanje,
- Pravo na ograničenje obrade podataka ukoliko nije precizno definisana svrha obrade ili ukoliko primjeti da se podaci koriste u svrhu koja nije prethodno definisana,
- Pravo na prenos podataka,
- Pravo na prigovor.

GDPR je kreiran kako bi preoblikovao način na koji javni i privatni subjekti, uključujući univerzitete i istraživačke institucije pristupaju zaštiti podataka. Unutar GDPR obrada podataka definisana je kao svaka radnja ili skup operacija koje se izvodi nad ličnim podacima ili na skupovima podataka poput prikupljanja, pohrane, izmjene, pronalaženja, upotrebe, prijenosa, brisanja ili uništavanja (Crutzen, *et al.*, 2019).

2.6.2. California Consumer Privacy Act (CCPA)

Kalifornijski zakon o privatnosti potrošača je državni zakon Kalifornije, nastao je 2020. godine i omogućava potrošačima veću kontrolu nad ličnim podacima koje organizacije prikupljaju o njima. CCPA daje potrošačima određena prava poput:

- Pravo na informisanost o načinu na koji organizacije prikupljaju njihove podatke, te kako se oni koriste i dijele,
- Pravo zahtijevanja brisanja ličnih podataka,
- Pravo na odbijanje prodaje ili dijeljenja ličnih podataka,
- Pravo na nediskriminaciju prilikom ostvarivanja CCPA prava (California Attorney General's Office , 2024).

CCPA se odnosi na organizacije koje se definišu kao profitni subjekti i koji:

- Prikupljaju lične podatke potrošača (u svoje ime ili u ime trećih strana) te određuju način i svrhu obrade
- Posluje u Kaliforniji te ispunjava jedan od sljedećih uslova:
  - Godišnji bruto prihod iznosi više od 25 miliona dolara
  - Godišnje preuzima, dijeli ili prodaje lične podatke za više od 50.000 potrošača
  - Ostvaruje 50 % ili više godišnjeg prihoda od prodaje ličnih podataka (Thomson Reuters, 2024).

Usklađivanje poslovanja sa CCPA ne predstavlja samo jedan korak, već kompletan proces koji je sastavljen od više radnji. Primarna radnja podrazumijeva promjenu načina razmišljanja kompanija prema potrošaču i shvatanje važnosti zaštite njihovih ličnih podataka. Također, od kompanija se zahtijeva da budu transparentne prilikom praksi prikupljanja i korištenja podataka, da na adekvatan način odgovore na zahtijeve svojih potrošača i da provedu sve potrebne sigurnosne mjere kako bi obezbijedili privatnost i zaštitu njihovih podataka. Veoma je važno pratiti sve promjene koje nalaže CCPA kako bi bili u korak sa tehnologijom i revizijama ovog propisa. Povrede podataka ne uključuju samo jednu stranu, to su najčešće masovni događaji koji uključuju veći broj potrošača (IBM, 2023).

Zajedničko kod GDPR-a i CCPA jeste:

- Zaštita privatnosti i ličnih podataka svojih građana,

- Pravo koje se daje potrošačima da budu informisani u koje svrhe će se koristiti njihovi podaci, te pravo na brisanje i izmjenu podataka,
- Pravo potrošača da pristupe svojim ličnim podacima,
- Obavještenje potrošača ukoliko se desi da privatnost njihovih podataka bude ugrožena.
- Mogućnost davanja kazni kompanijama koje počine određene prekršaje, poput neovlaštenog pristupa, korištenja i dijeljenja podataka (IBM, 2023).

Ovaj zakon omogućava izvršne i regulatorne ovlasti državnom tužilaštvu Kalifornije. Prije samog pokretanja postupka protiv organizacija koje krše propise CCPA, potrebno je prvenstveno obavijestiti organizaciju, pružatelja usluga o prekršaju te im dati rok od 30 dana da to isprave. Ukoliko kompanija ne ispravi svoju grešku tužilaštvo može tražiti ispatu građanskih kazni u iznosu od 2500 dolara po prekršaju ili 7500 dolara po namjernom prekršaju. Ove građanske kazne se odnosne na svakog pojedinca čiji su podaci nepropisno iskorišteni, pa samim tim ove kazne mogu rezultirati velikim ukupnim novčanim kaznama (Thomson Reuters, 2024).

2.6.3. Federal Act on Data Protection (FADP) – Savezni zakon o zaštiti podataka

Spichtinger (2024) navodi da je ovaj zakon je 1. septembra 2023. godine dobio svoju prvu reviziju od njegovog donošenja 1992. godine i sa sobom donosi nekoliko ključnih promjena u švicarskom zakonu o zaštiti podataka a to su:

- Interakcija sa GDPR-om – sa ciljem osiguranja slobodnog protoka podataka sa EU, jer se švicarske kompanije moraju uskladiti sa GDPR-om ukoliko obrađuju lične podatke pojedinaca koji se nalaze u EU, ukoliko nude robu ili usluge osobama iz EU,
- Poboljšana prava pojedinaca- revizija ovog zakona doprinijela je jačanju prava pojedinaca u smislu njihovih ličnih podataka, dajući im određena prava
- Strožiji zahtjevi usklađivanja – organizacije su dužne da izvrše usklađivanje sa novim zakonom, sličnim onima kao što je GDPR, kako bi neometano vršile prenos podataka između Švicarske i EU, te kako bi ostale konkurentne na tržištu.

Ovaj propis se na samom početku odnosio i na fizičke i na pravne osobe. Međutim njegovom revizijom odlučeno je da se odnosi samo na prava vezana za fizičke osobe i vladine institucije. Svaki građanin ima pravo da od kompanije traži informaciju o tome da li se njegovi podaci obrađuju ili su bili obrađivani nekada u prošlosti, te mogu zatražiti pristup tim podacima. Podaci moraju biti dostavljeni u pisanoj formi i moraju se dostaviti besplatno. Građani također imaju pravo da zahtijevaju ispravljanje njihovih podataka ukoliko su netačni ili ukoliko je došlo do nekih promjena. Istraga u vezi sa poštivanjem FADP u organizaciji može se pokrenuti samostalno ili nakon prijave. Ukoliko se istragom utvrdi da je došlo do nepoštivanja zakona, tada se organizacijama mogu izreći mjere koje podarzumijevaju prilagodbu ili u potpunosti obustavljanje obrade podataka, pa čak i njihovo brisanje.

Nepoštovanje FADP-a i onoga što on nalaže može rezultirati kaznama za organizacije u iznosu do 250.000 CHF. Razlika između GDPR-a i FADP-a jeste u tome što prema FADP-u svaka osoba pojedinačno može biti kažnjena, dok kod GDPR-a se fokus stavlja na kažnjavanje pravnih lica (Usercentrics, 2023).

2.6.4. Brazilian General Data Protection Law (LGPD)

Usercentrics (2024) navodi da je brazilski opšti zakon o zaštiti podataka je stupio na snagu 16.08.2020. godine i predstavlja najbolje kreiran zakon u toj regiji. Na kreiranje ovog zakona utjecala je Opšta uredba Evropske unije o zaštiti podataka (GDPR).

Ovaj zakon se primjenjuje na sve aktivnosti obrade podataka koje su:

- provedene u Brazilu,
- provedene u svrhu pružanja usluga ili obrade podatka pojedinaca koji se nalaze u Brazilu,
- prikupljene u Brazilu (Usercentrics, 2024).

Usercentrics (2024) ističe da se LGPD ne primjenjuje ukoliko obrada ličnih podataka:

- se vrši od strane fizičke osobe koja podatke koristi u privatne svrhe,
- se koristi isključivo u akademske, umjetničke ili novinarske svrhe,
- se vrši u svrhu javne sigurnosti,
- potiče izvan Brazila i ne dijele se podaci sa brazilskim agentima za obradu podataka (pod uslovom da zemlja koja koristi podatke pruža razuman stepen zaštite podataka).

Kako bi kompanije izvršile usklađenost sa LGPD-om, trebaju provesti nekoliko koraka kao što su provođenje revizije procesa privatnosti i zaštite podataka koji organizacija trenutno provodi, te ispitati ključna područja poput upravljanja pristankom, korištene mjere sigurnosti podataka, te korištene kontrole pristupa u cilju određivanja rizika i potencijalnih prilika za poboljšanje poslovnih modela i procesa. Nakon toga potrebno je imenovati službenika za zaštitu podataka koji će nadgledati strategije koje se koriste prilikom zaštite podataka, te pratiti da li je i u kojoj mjeri izvršena usklađenost sa LGPD-om. Omogućiti da ugovori sa trećim stranama budu ažurirani, kako bi sadržavali klauzule koje zahtijeva ovaj propis. Na samom kraju potrebno je implementirati snažne mehanizme za pristanak, omogućiti da zahtijevi za dobijanje pristanka budu jednostavni, jasni i precizni (Usercentrics, 2024).

Prenošenje podataka i odgovornosti prema ovom propisu je slično kao kod GDPR-a. Podaci stanovnika Brazila se mogu prenositi u inostranstvo, s tim da se brazilski zakon o zaštiti podataka primjenjuje i odnosi na bilo koju drugu državu koja vrši obradu podataka (Usercentrics, 2024).

(Usercentrics, 2024) navodi da obradu podataka treba prekinuti:

- kada je završen proces obrade podataka za svhu za koju su se podaci prikupljali odnosno kada oni više nisu potrebni za njeno postizanje,
- kada vlasnik podataka obavijesti organizaciju da povlači dozvolu za korištenje nihovih podataka,
- ukoliko se utvrdi da je došlo do kršenja propisa.

Ukoliko dođe do kršenja propisa koje LGPD nalaže uslijedit će kazne koje mogu iznositi do 2 % godišnjeg bruto prihoda organizacije ili 50 miliona brazilskih reala (10 miliona američkih dolara), u zavisnosti koji iznos je veći (Consentmo, 2024).

2.6.5. Personal Information Protection Law (PIPL) – Kineski zakon o zaštiti podataka

PIPL je stupio na snagu 1. novembra 2021. godine, a organizacije su imale nekoliko mjeseci da mu se prilagode i da usklade svoje poslovanje. Kao i prethodni zakoni i ovaj zakon se ne odnosi samo na kineske kompanije koje obrađuju podatke građana Kine, već na sve kompanije širom svijeta koje koriste podatke njihovih građana (ChinaBriefing, 2021).

ChinaBriefing (2021) navodi da bi svaka kompanija trebala unaprijediti svoje poslovne sisteme kako bi se prilagodili ovim propisima, te formirati službe koje će nadzirati sve procese u vezi sa time. Neki od zadataka ovih službi su:

- provođenje edukacija o zaštiti ličnih podataka,
- prihvatanje i obrade pristiglih prijava od strane vlasnika podataka,
- vršenje revizije postojećih sistema i objavljivanje rezultata,
- provođenje istraga u vezi sa nezakonitim obradama podataka,
- drugi poslovi definisani zakonima i propisima o zaštiti podataka.

Ukoliko se obrade podataka vrše u suprotnosti od odredbi ovog zakona ili se prilikom obrade podataka ne vodi računa o zaštiti ličnih podataka, službe koje obavljaju poslove zaštite podataka naredit će onima koji vrše obradu da urade ispravak, upozoriti ih na grešku ili obustaviti pružanje usluga. Ukoliko se ispravak odbije, izreći će se kazna u iznosu od 10.000 RMB (oko 1.300 eura) do 1 milion RMB (oko 130.000 eura) , te kazna u iznosu od 100.000 RMB (oko 13.000 eura) za osobu koja je direktno odgovorna za neadekvatnu obradu podataka (ChinaBriefing, 2021).

3. SISTEMATSKI PREGLED LITERATURE

Sistematski pregled literature podrazumijeva pretraživanje, identifikaciju i analizu postojećih istraživanja na određenu temu. Osnovni cilj sistematskog pregleda literature jeste da identifikuje, analizira i sumira dostupne podatke i istraživanja, te da se na osnovu toga

prikažu rezultati dobiveni ovim istraživanjem. Kroz sistematski pregled literature nastojimo bolje razumjeti postojeća saznanja i na kraju donijeti zaključke provedenog istraživanja.

Na samom početku izrade rada sam definisala ciljeve istraživanja i istraživačka pitanja na osnovu kojih sam vršila pretragu postojećih istraživačkih radova. S ciljem pronalaska adekvatnih radova, prilikom pretrage literature korištene su Web of Science baza podataka, Scopus, Google Scholar itd. Sljedeći korak jeste definisanje kriterija na osnovu kojih će se vršiti uključivanje ili isključivanje radova u proces detaljnijeg pregleda i analize.

Nakon pregleda baze podataka i pristupa istraživačkim radovima, identificirani su odgovarajući radovi na osnovu prethodno utvrđenih kriterija poput dozvoljenog pristupa, godine objavljivanja, jezika na kojem su napisani, sadržaja radova i mogućnosti davanja odgovora na definisana istraživačka pitanja. Kroz SLR prizmu u uvodu, tačnije u podnaslovu metodologija istraživanja je prikazan broj dostupnih radova, dupliciranih radova, radova sa dozvoljenim pristupom, te broj radova isključenih iz analize.

Nakon što je završen proces identifikacije, uslijedila je detaljna analiza izdvojenih radova, podataka i informacija kako bi se dobili odgovori na istraživačka pitanja. Neki od radova nisu zadovoljili pethodno definisane kriterije pa su samim tim prilikom detaljnije analize eliminisani iz procesa proučavanja i uzimanja u razmatranje rezultata njihovih istraživanja. Nakon čitanja i analiziranja radova predstavljena su zapažanja raznih autora, te njihovo viđenje i prezentacija rezultata do kojih su došli.

U posljednjoj fazi su predstavljeni finalni rezultati ovog istraživanja kao i prikaz tabele sa definisanim istraživačkim pitanjima, brojem korištenih radova za svako pitanje, imenovani autori, te dati odgovori na pitanja dobiveni sistematskim pregledom literature. Na samom kraju predstavljena je diskusija sa donesenim zaključcima na osnovu spovedenih svih prethodno definisanih faza.

Kao odgovor na prvo istraživačko pitanje autori u svojim radovima navode sljedeće: Dijeljenje ličnih podataka sa pružateljima usluga predstavlja neizbježan rizik koji se javlja usljed: nepravilnog rukovanja podacima, nedostatka svijesti korisnika prilikom dijeljenja podataka, nepotrebnog dijeljenja podataka na nepoznatim stranicama itd. Dok se podaci dijele posvuda svake minute, problemi pri zaštiti i sigurnosti podataka postaju sve veći. Neprikladno ponašanje, pogrešno ili prekomjerno dijeljenje podataka kao i zlonamjerno korištenje podataka od strane kompanija koje nude usluge putem interneta, često dovode do povrede podataka. Korisnici moraju biti upoznati kada i u koju svrhu se koriste njihovi podaci. Skladište ličnih podataka (Personal Data Storage- PDS) je usluga koja omogućava pojedincu da upravlja svojim podacima na vrlo siguran način. Korisnici ne samo da imaju pravo na kontrolu nad svojim podacima, već imaju vlasništvo nad podacima, samim tim oni mogu odlučiti koja kompanija ili pojedinac može pristupiti pohranjenim podacima i koji podaci eventulno mogu, a koji ne mogu biti iskorišteni za određene radnje. Dijeljenje ličnih podataka na web stranicama ili društvenim mrežama, jedna je od radnji koje veoma često dovode do gubitka kontrole nad ličnim podacima (Alessi, *et al*., 2019).

Alessi *et al.* (2019) navode da korisnici imaju sljedeća prava u vezi sa svojim ličnim podacima:

- Pravo na zaborav- tj. pravo na brisanje ličnih podataka gdje god su oni pohranjeni,
- Pravo na ispravak – korisnik ima pravo da traži ispravak netačnih ličnih podataka,
- Pravo na odustajanje – korisnik ima pravo povući svoj pristanak u bilo kojem trenutku.

Privatnost podataka je podjednako važna kako za organizacije tako i za same korisnike. Osnovna prava slobode mogu biti znatno narušena ukoliko dođe do zloupotrebe ličnih podataka. U skladu sa zakonima GDPR-a kompanije koje se ne pridržavaju pravila vezanih za privatnost su u opasnosti od kazni poput novčanih kazni i tužbi. Vlasti mogu zabraniti kompanijama buduće obrade ličnih podataka, a kazne mogu mogu doseći i do 20 miliona eura. Samim tim podizanje globalne svijesti o važnosti zaštite ličnih podataka pojedinaca je veoma važna za poslovne subjekte. GDPR se smatra najsloženijim zakonom o privatnosti podataka koji je uspostavljan u modernom dobu i on je zapravo proširenje prijašnjih politika zaštite podataka sa ciljem osiguranja zaštite temeljnih prava i slobode. Ovi propisi sa sobom donose nove brojne izazove za kompanije, ali i razne mogućnosti na globalnom nivou. Usklađenost kompanija sa GDPR-om je veoma važna kako bi se osiguralo sudjelovanje na jedinstvenom tržištu. Većina kompanija još uvijek nastoji uskladiti svoje poslovanje sa novim propisom, navodeći izazove poput nedostatka praktičnih vodiča, složenost GDPR, povećani troškovi savjetovanja, nedostatak informativne kampanje (Aseri, 2020).

Nove obaveze koje nastaju uvođenjem GDPR sa sobom donose značajne promjene u zaštiti i implementaciji privatnosti organizacija. Sve kompanije koje obrađuju lične podatke stanovnika EU ili prate ponašanje ispitanka unutar EU će bez obzira na to gdje se nalaze morati primjenjivati pravila GDPR. To znači da će se kompanije izvan EU tj. međunarodne kompanije morati pridržavati i svojih nacionalnih zakona i GDPR-a. Iako nove tehnologije i usluge donose korist kako preduzećima tako i potrošačima, one također donose i ozbiljne rizike privatnosti. Ovo može dovesti do smanjenja povjerenja ljudi prema preduzećima, a samim tim dovesti i do usporenog razvoja inovacija i novih tehnologija. Također, mnoge poslovne prilike mogu biti propuštene ukoliko se ne provedu odgovarajuće prakse zaštite podatka. Jedan od osnovnih ciljeva GDPR-a jeste odgovoriti na trenutne izazove povezane sa zaštitom ličnih podataka, te jačanje prava privatnosti na internetu. Kompanije koje prikupljaju, obrađuju i koriste lične podatke trebaju se unutar zadanog vremenskog roka pripremiti i prilagoditi promjenama koje GDPR donosi. Veliki izazov vezan za implementaciju GDPR-a jeste nedostatak svijesti i razumijevanja kompanija o nadolazećim promjenama i zahtjevima koje GDPR nameće kroz svoje propise. Ovi zahtjevi znatno utiču na na organizacijske procese i prakse, implementiranje tehnoloških sistema, osposobljavanje osoblja, te dodjeljivanje novih odgovornosti unutar organizacije. Navedeni zahtijevi ističu potrebu za revizijom postojećih praksi privatnosti i tehnoloških mjera zaštite podataka, kao i planiranje kako bi se osigurala usklađenost sa GDPR-om. GDPR zahtijeva od kompanija da ograniče obradu ličnih podataka što je manje moguće, samim tim kompanije moraju

odlučiti koja vrsta podataka im je potrebna kako bi neometano izvršavali svoje poslovne procese. Pored toga moraju navesti svrhu korištenja ličnih podataka, jer prikupljanje eventualnog viška podataka nije dozvoljeno. Neke kompanije imaju probleme sa razumijevanjem zahtijeva nove uredbe i sa onim šta tačno trebaju implementirati i izmijeniti u svom poslovanju. Što se prije kompanije prilagode novim zahtijevima, ne samo da će ispuniti zakonsku obavezu usklađivanja, već može osigurati i konkurentsku prednost na tržištu za svoju kompaniju (Tikkinen-Piri, *et al*., 2018).

Privatnost se može definisati kao sposobnost pojedinca ili grupe da zaštite svoj privatni život i svoje okruženje uključujući i podatke o sebi. Pojam privatnosti često se povezuje sa povjerljivošću ličnih podataka i njihovom zaštitom (pristup, korištenje, širenje, prijenos itd.). Novi propis EU (GDPR) promijenio je viziju privatnosti primjenjujući je i u digitalnom dobu, te uveo pravo na zaborav i brisanje ličnih podataka. Propis o privatnosti podataka uspostavljaju skup pravila koje se organizacije trebaju pridržavati u slučaju prikupljanja, korištenja i širenja informacija o pojedincima. Informacijska sigurnost se može definisati kao sposobnost zaštite informacionih sistema sa različitim vrstama podataka koji se pohranjuju, obrađuju ili prenose pomoću računarskih sistema i mreže. Ona mora zaštititi podatke od unutrašnjih i vanjskih radnji koje bi mogle dovesti do ometanja funkcionisanja sistema kao što je neautorizovani i neovlašteni pristup. Ova zaštita se omogućava korištenjem posebnih sredstava i alata (softvera i hardvera) uz poštivanje sigurnosnih politika. Informacijska sigurnost i zaštita podataka su područja koja se često suočavaju sa izazovima usljed konstantnog napretka tehnologija digitalnog doba i inovacija. Jasno je da loša informacijska sigurnost može ugroziti sistem, te stvoriti dodatne štete i troškove (Romansky i Noninska, 2020).

Romansky i Noninska (2020) navode dvije vrste komponenti informacijske sigurnosti a to su:

- Organizacijske - u koje ubrajamo fizičku sigurnost za zaštitu fizičkih izvora podataka i sistema kao što su hardver, softver, mreže itd. Oni podrazumijevaju određene postupke koji obezbjeđuju kontrolu pristupa, ograničenje kopiranja podataka na druge uređaje, te preventivno djelovanje u slučaju da se dese neke prirodne nepogode poput požara, poplava, te u slučaju terorističkih napada. Pored fizičke sigurnosti veoma je važna i sigurnost procesa naročito za poslovne procese, koja mora osigurati kontinuitet poslovanja u svim situacijama kao što su nezgode, prirodne katastrofe ili pogreške nastale djelovanjem ljudskog faktora.
- IT komponente – prije svega potrebno je obezbijediti sigurnost aplikacije (zaštita od prijetnji, krađa, izmjene ili brisanja aplikacija), zatim mobilna sigunost gdje je potrebno obezbijediti sredstava i alate za zaštitu različitih prijenosnih uređaja. Veoma je važno obezbijediti sigurnost interneta i mreže kroz zaštitu softverskih aplikacija, web stranica, te virtuelne privatne mreže kako bi se spriječio pokušaj prijenosa podataka od strane zlonamjernih softvera.

Dijeljenje podataka postala je veoma važna praksa u poslovnom svijetu koja pomaže organizacijama prilikom donošenja i provođenja poslovnih odluka. Međutim, ove aktivnosti dijeljenja podataka sa sobom donose i brigu o privatnosti, jer mnoge organizacije iskorištavaju lične podatke u marketinške svrhe kroz isporuku ciljanih oglasa i drugih sadržaja. Dijeljenje podatka sa organizacijama kao i sa trećim stranama značajno povećava rizik od povrede privatnosti. Ovaj problem se nastojao riješiti uvođenjem propisa o privatnosti podataka. Kako bi ispoštovale zakone koji novi procesi sa sobom donose, organizacije su dužne otkriti kako prikupljaju, obrađuju i dijele lične podatke, ali ovi propisi ne daju izričita tehnička uputstva za sigurnu implementaciju njihovih praksi. Sam pojam zaštite koji se koristi u ovim propisima često je preširok i dvosmislen, ne dajući organizacijama jasne smjernice za učinkovitu zaštitu ličnih podataka. Razmjena podataka je široko priznata praksa koja značajno utiče na učinkovitost i performanse organizacije, dok sa druge strane može predstavljati i izazove naročito u vezi sa problemima privatnosti (Ghorashi, *et al.*, 2023).

Politike privatnosti su ključne za organizacije jer osiguravaju usklađenost sa propisima o privatnosti podataka kao i zaštiti privatnosti kupaca. One zapravo služe kao pravni dokument koji daje informacije pojedincima o tome kako se njihovi lični podaci prikupljaju, obrađuju i dijele. Organizacije prikupljene podatke koriste kako bi bolje razumjeli svoje potrošače, te kako bi mogli odrediti koja su njihova iskustva o proizvodima i uslugama koje oni nude. Čak i pored ovih propisa, otkrivanje privatnosti se još uvijek može dogoditi iako su poduzeti pravni postupci za usklađivanje sa propisima o privatnosti. Neki od razloga zbog kojih se ovo može desiti su nenamjerne nezgode uzrokovane ljudskom greškom, nedostatak razumijevanja ili zloupotreba ličnih podataka. Ove situacije se obično dešavaju prilikom uključivanja trećih strana koje imaju različite politike ili im nedostaje transparentnost prilikom rukovanja sa ličnim podacima. Otkrivanje privatnosti predstavlja veliki problem za organizacije u finansijskom smislu i u smislu narušene reputacije. Kako bi se prilagodile propisima organizacije moraju redizajnirati svoje poslovne procese koje koriste prilikom rukovanja sa ličnim podacima. Jedan od primjera zloupotrebe podataka objavljen je 2018-te godine kada je konsultantska kompanija Cambridge Analytica izvršila prikupljanje ličnih podataka miliona korisnika Facebook-a bez njihovog znanja i odobrenja. Otkriveno je da su vršili obrade prikupljenih podataka u svrhu ciljanja korisnika za marketinške kampanje za izbore u SAD-u. Ovaj skandal je značajno uticao na tehnološku industiju, pa su samim tim mnoge organizacije revidirale svoja pravila i prakse privatnosti, naglašavajući pristanak korisnika više nego ikada prije. Također ovaj slučaj je pokazao i značajnu nepovezanost između očekivanja korisnika i praksi organizacija, ističući potrebu da organizacije postupaju sa korisničkim podacima sa većom pažnjom i poštenjem. Facebook je suočen sa velikom kaznom od 5 milijardi dolara od strane Savezne komisije za trgovinu i povredu privatnosti, a također ovaj incident je prisilio vlade da poboljšaju zakone o zaštiti podataka širom svijeta. Propisi o privatnosti su pravne obaveze kojih se svaka organizacija mora pridržavati, te tražiti odobrenje za pristup podacima. Procesi prikupljanja i obrade moraju biti transparentni i pouzdani, te obezbijediti sigurnost i privatnost korisnika (Ghorashi, *et al.*, 2023).

U toku inovacija u informacijskim i komunikacijskim tehnologijama, organizacije su počele prikupljati sve veću količinu podataka o ljudima i njihovom ponašanju. S obzirom na to da ovakvi događaji značajno zadiru u privatnost pojedinaca, pitanja o tome kako osobe koje se bave prikupljanjem, upravljaju i koriste podatke, postaju ključna. Pojedinci koji svjesno dijele svoje podatke, ispunjavanjem ličnih i finansijskih podataka prilikom kupovine, trebaju imati povjerenje u organizacije, da su njihovi podaci sigurni i da se ne koriste na njihovu štetu. Povjerenje u način prikupljanja podataka nije samo potencijalna odrednica prilikom ponašanja pojedinaca u dijeljenu podataka, već je i pokazatelj u kojoj mjeri se pojedinci osjećaju sigurno u vezi sa praksama prikupljanja podataka koje provode organizacije. Regulatorni okviri koje vlade kreiraju daju pravila i smjernice za one koji primaju, ali i za one koji trebaju dati podatke. Propisi poput GDPR-a mogu uticati na ponašanje ljudi i na njihova očekivanja. U svom radu autori nastoje istražiti da li promjena propisa utječe na pojedince tj. na njihovo povjerenje u one koje prikupljaju podatke. Prije samog istraživanja vjerovali su da će povjerenje pojedinaca u sakupljače podataka porasti zbog novih propisa, ali nakon provedenog istraživanja nisu se baš uvjerili u to. Istraživanja su pokazala da ljudi imaju probleme sa čitanjem i razumijevanja pravila o privatnosti kao i sa politikama o pristanku (Bauer, *et al.*, 2022).

Kao odgovor na drugo istraživačko pitanje autori Kabanov (2016) navode da prilikom usklađivanja GDPR-a sa uslovima poslovanja, kompanije trebaju uzeti u obzir razne izazove sa kojima se mogu susresti, a koji su veoma česti poput :

- Složenost- kompanije trebaju osigurati usklađenost na svim razinama poslovanja u odnosu na zemlju, vrste i količine podataka, te različitih prebivališta organizacija koje se bave obradom podataka,
- Prilagodljivost i dosljednost – je neophodan faktor s obzirom na to da se zakoni stalno mijenjaju , te da se smanjuje vremenski rok za njihovu implementaciju,
- Kapacitet i dostupnost stručnjaka – nedostatak eksperata u oblasti sigurnosti kao i nedostatak IT stručnjaka u području zaštite.

Prilikom implementacije propisa o privatnosti podataka projektni tim organizacije nastoji osigurati sigurnost i usklađenost propisa sa poslovanjem kompanije kroz određene sisteme i aplikacije pomoću kojih klijentima, kupcima i zaposlenicima garantuju zaštitu ličnih podataka i podataka organizacije (Kabanov, 2016).

Digitalizacija ubrzano prodire u gotovo svaku industriju, te stvara nove izazove za organizacije u smislu izgradnje povjerenja među klijentima i osiguravanju odgovarajuće zaštite njihovih ličnih podataka kroz poštivanje zakonskih propisa. Sve u današnjem poslovanju od samog pregovaranja posla, dopisivanja sa klijentima, razmjene kontakta informacija za dostavu pošiljki obično uključuje prikupljanje, prenos, korištenje ili pohranjivanje ličnih podataka. Vlade širom svijeta su kreirale različite zakone o zaštiti podataka i povećanju obaveza organizacija koje prikupljaju i koriste lične podatke. Dva

glavna izazova sa kojima se kompanije susreću su ti da se zakoni o zaštiti privatnosti konstantno razvijaju i mijenjaju, te brzi tempo rasta i promjena tehnologije koje je potrebno stalno pratiti, te prilagođavati poslovanje i poslovne procese, kako bi opstali na tržištu i kako bi ostvarivali konkurentsku prednost (Kabanov, 2016).

Nakon što je GDPR stupio na snagu, istraživači su počeli sprovoditi istraživanja o stavovima pojedinaca i organizacija o uvođenju ovog zakona. Labadie i Legner (2023) navode da su se prilikom sprovođenja istraživanja njihove istraživačke aktivnosti odvijale u višegodišnjem periodu, što im je omogućilo blisku saradnju između akademika i stručnjaka iz multinacionalnih kompanija, te detaljan uvid u EU GDPR inicijativu. Jedan od ciljeva ovog istraživanja jeste razviti određena znanja i teorije koje će pomoći organizacijama prilikom lakšeg usklađivanja GDPR-a. Provodeći ovo istraživanje došli su do zaključka da postoje dva glavna izazova u vezi sa usklađivanjem GRPR-a. Kao prvi izazov navode da su prilikom razmatranja usklađivanja sa GDPR-om uočene značajne promjene dosadašnjeg način skladištenja i obrade ličnih podataka na nivou preduzeća, shvatili su da je ono što im zapravo nedostaje jeste razumijevanje nove uredbe i onoga što ona sa sobom donosi. Kao drugi izazov navode nedostatak zajedičkog jezika sa pravnim odjelima. U njihovim organizacijama rasprave o zaštiti podataka i propisima o privatnosti podataka, često su prekidane zbog nedostatka zajedničkih pristupa, mišljenja, što spriječava stvaranje izvedivih i usklađenih rješenja, te onemogućava napredak. Sve to je dovelo do sprovođenja istraživanja o sposobnosti uvođenja GDPR-a koji će znatno pomoći prilikom upravljanja podacima, profesionalnom razumijevanju i provedbi propisa, te saradnji sa kolegama iz pravnih odjela.

Sirur *et al.* (2018) navode da se njihov istraživački pristup oslanja na literaturu i temelji se na detaljnim intervjuima sa nekoliko organizacija. Iako je GDPR bez sumnje znatno koristan za građane i organizacije, stvarnost pokazuje da kompanije imaju ozbiljne poteškoće u razumijevanju šta znači usklađenost u ovom novom okruženju i kako to sve implementirati. Ovo istraživanje nastoji ispitati probleme sa kojima se suočavaju organizacije kada nastoje izvršiti usklađivanje i implementaciju GDPR-a. Prvi cilj jeste razumjeti iskustva organizacija prilikom sprovođenja propisa, istražiti kako je moguće provesti propise u tehničkom smislu, razumijevanje percepcije kompanija o propisima i lakoći razumijevanja, mjerenje svijesti organizacija o GDPR-u i kako je to uticalo na njihov proces usklađivanja, te očekivanja organizacija o samoj provedbi GDPR-a. Drugi cilj jeste proučavanje procesa koje koristi organizacija prilikom implementacije GDPR-a, koji mehanizmi i tehnike su korištene prilikom implementacije, kakvu su potporu tražili od vlade, te kako su provjeravali njihovu usklađenost.

Opšta uredba o zaštiti podataka Europske unije objavljena je u službenim novinama EU 4.maja 2016. godine, a počet će se primjenjivat od 25.maja 2018. godine, te ističe da će sve kompanije koje imaju preko 250 zaposlenih koji se bave obradom podataka građana EU, morati poštovati pravila GDPR-a. Prema istraživanju iz 2016. godine većina ispitanika čak 84 % je istaklo da smatraju da će Opšta uredba o zaštiti podataka uticati na njihove

kompanije. GDPR se odnosi na cijeli privatni sektor EU koji se bavi obradom ličnih podataka, kao i na organizacije van EU čije su ciljno tržište stanovnici EU odnosno njihovi lični podaci. U slučaju da se kompanije ne pridržavaju ove uredbe, slijede novčane kazne u iznosu većem od 20 miliona eura (Kabanov, 2016).

Sirur *et al.* (2018) su za svoje istraživanje izabrali intervju kao prikladan metod za rješavanje istraživačkih pitanja. Definisan je skup pitanja za intervju koji su pokrivali sva područja interesa, a pri tome i bila dovoljno fleksibilna da na njih mogu dati odgovor ispitanici iz različitih oblasti. Intervjui su bili polustruktuirani kako bi se omogućilo da postavljanje pitanja bude prirodno i kako bi se dobili iskreni odgovori od ispitanika, te kako bi im se omogućilo da slobodno govore. To je ispitivaču dalo priliku da procjeni nivo interesa i stučnosti koju je svaki ispitanik imao za razne teme, te su nastojali da pitanja budu što neutralnija. Intervjui su vođeni lično, putem telefona ili putem internet glasovnog chata. Ovo istraživanje se odnosilo za ispitanike iz različitih sredina koji rade u različitim oblastima. Svi osim jednog ispitanika imali su iskustvo sa implementacijom GDPR-a. Oni koji su imali direktni doticaj sa GDRP-om smatraju da je usklađenost, iako naporan, veoma vrijedan poduhvat. Najveći tehnički problem za većinu ispitanika bio je u dešifriranju očekivanja GDPR-a. Ispitanici iz većih organizacija izrazili su osjećaj zadovoljstva sa procesom u cjelini, tvrdeći da je trud dao rezultate u smislu boljeg razumijevanja zaštite podataka unutar njihove kompanije. Za mala i srednja preduzeća potrebno je uložiti veliki trud, kako bi razumjeli šta se tačno očekuje od njihovih organizacija. Također svi ispitanici su se složili da je GDPR korak više ka razmišljanju kako poboljšati sigurnost i očuvati privatnost podataka. Sve ovo bila je prilika za preispitivanje o sposobnosti organizacije da upravlja cyber rizicima i prijetnjama, pri čemu procjene vezane za zaštitu podataka imaju ključnu ulogu u tom procesu. Dok su veće i sigurnije kompanije pohvalile novu uredbu u smislu objašnjenja složenosti zaštite podataka, mala i srednja preduzeća ističu da je usklađivanje propisa na samom početku bilo veliki stres.

Ispitanici koji su bolje razumijevali prava i polike za zaštitu podataka bili su podjeljeni ističući da je idealistički gledano GDPR definitivno poboljšanje, ali da je daleko od standarda potrebnog da se uistinu osigura praksa za sigurnost podataka. Sve organizacije koje su bile uključene u ovo istraživanje su bile svjesne GDPR-a i poduzeli su potrebne korake za početak procesa usklađivanja. Čini se da su sigurnosno osvještene organizacije bile svjesne GDPR-a relativno dugo, druge organizacije i pojedinci nisu prepoznali sprovođenje GDPR-a kao prioritet. Kompanije su imale nekoliko godina da se pripreme za uvođenje GDPR-a, ali to vrijeme pripreme je moglo biti izgubljeno ako previše kompanija ili nije bilo svjesno GDPR-a ili su tek počeli sa usklađivanjem pred sami kraj dozvoljenog roka. Neka mala i srednja preduzeća koja su bila svjesna GDPR-a, unatoč zabrinutosti oko tog pitanja nisu mogli učiniti značajne korake prema usklađivanju zbog nedostatka resursa i nedostatka smjernica. Mnogi ispitanici su izjavili da je njihova organizacija obezbijedila većini zaposlenika obavezne seminare i obuku koji su isticali važnost podizanja svijesti o zaštiti podataka (Sirur, *et al.*, 2018).

Jantti (2020) navodi da je digitalna transformacija sa sobom donijela i nove vrste sigurnosnih izazova za informacione tehnologije i IT odjele. Uloga privatnosti podataka postala je ključni dio sigurnosti informacijskog sistema i IT upravljanje usugama kada je Europska unija pokrenula GDPR. Glavni zadatak ove studije jeste pokazati da li su i koliko male i srednje kompanije pripremljene za zaštitu privatnosti podataka u skladu sa propisima GDPR-a, te sa kojim su se sve izazovima susretali u pripremnim fazama kao i u fazi implementacije. Iako je ova uredba na snazi od 2018-te godine, još uvijek postoje male kompanije koje nisu dovoljno svjesne zahtijeva privatnosti i koje nisu provele potrebne mjere zaštite privatnosti podataka. Podaci su prikupljeni putem intervjua kao i promatranjem projektnih aktivnosti kompanija tokom regionalnog razvojnog projekta pokrenutog od strane Digital Innovation Hub zaposlenika. Kako bi dobili odgovore na pitanja, intervjuirali su dvadeset osoba iz različitih organizacija. Rezultati ovog istraživanja daju odgovore na tri istraživačka pitanja a to su: 1. Kako su se mala i srednja preduzeća pripremila za privatnost podataka i GDPR?, 2. Koje vrste izazova su povezane sa osiguravanjem privatnosti podataka?, 3. Kako mala i srednja preduzeća upravljaju promjenama vezanim za implementaciju GDPR-a?. Za prvo pitanje jedan od ispitanika je istakao da su oni procijenili informacijsku sigurnost svoje kompanije, te da su proučavali načine prikupljanja i pohranjivanja podataka, a zatim i sudjelovali na edukacijama vezanim za GDPR i njegovu implementaciju. Sljedeći ispitanik je istakao da su oni opisali na koji način se podaci obrađuju u njihovoj organizaciji, te su proveli konkretne mjere za usklađivanje sa GDPR-om kao što su ugovori o obradi podataka i utvrdili da li se dobavljači pridržavaju pravila GDPR-a, a zatim su analizirali svoje registre sa podacima i njihov nivo informacijske sigurnosti. Naredni ispitanik je rekao da su napravili istraživanje šta zapravo GDPR za njih znači, organizirali su interne treninge i analizirali GDPR, te šta se sve smije a šta ne. Što se tiče njihovog drugog istraživačkog pitanja autori navode izazove koje su utvrdili nakon sprovedenih intervjua a to su:

- GDPR timovi bi trebali više ulagati u komunikaciju i informisanje korisnika (dati više smjernica kompanijama radi lakše i jednostavnije implementacije),
- Izvršiti pažljivu pripremu i uložiti više sredstava za pripremu, posebno u malim i srednjim preduzećima,
- Kako potaknuti korisnike da se više brinu o sigurnosti i zaštiti vlastitih podataka,
- Nedostatak obuke i edukacija vezano za GDPR.

Većina ispitanika za treće istraživačko pitanje navode da imaju vlastiti IT odjel koji je zadužen za održavanje i unapređenje informacijskih sistema, kao i za praćenje načina na koji se vrši zaštita podataka, te usklađivanje pravila GDPR-a sa njihovim poslovanjem. Cilj ove analize jeste dati pregled GDPR-a iz perspektive preduzeća. Na osnovu njihovih opažanja ističu da mnoge male i srednje kompanije još uvijek poduzimaju svoje prve korake vezane za GDPR, iako je on stupio na snagu 2018. godine. Kao zaključak i odgovor na istraživačka pitanja autori navode da su došli do spoznaje da su se mala i srednja preduzeća za privatnost podataka i uvođenje GDPR propisa pripremili na razne načine kao što su kreiranje registara podataka, outsourcing, održavanje registara podataka, sudjelovanje u GDPR obukama, analiziranje GDPR-a iz poslovne perspektive. Što se tiče drugog istraživačkog pitanja, kao

ključne izazove povezane sa privatnosti podataka također navode neophodnu isporuku dovoljnih informacija vezanih za privatnost podataka i komunikaciju sa poslovnim korisnicima, upotreba raznih resursa za pripremu GDPR-a, veliki broj informacijskih sistema koje je potrebno provjeriti i uskladiti sa pravilima GDPR-a. Za treće istraživačko pitanje navode da su organizacije morale upotrijebiti vlastite resurse za pripremu za GDPR. Kako bi smanjili rizike privatnosti podataka, izmjenili su neke tradicionalne načine rada, te kreirali plan privatnosti podataka (Jantti, 2020).

Opšta uredba o zaštiti podataka (GDPR) i Kalifornijski zakon o privatnosti potrošača (CCPA) predstavljaju veoma važne propise zaštite privatnosti podataka. Ovi propisi zahtijevaju od kompanija konstantno ulaganje i unaprjeđenje poslovnih procesa. U svom radu autori nastoje definisati izazove sa kojima se susreću kompanije prilikom usklađivanja sa ovim propisima. Ubrzani napredak i razvoj tehnologija omogućio je povećanje prikupljanja, prijenosa i pohrane podataka. GDPR zahtijeva sigurnost obrade podataka i omogućava kontroloru da provodi odgovarajuće tehničke i organizacijske mjere u cilju pružanja sigurnosti u mnogim rizičnim situacijama. Ovi propisi se odnose na sve kompanije, ali nisu sve kompanije podjednako spremne da se nose sa troškovima i izazovima koje ovi propisi donose. Ulaganje u cyber security štiti od gubitaka, ali također se postavlja pitanje kakvu korist kompanije imaju od GDPR-a osim usklađivanja sa zakonom i eventualno izbjegavanje novčanih kazni. Također, mnoge kompanije ističu da GDPR ima više definicija ličnih podataka koje mogu stvoriti izazove za kompanije prilikom utvrđivanja koje informacije treba zaštititi i kako to učiniti. GDPR i CCPA se ne primjenjuju samo na osnovne lične podatke poput imena i prezimena već i na podatke poput IP adrese, lične evidencije, biometrijski podaci, internet pregledavanja itd. Prema izvještaju međunarodne organizacije za privatnost, prosječni troškovi evropskih kompanija za usklađivanje sa GDPR-om iznosi 2,7 miliona eura. Mnoge kompanije naročito male i srednje odlučile su da ne izvrše usklađivanje sa GDPR-om zbog velikih troškova i složenosti samog procesa u nadi da neće biti cilj vlade u smislu sankcionisanja i davanja kazni. U nedavnoj anketi devet od deset vlasnika malih preduzeća u EU su se izjasnili da ne znaju za GDPR niti za kazne koje bi mogle uslijediti u slučaju nepoštivanja istog (Layton i Elaluf-Calderwood, 2019).

Lonzetta i Hayajneh (2021) navode da organizacije koriste prikupljene lične podatke za strateški razvoj, razvoj proizvoda, ciljanje i iskustvo potrošača, te identifikaciju budućih tržišnih trendova. Pored toga pojedinci postaju sve svjesniji o prikupljanju i korištenju njihovih podataka od strane kompanija. Nedavna američka istraživanja su pokazala da postoji znatno veći broj pojedinaca koji su zabrinuti za sigurnost svojih podataka i način na koji se njihovi podaci koriste, u odnosu na one koji nisu previše zabrinuti. GDPR i CCPA su najnoviji propisi o zaštiti privatnosti podataka. Osnovna načela GDPR-a koja je potrebno ispoštovati su:

- Zakonitost, poštenje i transparentnost – svi podaci moraju biti obrađeni zakonito, pošteno i transparentno

- Ograničenje namjene – podaci se mogu prikupljati isključivo u svrhu namjene koja je prethodno definisana,
- Minimizacija podataka – prikupljanje podataka ograničeno je na podatke koji su neophodni za potrebe obrade,
- Tačnost – podaci moraju biti tačni i ažurirani,
- Ograničenje pohrane podataka – podaci se ne smiju čuvati duži period odnosno nakon što se izvrši neophodna obrada,
- Integritet i povjerljivost (sigurnost) – osigurati da su podaci zaštićeni od strane neovlaštenih i nezakonitih obrada, gubitaka i oštećenja,
- Odgovornost - kontrolori su zaduženi da osiguraju uskađenost sa GDPR-om i za osiguranje svih odgovarajućih mjera.

Kalifornijski zakon o privatnosti potrošača donesen je 2018. godine, a stupio je na snagu 2020- te godine. Ovaj zakon se odnosi na organizacije koje posluju u Kaliforniji i obrađuju podatke stanovnika Kalifornije (Lonzetta i Hayajneh, 2021).

Neke od stavki koje su navedene u zakonu su:

- Pojedinci imaju pravo znati kada se njihovi podaci prikupljaju i koriste,
- Pojedinci imaju pravo da znaju da li se njihovi podaci prosljeđuju drugima,
- Pojedinci imaju pravo pristupa svojim podacima, kao i mogućnost da zatraže kopije istih,
- Pojedinci imaju pravo zatražiti da se obrišu njihovi podaci,
- Pojedinci imaju pravo znati za šta se koriste njihovi lični podaci,
- Organizacije trebaju izričitu saglasnost za prikupljanje i upotrebu podataka o maloljetnicima,
- Pojedinci imaju pravo tužiti organizacije koje se ne pridržavaju CCPA (Lonzetta i Hayajneh, 2021).

Mnoge kompanije kao izazove sa kojima se susreću prilikom usklađivanja sa ovim propisima navode da je kontekst propisa nejasan, da su opširno napisani i da sve to zahtijeva njihovo dešifriranje. Organizacije moraju uložiti dosta napora kako bi ih razumijeli. Nakon toga, organizacije trebaju utvrditi da li se ovi propisi i u kojoj mjeri odnose na njih, za koja područja vrijede i šta sve trebaju učiniti kako bi ih se pridržavali. To stvara veliko opterećenje za kompanije, naročito za male i srednje kompanije sa malim odjelima i ograničenim resursima. Mnogi propisi nalažu sigurnosne kontrole kao što su enkripcija, anonimnost podataka, upravljanje pristupom i identitetom itd. Propisi ne definišu precizno koje to sve kontrole je potrebno ispoštovati, što stvara značajne probleme kompanijama prilikom tumačenja. Pored toga ove zaštitne mjere mogu oduzeti mnogo vremena dok se implementiraju, te mogu biti posebno izazovne za organizacije koje imaju ograničene resurse. Također ističu da bi kompanije trebale uvesti procese automatizacije podataka kako bi omogućile učinkovit i djelotvoran proces prikupljanja, obrade i korištenja podataka, a sve to bi im moglo olakšati izazove koji se javljaju prilikom zaštite podataka te usklađivanja sa

propisima. Smatraju da bi automatizacija mogla olakšati tehničku usklađenost sa GDPR-om. U slučaju kada vlasnici podataka zatraže od kompanije da obrišu njihove podatke, kompanije moraju ručno pretražiti, identificirati i ukloniti podatke, dok bi proces automatizacije značajno pomogao i ubrzao proces (Lonzetta i Hayajneh, 2021).

GDPR predstavlja novi izazov i potencijalnu priliku za tehnološke kompanije, podatkovne centre i trgovce koji moraju usvojiti strožije sigurnosne mjere, standarde i procese za zaštitu, obradu i upravljanje ličnim podacim kako bi se osigurala njihova usklađenost sa GDPR-om. GDPR definiše lične podatke kao sve što se može iskoristiti za identifikaciju pojedinačnih osoba. Velike tehnološke kompanije poput Google-a, Facebook-a i Amazona su već odavno ažurirali svoju praksu i pravila o privatnosti u skladu sa GDPR-om. Kompanije koje su izvršile usklađivanje će ostvariti konkurentsku prednost u odnosu na kompanije koje to nisu učinile. Nakon što izvrše internu procjenu svojih sistema, organizacije će vjerovatno morati unijeti promjene u svoje tehnološke platforme kako bi ispunili zahtjeve GDPR-a. Ovaj propis također zahtijeva od kompanija da stanovnicima EU ponude prava na privatnost, pravo na pristup podacima, pravo na prenosivost podataka. Korisnik ima pravo da od kompanije zatraži informaciju u koju svrhu će se koristiti njihovi podaci, ukoliko korisnik nije zadovoljan načinom na koji kompanija obrađuje njihove podatke može od kompanije da zatraži brisanje ličnih podataka. Kako bi udovoljili zahtijevima svojih klijenata kompanije će morati prilagoditi i unaprijediti svoje platforme i sisteme, uložiti mnogo resursa i radne snage, te promijeniti prakse oglašavanja i procese pohrane podataka. Uticaj GDPR-a na američke i kineske kompanije je veliki s obzirom na to da SAD i Kina, dvije vodeće svjetske gospodarske sile, imaju mnogo kompanije koje posluju sa EU. Prema istraživanju PricewaterhouseCoopers, 68 % američkih kompanija će potrošiti između 1 i 10 miliona dolara kako bi ispunile zahtijeve GDPR-a, a 9 % će potrošiti više od 10 miliona dolara. Ovi visoki troškovi na samom kraju će najviše utjecati na potrošače i samim tim će oslabiti konkurentsku prednost kineskih i američkih preduzeća. Pozivajući se na zakone GDPR-a, Evopska komisija će opužiti kineske i amričke kompanije da imaju probleme u vezi sa zaštitom podataka stanovnika EU i na taj način oslabiti i blokirati njihova ulaganja na području Evropske unije. Neke kineske i američke kompanije pokušale su uskladiti svoje poslovanje sa GDPR-om kao npr. Huawei koji je imenovao službenike za zaštitu podataka i YouTube koji je nakon stupanja na snagu ovog propisa prestao podržavati usluge oglašavanja trećih strana za kupovinu u Evropi. Sa druge strane mnoge kompanije su objavile da neće više pružati usluge evropskim korisnicima, zbog nemogućnosti usklađivanja sa propisima GDPR-a. Facebook, Instagram, WhatsApp kao i Google su tuženi nekoliko sati nakon stupanja GDPR na snagu (Li*, et al.*, 2019).

U veoma zahtijevnom okruženju gdje vlada konstantni tehnološki napredak, zaštita osjetljivih podataka postala je sve veći izazov. U svom istraživanju autori nastoje istražiti uobičajene izazove sa kojima se součava sigurnost podataka, ističući i konstantne prijetnje kao što su kršenje privatnosti podataka, unutrašnje i vanjske prijetnje. Povrede podataka predstavljaju ogromnu i konstantno prisutnu prijetnju, izlažući kompanije rizicima i

ostavljajući velike posljedice na samo poslovanje. Ovo kršenje privatnosti često od strane cyber kriminalaca ugrožava povjerljivost i cjelovitost ličnih podataka. Uticaj povrede podataka sa sobom nosi i mnoge posljedice, poput finansijskih gubitaka, narušenog ugleda kompanije, te pravnih posljedica. Insajderske prijetnje zlonamjerne ili nenamjerne predstavljaju značajan rizik za sigurnost podataka. Zaposlenici ili poslovni partneri mogu namjerno ili nenamjerno ugroziti sigurnost ličnih podataka kroz neovlašteni pristup, krađu podataka ili sabotažu. Uspostavljanje ravnoteže između povjerenja i potrebe za strogim kontrolama predstavlja konstantni izazov za organizacije. Ransomware napadi su sveprisutan oblik cyber kriminala. U ovim napadima zlonamjerni softver kodira podatke kompanije, čineći podatke nedostupnim dok se ne plati tražena otkupnina. Kako bi to spriječili organizacije moraju usvojiti proaktivne mjere, poput redovnih sigurnosnih kopija, obuke zaposlenika, napredne sisteme za otkrivanje prijetnji s ciljem sprječavanja ransomware napada i minimiziranja njihovog uticaja (Miryala i Gupta, 2022).

U području digitalnih informacija, gdje je protok osjetljivih podataka konstantan, uloga enkripcije je veoma važna. Enkripcija osigurava povjerljivost i integritet podataka u mirovanju i podataka koji se dijele. Pretvaranje običnog teksta u nečitljiv kod, onemogućava pristup neovlaštenim osobama. End-to-end enkripcija osigurava da podaci ostanu sigurni od svoje izvorne tačke do svog odredišta. Povrede podataka povećale su strahove u vezi sa sigurnošću ličnih podatakai rizike od krađe identiteta ili zlonamjernog iskorištavanja. Kao odgovor na ovu zabrinutost kreirani su opći propisi o zaštiti podataka (GDPR) i Kalifornijski zakon o privatnosti potrošača (CCPA). GDPR omogućava pojedincima pravo nad vlastitim podacima, uključujući pravo na pristup, brisanje, ispravljanje i zabranu obrade podataka (Miryala i Gupta, 2022).

Politou *et al.* (2018) navode da velike promjene koje GDPR donosi značajno utiču na kompanije koje posluju unutar i izvan teritorija EU. Privatnost i zaštita ličnih podataka dva su međusobno povezana pojma koja se često koriste naizmjenično, ali su zapravo dva različita pojma. Privatnost se prvenstveno odnosi na zaštitu "ličnog prostora" pojedinca, dok se zaštita podataka odnosi na ograničenja ili određene uslove obrade podataka koji se odnose na pojedince. Kako bi se spriječile i ublažile štete koje se dešavaju prilikom obrade ličnih podataka i posljedice za vlasnike podataka, mnoge metode i tehnička rješenja su uvedena proteklih godina. Neke od njih su i minimalizacija podataka i ograničenje svrhe gdje su organizacije dužne ograničiti prikupljanje ličnih podataka na najmanji mogući nivo potreban za postizanje konkretnih ciljeva, kao i brisanje podataka koji se više ne koriste u svrhe za koje su prikupljeni. Također, izgradnja povjerenja korisnika je veoma važna, naročito u doba kada većina današnjih korisnika nije ni svjesna količine podataka koji se prikupljaju i koje kompanije obrađuju.

Uvođenje GDPR-a sa sobom donosi i brojne izazove za kompanije. Uslovi za dobivanje odobrenja od korisnika prema GDPR-u postali su strožiji, kompanije moraju definisati uslove za dobivanje odobrenja, jer oni ne mogu samo biti informativni i konkretni, već

moraju biti nedvosmisleni i jednostavni za tumačenje. Samim tim potrebno je uložiti dosta vremena i napora kako bi se izvršile izmjene i dopune aktuelnih obavijesti o zaštiti podataka. GDPR također dozvoljava korisnicima da povuku dozvolu za korištenje njihovih podataka koju su prethodno dali. Korisnik ima pravo povući svoju dozvolu u bilo kojem trenutku i to će se odnositi na sve buduće obrade podataka, ali ne i na obrade koje su ranije izvršene. Sve ovo navedeno može značajno uticati na planove koje je kompanija nastojala provesti upotrebom prethodno prikupljenih podataka. Još neki od izazova sa kojima se kompanije susreću prilikom usklađivanja vlastitog poslovanja sa GDPR-om jeste taj što je GDPR uglavnom pravni dokument, koji pruža veoma malo ili čak nimalo tehničkih smjernica kompanijama koje su dužne da ga implementiraju. Sve ovo može uzrokovati nepredviđene komplikacije organizacijama koje pokušavaju prilagoditi svoje interne procese propisima GDPR-a. Jedna od najčešćih poteškoća jeste i usklađenost postojećih sigurnosnih procesa kako bi se ispunili zahtijevi zaboravljanja ili brisanja podataka. Kompanije su dužne redovno kreirati i čuvati sigurnosne kopije svojih podataka u slučaju da se dese sigurnosni incidenti ili fizičke katastrofe (Politou, *et al.*, 2018).

Kao odgovor na treće istraživačko pitanje u svom istraživanju autori Presthus & Sorum (2019) proučavaju privatnost informacija iz perspektive potrošača prateći Opštu uredbu EU o zaštiti podataka (GDPR), kao i podkategoriju informacijska privatnost, čiji je glavni fokus kontrola pojedinaca nad njegovim ličnim podacima. Istraživanja su pokazala da potrošači nisu mnogo zabrinuti za svoju privatnost, te da su razlozi za to različiti, od potrošačevog nerazumijevanja i nedovoljne informisanosti, do svjesne odluke o odricanju zaštite ličnih podataka u zamjenu za određene beneficije.

Obično se svako uvođenje novina i usklađivanja novih zakonskih uredbi doživljava kao trošak za kompanije, međutim uvođenje novih propisa ne treba gledati kao na neku prepreku već kao izvrsnu priliku za poboljšanje utiska o kompaniji među postojećim klijentima, te kao veliku prednost prilikom pridobijanja novih potencijalnih klijenata (Kabanov, 2016).

Presthus i Sorum (2019) navode da 74 % ljudi koji su se prijavili za pristup nekoj društvenoj uslužnoj mreži su preskočili čitanje pravila o privatnosti za šta bi im trebalo 29-32 minute, a u prosjeku su proveli manje od 1 minute čitajući uslove usluge, za šta bi im inače trebalo 15-17 minuta. To ukazuje da korisnici obraćaju veoma malo ili nimalo pažnje na takve informacije i govori zapravo o onome što istraživači nazivaju paradoksom privatnosti, u kojem potrošači tvrde da su zabrinuti za svoju privatnost, ali se ne ponašaju u skladu sa tim. Kao primjer autori navode da potrošači mogu izraziti namjeru da zaštite svoje lične podatke, ali će veoma brzo odustati od toga i otkriti podatke u zamjenu za pogodnosti pri online kupovini. Tehnološki napredak poput big data-e i umjetne inteligencije omogućio je široku dostupnost ličnih podataka, pa je samim tim kompanijama znatno olakšano prikupljanje i analiziranje ponašanja potrošača, kao i kupovne navike online potrošača. Osnovni cilj GDPR-a jeste usklađivanje zakona o privatnosti podataka širom Europe, te povećanje

transparentnosti i prava potrošača. Sama provedba GDPR-a predstavlja niz tehnoloških izazova kao i rješenja.

Presthus i Sorum (2019) su vršili prikupljanje podataka tokom februara i marta 2019. godine putem online anketnog upitnika. Upitnik se sastojao od 17 pitanja, 4 popratna pitanja, 12 primarnih anketnih pitanja i 1 otvoreno polje za komentare na kraju ankete. Ispitanici su također imali mogućnost pružiti kvalitativne povratne informacije za svih 12 primarnih anketnih pitanja. Osnovna svrha ove ankete jeste uvid u stavove potrošača o privatnosti informacija, kao i davanje ispitanicima mogućnost da podijele svoja razmišljanja u vezi sa temom ankete. Upitnik je sastavljen pomoću Likertove skale, pitanja višestrukog izbora, te pitanja otvorenog tipa koja su zahtijevala kvalitativne odgovore. Učestvovanje u anketi je bilo dobrovoljno i anonimno, a učesnici su imali mogućnost odustati od ispunjavanja ankete u svakom momentu. U ovoj anketi učestvovalo je 327 ispitanika, a prosječno vrijeme ispunjavanja ankete je bilo 6 minuta. Istraživački tim je izvršio detaljnu analizu dobivenih rezultata uz upotrebu deskriptivne statistike, s ciljem dobivanja općeg dojma o podacima. U istraživanju je učestvovalo 54 % muškaraca i 45 % žena , a najviše ispitanika bilo je u dobi od 21 do 25 godina , a zatim u skupini od 26 do 30 godina. Analizom podataka također je utvrđeno da je 62 % ispitanika izjavilo da su čuli za GDPR, te izjavili da razumiju značenje i sadržaj ove uredbe, 31 % ispitanika je znalo malo o GDPR-u, 3 % nisu baš razumjeli uredbu, a gotovo 5 % nikada nije čulo za GDPR.

Presthus i Sorum (2019) su došli do zaključka da je većina potrošača bila umjereno ili vrlo svjesna uloge GDPR-a i svojih prava prema ovoj uredbi, ali nisu baš bili sigurni kako će se organizacije prilagoditi i kako će postupati s novih propisima, također bilo je varijacija u načinima razmišljana potrošača i tome kako oni gledaju na prikupljanje i obradu ličnih podataka, te smatraju da su potrošači pokazali relativnu veliku zabrinutost za svoju privatnost. GDPR omogućava potrošačima da vide koje se informacije prikupljaju, obrađuju i pohranjuju i daju im pravo na ispravljanje pogrešaka, međutim niko od sudionika nije rekao da je izvršio bilo kakve ispravke.

Prema propisima GDPR-a potrošači također imaju pravo i na brisanje nekih svojih ličnih podataka. Ovo se odnosi na podatke koje je kompanija prikupila i pohranila o pojedincu, ali također važno je napomenuti da GDPR ne uključuj pravo na brisanje svih podataka, već na odabrane dijelove. Među njihovim ispitanicima 68 % vjeruje da bi možda željeli zatražiti od kompanije da izbriše njihove podatke, a 15 % je već to učinilo. Ovo je zapravo još jedan dokaz da pitanje privatnosti zabrinjava mnoge potrošače. Iako potrošači imaju pravo da ne prihvate uslove i odredbe web stranice ili aplikacije, rezultati pokazuju da su potrošači veoma brzo odobravali te uslove iako je bilo sasvim jasno da nisu bili dobro upoznati sa sadržajem koji odobravaju, bez čitanja prihvatali su sve uslove. Samo 1% ispitanika je izjavilo da su uzeli vremena za čitanje cijelog teksta, dok je 17 % brzo prelistalo i nisu pročitali sve, 60 % ispitanika je kliknulo prihvatam bez da su uopšte pročitali tekst, preostalih 20 % je izjavilo da su im reakcije različite. Većina ispitanika je izjavilo da im je

stalo do privatnosti, ali da su tekstovi za prihvatanje uslova i odredbi predugi ili preteški za razumijevanje. Na samom kraju ispitanicima je bilo omogućeno da ostave bilo kakav komentar o samoj anketi. U komentrima koje su dobili od 8 osoba, pola su bili pozitivni i anketu su okarakterisali kao zanimljivu i poučnu, dok je troje izjavilo da je bilo previše obimno i da je čitanje pitanja trajalo predugo (Presthus i Sorum, 2019).

GDPR također omogućava potrošačima da odluče prihvatiti neke, ali ne sve kolačiće na web stranicama prilikom posjete web stranice. Kompanije bi trebale otkriti svrhu za koje će se koristiti podaci koji pohranjuje svaki kolačić. Od stupanja na snagu GDPR-a, mnoge kompanije su implementirale ovo pravilo, samim tim posjetitelji često nailaze na informacije koje opisuju korištenje kolačića na web stranici. Gotovo polovina ispitanika smatra da su kompanije postale puno bolje u informiranju posjetitelja njihove web stranice o kolačićima od kada su implementirali GDPR. Nešto manje od 30 % ispitanika je izjavilo da se osjeća nesigurno po pitanju svrhe kolačića na web stranici, a nešto više od 20 % tvrdi da kompanije daju potrošačima mogućnost isključivanja nekih kolačića (Presthus i Sorum, 2019).

Povećana zabrinutost u vezi sa privatnosti podataka, doprinijela je razvoju sposobnosti potrošača da kontrolišu kako se njihovi lični podaci prikupljaju, pohranjuju, koriste i dijele. Posljednjih 25 godina primijetan je sve veći uticaj i korištenje društvenih medija od strane potrošača. Prikupljanje podataka, istraživanje i analiza navika potrošača u cilju poboljšanja poslovanja se također značajno preusmjerilo na društvene medije i internet. Potrošači često dijele vlastite informacije kao što je ime, datum rođenja, podatke o kreditnoj kartici sa određenim web stranicama koje posjećuju, a 79% odraslih u SAD-u navodi da su veoma ili donekle zabrinuti kako kompanije koriste podatke koje prikupljaju o njima. Prije nego što su propisi o privatnosti podataka stupili na snagu, potrošači su mogli brisati kolačiće ručno ili putem postavki web preglednika, ali potpuna prevencija zaštite ličnih podataka nije bila moguća. Kompanije su mogle kupiti lične podatke od trećih strana bez pristanka potrošača. U skladu sa tim, dva osnovna zahtijeva prema GDPR-u koje kompanije moraju ispoštovati jeste da moraju obavijestiti potrošače koji će se podaci prikupljati i u koje svrhe, te da je potrebno dobiti izričitu potvrdnu saglasnost za korištenje podataka. Ukoliko potrošači ne pristanu na prikupljanje i dijeljenje njihovih podataka, tada oglašivači ne mogu učinkovito pratiti ponašanje potrošača preko web stranica. Samim tim mogućnosti ciljanja oglašivača na stvarne potrošače su drastično smanjena, te ulaganje u oglase na društvenim medijima mogu biti uzaludna, jer kompanije ne znaju na koga tačno trebaju usmjeriti te oglase (npr. prikaz oglasa potrošačima koji su već obavili kupovinu, a cilj su im zapravo novi potencijalni klijenti). Dok sa druge strane ukoliko potrošači pristanu na prikupljanje njihovih podataka, oglašivači mogu ciljati oglase na publiku od koje mogu imati koristi. Više podataka omogućava bolje ciljanje potrošača od strane kompanija na tržištu oglašavanja. Zaključak ovog istraživanja jeste da propisi o privatnosti podataka pomažu potrošačima prilikom sprječavanja dijeljenja njihovih podataka ukoliko bi to dijeljenje moglo narušiti njihovu privatnost, dok sa druge strane ovi propisi mogu naštetiti manjim izdavačima, oglašivačima i oglasnim mežama. Nakon ovih propisa, manjina potrošača je odlučila ne dati pristanak za

prikupljanje, korištenje i dijeljenje njihovih ličnih podataka, dok većina potrošača i dalje ne shvataju suštinu pravila o privatnosti, te je potrebno uložiti više napora kako bi se to promijenilo (Choi i Jerath, 2022).

Važnost razumijevanja brige o privatnosti potrošača i načina na koji treba ublažiti tu zabrinutost treba biti prioritet svake organizacije. Potrošači osjećaju nesigurnost kada organizacije prikupljaju prekomjerne količine njihovih ličnih podataka. Povećanje kontrole, smanjenje rizika i izgradnja povjerenja predstavlja mehanizme za vraćanje osjećaja privatnosti kod potrošača. Da bi izgradile te mehanizme organizacije moraju biti transparentne prilikom prikupljanja i obrade podataka. Politike privatnosti, predstavljaju oblik osiguranja privatnosti i alate komunikacije koji se koriste kako bi informisali kupce o praksi privatnosti organizacije. Uprkos svojoj popularnosti, politike privatnosti donose i mnoge probleme. Često znaju biti prilično dugačke i teške za čitanje, mnogi potrošači ne čitaju pravila o privatnosti, a oni koji čitaju ponekad ne razumiju sadržaj istih. Nedavno israživanje je pokazalo da 38 % odraslih Amerikanaca ponekad čita pravila o privatnosti, ali samo 8 % razumije sadržaj. Samim tim politike privatnosti mogu imati suprotne efekte u odnosu na planirane, pogoršavajući, a ne umirujući zbunjenost potrošača. Prema GDPR-u vlasnici podataka imaju bravo biti upućeni o: kontakt podacima osobe koja vrši kontrolu podataka; svrsi i pravnoj osnovi za obradu ličnih podataka; mjerama zaštite u slučaju prijenosa podataka trećoj osobi; pravima za pristup, ispravak, ograničenje obrade, brisanje i prenosivost podataka; pravu na povlačenje dozvole u bilo kojem trenutku; pravu na žalbu nadzornom tijelu itd (Fox, *et al.,* 2022).

Van Ooijen i Vrabec (2019) navode da je napredak informacionog doba doveo do porasta online transakcija a samim tim i do sve većeg protoka podataka o potrošačima. Zbog povećane tehnološke složenosti i velikog iskorištavanja podataka, potrošačima je sve teže da steknu kontrolu nad svojim ličnim podacima. Jačanje kontole pojedinaca nad vlastitim podacima bio je jedan od ključnih ciljeva GDPR-a. Osnovni preduslov koji bi se trebao ispuniti kako bi vlasnici podataka imali kontrolu nad nad svojim podacima jeste informisanost o obradi podataka. Kako bi imao kontrolu, vlasnik podataka bi trebao biti u mogućnosti da donosi odluke koje su u skladu sa njihovim stavovima i preferencijama ili bi barem trebali biti upoznati sa tim šta ta obrada podataka podrazumijeva. Prema propisima GDPR-a, vlasnik podataka mora biti obaviješten prije nego što se izvrši obrada njihovih podataka, zatim mora biti obaviješten o svrhama za koje će se podaci obrađivati, o identitetu osoba koje vrše obradu, o primateljima njihovih ličnih podataka, te o roku čuvanja tih podataka.

U današnjem modernom dobu podaci se ne koriste samo jednom, oni se dijele i koriste više puta i često su zloupotrebljeni. Jedan od primjera zloupotrebe je slučaj Cambridge Analytica, kompanije koja je neovlašteno koristila lične podatke miliona američkih korisnika Facebook-a, te je te podatke koristila za ciljanje korisnika u svrhu promoviranje vlastitog poslovanja. U situacijama kada obrada podataka nije u skladu sa zakonima koje propisuje

GDPR, obrada se može smatrati nezakonitom i vlasnici podataka imaju pravo da zahtijevaju da se njihovi podaci izbrišu. To se može desiti kada podaci više nisu potrebni za svrhu za koju su se prvenstveno prikupljali i obrađivali ili jednostavno kada vlasnik podataka povuče svoju dozvolu za korištenje. Pravo na brisanje podataka kao i obaveza osobe koja je vršila obradu podataka da obavijesti drugu stranu o zahtijevu vlasnika podataka za brisanje, povećava individualnu kontrolu vlasnika nad njegovim podacima (Van Ooijen i Vrabec, 2019).

Za četvrto istraživačko pitanje autori navode: Kompanije sve više iskorištavaju lične podatka kako bi poboljšali proizvode te kreirali nove poslovne modele. Ipak, korištenje ličnih podataka od strane organizacije može stvoriti izazove za pojedince, grupe i društva. Propisi o privatnosti podataka pokušavaju riješiti te izazove definisanjem pravila o tome kako kompanije trebaju rukovati sa podacima. Kompanije često navode da ih strogi propisi EU o zaštiti podataka stavljaju u nepovoljniji položaj u odnosu na kompanije u zemljama sa blažom regulativom. Međutim drugi tvrde da su strožiji propisi potrebni kako bi se vratilo povjerenje u digitalnu ekonomiju. U svom istraživanju autori nastoje istražiti kako propisi o privatnosti podataka utječu na korporativne inovacije, fokusirajući se na start up kompanije. Željeli su dati odgovor na pitanja poput toga kako regulacije o privatnosti podataka utiču na inovacije u start up kompanijama?, da li oni sputavaju ili potiču razvoj novih proizvoda i usluga i da li povećavaju ili smanjuju ukupnu inovativnost?. Blind (2012) ističe da se "regulacija odnosi na bilo koji opći oblik prisilne vladavine postavljene od strane vlada s ciljem uticaja na tržišnu aktivnost i njene aktere". Evropski zakon o zaštiti podataka (GDPR) nastoji zaštititi lične podatke od strane cyber kriminalaca (hakera) i insajdera tj. zaposlenika kompanija koje rade u suprotnosti sa pravilima
organizacija, te od nezakonite obrade podataka od strane organizacija. Ovo se može postići provođenjem oštrih kontrola procesa obrade i uslova pod kojima se podaci mogu prenijeti u inostranstvo (Martin, *et al.*, 2019).

Kroz ovo istraživanje došli su do zaključka da nametnuto provođenje ovih propisa može dovesti do toga da kompanije odustanu od sprovođenja inovacija, te se usredotočiti na druge procese sa manje regultornih ograničenja, zatim mogu prilagoditi inovacije zakonskim propisima na način da koriste anonimne podatke umjesto ličih podataka. Treća opcija jeste da namjerno krše propise, uz rizik da se suprotstave vlastima i suoče sa kaznenim posljedicama. Za koju od ove tri opcije će se kompanije odlučiti ovisi o kombinaciji unutrašnjih i vanjskih faktora, uključujući njihove finansijske i tehnološke faktore, očekivanog nivoa tržišne potražnje za proizvodom i očekivanog nivoa provedbe propisa. Detalji navedeni u propisima također mogu uticati na izbore i rezultate kompanija. Ukoliko propisi zabranjuju mogućnost razvoja i dizajna proizvoda do nivoa da je veoma teško inovirati proizvod koji će poštovati zakone propisa i pored svega imati tržišni potencijal. Kao četvrtu opciju navode kreiranje rješenja koji će pomoći kompanijama prilikom postizanja usklađenosti, a bez oštećenja njihove redovne proizvodnje i aktivnosti stvaranja proizvoda koji se može prodati onima na koje se propis i odnosi (Martin, *et al.*, 2019).

U dobu brze digitalne transformacije, vještačka inteligencija (AI) se počela primjenjivati u različitim sektorima, pa se samim tim počela postavljati pitanja u vezi sa zaštitom podataka, implementacijom vještačke inteligencije i njene usklađenosti sa novim propisima. U svom istraživanju autori nastoje predstaviti interakciju između AI tehnologija i zaštite podataka. Uvođenje vještačke inteligencije u različite sektore sa sobom donosi i brojne izazove, naročito u pogledu zaštite privatnosti i podataka pojedinaca. Sposobnost AI tehnologija da obrađuje velike količine podataka, uključujući osjetljive i lične podatke i informacije, postavlja važna pitanja o etičkim i pravnim posljedicama usljed njihove upotrebe. U savremenom digitalnom dobu podaci se smatraju osnovnim resursom koji potiče stvaranje AI algoritama i modela. Ti resursi se odnose na lične živote pojedinaca, te njihova zloupotreba može dovesti do ozbiljnih povreda privatnosti i narušenog povjerenja. Osnovna tema u raspravama o umjetnoj inteligenciji i zaštiti podataka jeste provedba regulatornih propisa kreiranih kako bi zaštitili lične podatke u digitalnom okruženju. Opšta uredba o zaštiti podataka (GDPR) koja je stupila na snagu 2018. godine predstavlja stroge zakonske standarde za privatnost i sigurnost podataka širom Evrope. Mnoge studije istražile su ulogu GDPR-a u odnosu na druge regulatorne propise poput CCPA. Dok GDPR naglašava prava ispitanika i transparentnost, CCPA uvodi nove propise u vezi sa zabranom prodaje podataka potrošača i poboljšanim provođenjem privatnosti. Kako se vještačka inteligencija nastavlja širiti u raznim sektorima, zabrinutost oko zaštite i privatnosti podataka su se pojačale. Predloženi zakon EU o umjetnoj inteligenciji nastoji regulisati viskorizične aplikacije umjetne inteligencije nametanjem obaveza programerima da osiguraju usklađenost sistema umjetne inteligencije sa osnovnim pravima i sigurnosnim zahtjevima. Jedan od najvažnijih zadataka koji bi se trebao ispuniti kada je u pitanju vještačka inteligencija jeste minimizacija podataka, koja podrazumijeva prikupljanje samo onih podataka koji su nužni za određenu svrhu i njihovo zadržavanje i skladištenje ne bi trebalo biti duže nego što je potrebno. Obezbjeđivanje prakse minimizacije podataka može ublažiti rizik od prekomjernog prikupljanja i skladištenja podataka. Dobivanje dozvole za korištenje i obradu podataka je veoma važna stavka. Međutim kada je umjetna inteligencija u pitanju, gdje obrada podataka može biti veoma složena, osiguranje prava na pristanak postaje izazov. Kompanije koje koriste vještačku inteligenciju trebale bi uložiti velike napore kako bi omogućile usklađenost sa regulatornim propisima i omogućiti očuvanje privatnosti uprkos konstantnom tehnološkom napretku (Yanamala i Suryadevara, 2023).

U današnjem konkurentskom okruženju pružanje kvalitetnih usluga postala je veoma važna strategija za organizacije koje se oslanjaju na prikupljanje podataka o svojim klijentima. Organizacije sve više koriste lične podatke kako bi identificirali potrebe svojih klijenata i kako bi im na osnovu toga omogućili potreban proizvod ili određene pogodnosti. Zahvaljujući sve većoj upotrebi ličnih podataka javili su se i izazovi u vezi sigurnosti i privatnosti. Organizacije spremaju podatke u skladišta tj. u baze podataka koje često znaju biti meta napada zlonamjernih hakera. Napadi na baze podataka mogu ugroziti poslovanje organizacija i dovesti do velikih gubitaka, te ugroziti privatnost milionima ljudi. Klijenti burno reaguju i bojkotuju preduzeća u kojima lični podaci nisu sigurni ili su dospjeli u ruke

hakera. Blockchain tehnologija nudi rješenje za ovakve problem kroz decentralizaciju, prikupljanje, pohranjivanje i obradu podataka. To je baza podataka kojom se upravlja pomoću peer-to-peer mreže u kojoj je potrebno pridržavati se unaprijed definisanog protokola za komunikaciju i provjeru valjanosti zapisa ili blokova (Al-Abdullah, *et al.*, 2020).

Blockchain je trustless sistem koji eliminiše potrebu da treća strana potvrdi transakcije ili da olakša interakciju između kupca i preduzeća. Evropska unija je donijela Opštu uredbu o zaštiti podataka (GDPR). Ova uredba ima za cilj da standardizira pravila zaštite ličnih podataka u svim državama članicama EU, te da poboljša sposobnost preduzeća da obrađuju informacija građana EU u cilju pružanja boljih usluga, a istovremeno i zaštite prava i slobode građana. Nakon uspostave GDPR-a, blockchain tehnologije su brzo uznapredovale. U trenutku kada je GDPR postao aktivan, propisi nisu razmatrali blockchain, što je dovelo do napetosti među njima. Ovaj rad nastoji istražiti nepovezanost između GDPR-a i razvoja blockchain tehnologije, te mogućnosti i prepreke njihovog usklađivanja. Blockchain je decentralizirano rješenje koje korisnicima daje vlasništvo nad njihovim podacima i eliminiše potrebu za trećom stranom u interakciji sa korisnikom. Iako blockchain koristi kriptografske tehnike za šifriranje podataka, pokazalo se da se i takvi podaci (iako su to šifrirani podaci razumljivi samo onima koji ih znaju pročitati tj. oni kojima su ti podaci namjenjeni) definišu kao lični podaci, pa se samim ti blockchain tehnologije trebaju pridržavati propisa koje nameće GDPR. Da bi blokchain tehnologija bila u skladu sa pravilima GDPR-a , potrebno je pripremiti detaljan ugovor koji objašnjava sigurnost transakcija i metode koje se koriste prilikom upotrebe i obrade podataka. Iako određeni tehnički aspekti ne mogu biti ispunjeni, usklađivanje sa GDPR-om ipak može biti postignuto. Potrebno je da se definišu pravila, propisi i politike za osiguranje privatnosti putem određene dokumentacije. Ti propisi trebaju uključivati korisničke ugovore koji precizno definišu kako korisnici mogu ostvariti svoja prava na upravljanje podacima i koja su to sve ograničenja prisutna u samom sistemu. Također propisi za provjeru uključuju i mogućnost praćenja i revizije mjera privatnosti obrade podataka, posjedovanje pravih razloga za provođenje aktivnosti obrade podataka, imati jasnu politiku privatnosti podataka, kao i posjedovanje tehničkih mjera za obezbijeđenje sigurnosti, svijesti i privatnosti ličnih podataka (Al-Abdullah, *et al.*, 2020).

Opšta uredba o zaštiti podataka stupila je na snagu 25. maja 2018-te godine i njen osnovni zadatak jeste postaviti nove standarde za obradu ličnih podataka unutar EU i van EU ukoliko se koriste podaci njihovih građana. Na osnovu svojih propisa GDPR utiče i na milione web usluga iz cijelog svijeta koje su dostupne na području EU. Osim što utiče na promjene načina na koji se obrađuju lični podaci, kompanije također moraju transparentno otkriti kako postupaju sa podacima, pravne osnove za prikupljanje podataka, te mehanizme za pojedinačni pristanak, pristup podacima i mogućnost brisanja i prenošenja podataka. Čak i online usluge koje su van EU su se morale pripremiti za GDPR, jer se on odnosi na sve kompanije koje nude svoje usluge na području EU. Kao rezultat toga, očekuje se da će ovi propisi imati veliki utjecaj na kompanije širom svijeta. Istraživanja su pokazala da su

promjene koje je sa sobom donio GDPR od datuma stupanja na snagu imale pozitivan efekat na transparentnost na web stranicama, 4,9% više stranica sada ima obavijesti za korisnike u vidu kolačića, s ciljem informisanja korisnika o njihovim pravima i pravnim osnovama vezanim za obradu njihovih podataka. U svom istaživanju analizirali su 500 najboljih web stranica u svakoj od država članica EU, uključujući i analizu politika privatnosti na 24 jezika u periodu stupanja GDPR-a na snagu. Dosta web stranica je već imalo pravila o privatnosti, a većina se prilagodila novim propisima. Najznačajniji je porast prikaza kolačića sa davanjem odobrenja na više od polovine web stranica. Međutim, ovi kolačići mogu korisnicima dati lažni osjećaj sigurnosti ukoliko nisu definisani u skladu sa propisima koje nalaže GDPR (Degeling, *et al.*, 2018).

Degeling *et al.* (2018) navode neke od zahtijeva koje su kompanije trebale ispuniti primjenjujući zakone koje GDPR nalaže su:

- Transparentnost – GDPR zahtijeva da svako ko vrši obradu ličnih podataka treba da obavijesti vlasnike podataka npr. u politici privatnosti, te predstaviti informacije na transaprentan i lako razumljiv način, koristeći jasnu i jednostavnu terminologiju koju će moći svi razumjeti,
- Zaštita podataka prema dizajnu i prema zadanim postavkama – gdje kompanije koje prikupljaju podatke trebaju osigurati da lični podaci budu zaštićeni u skladu sa zadanim postavkama i zahtijevom korisnika,
- Pristanak – obrada ličnih podataka je zakonita samo onda kada je vlasnik podataka dao saglasnost. Ukoliko je vlasnik podataka prisiljen dati saglasnost, to se ne smatra valjanom saglasnosti. Za djecu mlađu od 16 godina pristanak mogu dati samo roditelji,
- Pristanak na korištenje kolačića - zahtijev za pristankom ne vrijedi ukoliko je za pristup web stranici ili za isporuku usluge koju korisnik traži strogo neophodno prihvatiti sve navedene uslove. Izuzetak su web stranice koje ne bi radile bez postavljenih kolačića čiji je osnovni zadatak da pamte prijavu korisnika ili da npr. pamte stanje košarice prilikom internet kupovine.

Kao odgovor na posljednje istraživačko pitanje autori Buckley *et al.* (2021) ističu da je fokus njihovog istraživanja na regulaciji privatnosti podataka iz perspektive zanemarenih kompanija, s obzirom na to da je najviše pažnje usmjereno na prednosti GDPR-a u smislu poboljšanja privatnosti potrošača. Veoma malo ili nimalo istraživanja govori o uticaju GDPR-a na kompanije, koje moraju uložiti određena sredstva kako bi sve to uskladili sa svojim poslovanjem. Odlučili su sprovesti polustrukturirani intervju sa 14 rukovodilaca poslovanja u različitim kompanijama koje obrađuju podatke o kupcima, te smatraju da je ovo prva studija koja analizira iskustvo GDPR-a unutar preduzeća od njegovog uvođenja tokom tri godine i prva studija koja je identificirala kako je GDPR promijenio ravnotežu moći i donošenja odluka unutar organizacije. Cilj je bio ispitati male, srednje i velike kompanije kao i niz uloga i odjela poput IT, marketing odjela, pravnog odjela i sl. Sve

intervjue je vodio jedan autor kako bi se održala dosljednost. Istraživačka pitanja su bila sljedeća:

RQ1: Koje su prednosti GDPR-a za poslovanje?
RQ2: Jesu li prednosti GDPR-a različite unutar preduzeća?

Buckley *et al.* (2021) navode da regulacija donosi kako koristi tako i troškove. Može stimulirati ideje i može blokirati njihovu provedbu, može povećati ili smanjiti rizik ulaganja u nove proizvode i poslovne modele, može utjecati na povjerenje i potražnju potrošača. Iz tog razloga većina razvijenih ekonomija ima politike, procedure i institucije koje upravljaju načinom na koji se propisi razvijaju, provode i pregledavaju. Pored prednosti, postoji i veliki broj studija o izazovima koji donosi GDPR. To je složeni proces, ne specificira tehnička rješenja, uključuje subjektivnost i usklađivanje može biti veoma skupo.

Kompanije će možda trebati dodatne zaposlenike u administraciji, ekstra obuke zaposlenika, a također se suočavaju sa poteškoćama prilikom zapošljavanja i zadržavanja ljudi. Regulatorna ograničenje mogu uticati na kompanije izvan EU, te uvjeriti neke da smanje njihovu ponudu usluga unutar Europske unije kako bi to izbjegli. Prenos podataka, kao i pristanak za obradu podataka, ispravak i procesi brisanja zahtijevat će tehnička i organizacijska ulaganja. Brisanje podataka bi predstavljalo problem za velike kompanije, revizije sistema i procesa kao i zapošljavanje više stručnjaka za cyber sigurnost zahtijevat će velika ulaganja. Proces razumijevanja kako se postupa sa ličnim podacima može znatno usporiti razvoj i primjenu novih tehnologija poput IoT i blockchain. GDPR je stavio u nepovoljan položaj mala i srednja preduzeća nametanjem previsokih troškova, a samim tim ih potiču i na izlazak sa tržišta (Buckley, *et al.*, 2021).

Svaki intervju se sastojao od četiri dijela:

1. Otvorena pitanja o pojedincu, njegovom poslu, naziv kompanije, veličinu kompanije i sektor kojem pripada
2. Otvorena pitanja kako je to GDPR uticao na njihov posao, odjele i cjelokupnu kompaniju
3. Ciljana pitanja koja su istraživala prednosti GDPR-a
4. Ciljana pitanja koja su istraživala nedostatke GDPR-a.

Buckley *et al.* (2021) su željeli istražiti koje su prednosti GDPR-a za poslovanje, te da li se one razlikuju unutar preduzeća. Kompanije najčešće koristi klasificiraju kao direktne i indirektne. Direktne koristi imaju jasan uzročno-posljedični odnos, dok su indirektne koristi manje jasne. Direktne koristi će dovesti do novih prihoda ili smanjenja troškova i može se kvantificirati, dok se indirektna korist često ne može izmjeriti. Također, prednosti mogu biti planirane ili neplanirane.

Svi sagovornici istakli su važnost zaštite podataka i privatnost. GDPR je rukovodioce posla učinio svjesnijim o privatnosti podataka kako na poslovnoj tako i na ličnoj razini. Jedan od

ispitanika ističe da svi imamo privatne živote i znamo kako je to kada neko bez odobrenja koristi naše podatke, te smatra da se sa tuđim podacima treba ponašati kao sa vlastitim. GDPR je promijenio način ponašanja kompanija prilikom korištenja podataka. Drugi ispitanik ističe da je GDPR podigao svijest unutar poslovanja o ličnim podacima, istakao važnost njihove zaštite i tretiranja na specifične načine. Ukratko GDPR je učinio da kompanije postanu odgovornije i pažljivije prilikom korištenja informacija. Novi propisi o zaštiti podataka mogu od kompanije zahtijevati promjene u vidu ljudi, procesa i tehnologija, u zavisnosti od toga koliko je njihov model rada bio približan modelu koji zagovara GDPR. Pretpostavimo da je kompanija morala kupiti novi sistem kako bi ispunila uslove nove uredbe, koji sa sobom donosi i određene troškove, a u isto vrijeme mogla je taj novac uložiti u nešto što stvara višu vrijednost kao što je razvoj novih proizvoda ili širenje na novo tržište. Od šest kompanija koje su učestvovale u istraživanju, dvije nisu napravile nikakve promjene na njihovu IT strukturu, jedna je poboljšala klasifikaciju podataka, jedna kompanija je osnovana u istom periodu kada je nastao i GDPR te su na samom početku usvojili ovu uredbu, a kao najznačajniju korist od GDPR-a navodi "dovođenje stvari u red", provođenje digitalizacije i automatizacija mnogih sistema. Jedna od većih kompanija ističe da su iskoristili GDPR kao priliku za objedinjavanje baze podataka svih potrošača u zemlji, za standardizaciju unosa podataka, proširenje kontrole pristupa, te unapređenje informacijske sigurnosti. Oni su uveli i standarde kao što su minimizacija podataka i razdoblja zadržavanja podataka tj. kompanija sada ima pravilo koje podrazumijeva brisanje podataka o potrošačima ukoliko nisu komunicirali sa njima više od godinu dana (Buckley, *et al*., 2021).

Način na koji kompanije doživljavaju troškove je različit. Osim troškova povezanih sa GDPR-om, kao što su dodaci o obavijestima za kolačiće, mala i srednja preduzeća ističu da im je teško odrediti dodatne troškove. Većim kompanijama bilo je lakše jer su napravile velika ulaganja u sisteme, procese i radnu snagu koji će im u buduće znatno olakšavati posao. Na samom kraju intervjua zamolili su ispitanike da iznesu svoje ideje kako bi GDPR mogao biti bolji. Sva mala i srednja preduzeća smatraju da je GDPR pretjeran za kompanije poput njihovih koji sadrže mali broj podataka u odnosu na velike kompanije koje imaju veliki broj podataka. Jedan od ispitanika se pita zašto bi se oni trebali pridržavati istog standarda kao i neka medicinska ustanova koja ima osjetljive lične podatke. Također, istraživanje je pokazalo da GDPR predstavlja neočekivanu dobit za kompanije koje pružaju pravne ili tehnološke savjete i usluge povezane sa GDPR-om. Za većinu kompanija kojoj GDPR nije osnovna djelatnost također ima koristi, jer je prijetnja kaznama promijenila način razmišljanja kompanija. U svijetu u kojem privatnost podataka postaje sve važnija, GDPR je prisilio kompanije da prate želje svojih klijenata i da koriste njihove podatke samo na način na koji oni to žele. GDPR je natjerao kompanije da moderniziraju i unaprijede svoje upravljanje podacima, kvalitetu podataka i informacijsku sigurnost (Buckley, *et al.*, 2021).

Frey i Presidente (2024) u svom radu ispituju kako je regulacija o privatnosti podataka uticala i oblikovala poslovanje kompanija. Kako bi dobili odgovor na ovo istraživanje, ispitali su uticaj GDPR-a na dobit i prodaju kompanija u 31 zemlji i 22 industrije. GDPR bi mogao uticati na poslovanje kompanija na dva načina. Kao prvo od kompanija se zahtijeva

da razvija procese i tehnologije usklađene sa GDPR-om, što stvara dodatne troškove i smanjuje profit. Drugo, ukoliko korisnici imaju poteškoće u razumijevanju uslova i njihovom prihvatanju, to može dovesti do smanjenja online kupovine, a samim tim i smanjenja ukupne prodaje. Pored toga, ukoliko pretpostavimo da su dostupni podaci veoma važni za ciljano oglašavanje, koje utiče na povećanje prodaje, naglo povećanje troškova pohrane i obrade podataka povezanih sa GDPR-om, moglo bi doprinijeti lošem ciljnom oglašavanju, što narušava uspješnost kompanije. Također ističu da je uvođenje GDPR-a negativno uticalo na uspješnost preduzeća, tačnije na njene troškove, gdje su kompanije istakle da su doživjele smanjenje dobiti od 2,1% kao odgovor na provedbu GDPR-a, dok je prodaja ostala nepromjenjena, što znači da je ova nova uredba utjecala negativno na kompanije zbog dodatnih i neplaniranih troškova usklađivanja. GDPR je dodatno povećao troškove kompanija, iako ne operativne troškove, što ukazuje na to da je negativni učinak GDPR-a vjerovatno prolazan, s obzirom na to da se negativni efekat na dobit znatno smanjio godinu dana nakon provedbe novih propisa.

Kompanije koje posluju unutar Evropske unije su dužne poštovati GDPR, koji utvrđuje pravila o tome kako se trebaju obrađivati lični podaci stanovnika EU. GDPR se također odnosi i na kompanije koje su registrovane izvan EU, a koje ciljaju potrošače koji žive na području Evropske unije. Osnovni cilj ove regulacije jeste dati pojedincima više kontrole nad ličnim podacima, dok istovremeno potiče kompanije da ograniče upotrebu takvih podataka za aktivnosti poput marketinga ili za obradu podataka bez prethodnog odobrenja. Samim tim što ova regulacija određuje pravnu osnovu na osnovu koje kompanije može ili ne može obrađivati lične podatke, GDPR utiče na preduzeće na nekoliko načina kao što je zabrana web stranicama dijeljenje korisničkih podataka sa trećim stranama, bez odobrenja vlasnika podataka (što utiče na povećanje troškova kompanije prilikom prikupljanja podataka i smanjuje mogućnost kompanije da dođe do podataka). To također omogućava stanovnicima EU pravo na pristup, ažuriranje, ispravljanje i brisanje ličnih podataka, što znači da kompanije moraju dosta uložiti u razvoj informacionih tehnologija i softvera koji će sve to omogućiti. Pored toga kompanije koje koriste lične podatke stanovnika EU moraju ih šifrirati i učiniti anonimnim, te ažurirati svoje postojeće interne procese kako bi osigurali usklađenost. To uključuje i angažovanje službenika za zaštitu podataka koji će nadgledati sve aktivnosti upravljanja podacima. Troškovi usklađivanja koji su nametnuti kompanijama su značajni, posebno za one kompanije čije se poslovanje temelji na obradi ličnih podataka. Prema PwC-u neke kompanije su potrošile više od miliona eura godišnje samo na usklađivanje sa GDPR-om. Međutim, cijena za nepoštivanje ovih propisa mogu biti znatno veće i iznose 20 miliona eura ili 4 % globalnog prihoda. Primjenom kazni na globalni prihod, a ne na prihod iz zemalja EU, ovaj propis potiče multinacionalne kompanije čije je ciljno tržište stanovništvo EU, da se pridržavaju njegovih pravila. Velike novčane kazne su izrečene brojnim kompanijama kao što su Google (50 miliona eura), H&M (35 miliona eura), British Airways (22 miliona eura), Marriot (20,4 miliona eura). Također ističu i da u u periodu od januara 2020-te do 2021. godine agencije za zaštitu podataka zabilježile 121.165 obavijesti o kršenju podataka, što je povećanje od 19 % u odnosu na prethodnu godinu (Frey i Presidente, 2024)

Tabela 1. Pregled korištenih istraživačkih radova

Istraživačka pitanja	***Broj radova***	***Autori***	***Odgovori na pitanja***
Koje su ključne teme i aspekti privatnosti podataka?	6 radova	(Alessi, *et al.*, 2019) (Aseri, 2020) (Tikkinen-Piri, *et al.*, 2018) (Romansky i Noninska, 2020) (Ghorashi, *et al.*, 2023) (Bauer, *et al.*, 2022)	-Privatnost podataka je podjednako važna kako za organizacije tako i za korisnike, -Kompanije koje prikupljaju, obrađuju i koriste lične podatke trebaju provesti određene prakse koje propisi nalažu kako bi obezbijedili zaštitu podataka potrošača, -Propisi o privatnosti podataka predstavaljaju skup pravila kojih se organizacije trebaju pridržavati u slučaju prikupljanja, korištenja i širenja podataka o pojedincima
Sa kojim izazovima se organizacije susreću prilikom sprovođenja propisa o privatnosti podataka?	9 radova	(Kabanov, 2016) (Labadie i Legner, 2023) (Sirur, *et al.*, 2018) (Jantti, 2020) (Layton i Elaluf-Calderwood, 2019) (Lonzetta i Hayajneh, 2021) (Li, *et al.*, 2019) (Miryala i Gupta, 2022) (Politou, *et al.*, 2018)	-Potrebno osigurati usklađenost na svim razinama poslovanja, -Nedostatak eksperata u oblasti sigurnosti kao i IT stručnjaka, -Problem razumijevanja nove uredbe, -Promjene dosadašnjeg načina skladištenja podataka, -Nedostatak resursa i smjernica prilikom usklađivanja, -Izvršiti unaprijeđenje postojećih informacionih sistema, -Veliki troškovi usklađivanja naročito za male i srednje kompanije, -Kontekst propisa nejasan, propisi opširno napisani -Promjena dosadašnjih praksi oglašavanja i procesa pohrane podataka, -Potrebe za kreiranjem sigurnosnih kopija itd.

Istraživačka pitanja	*Broj radova*	*Autori*	*Odgovori na pitanja*
Koja su prava građana i mjere zaštite njihovih podataka?	4 rada	(Presthus i Sorum, 2019) (Choi i Jerath, 2022) (Fox, *et al.*, 2022) (Van Ooijen i Vrabec, 2019)	-Zahvaljujući propisima o privatnosti podataka građani imaju pravo uvida u informacije koje se prikupljaju, obrađuju i pohranjuju, -Pravo na ispravljanje grešaka i zahtijevanje brisanja podataka, -Pravo kontrole prikupljanja, pohrane i korištenja njihovih podataka, -Kompanije moraju obavijestiti potrošače o svrsi i vrsti prikupljanja podataka, -Potrebno je dobiti saglasnost za korištenje podataka, -Povećanje kontrole, smanjenje rizika i izgradnja povjerenja
Kako se propisi o privatnosti podataka odnose na nove tehnologije i trendove?	4 rada	(Martin, *et al.*, 2019) (Yanamala i Suryadevara, 2023) (Al-Abdullah, *et al.*, 2020) (Degeling, *et al.*, 2018)	-Namenuto provođenje propisa može dovesti do toga da kompanije odustanu od sprovođenja inovacija, te da se usmjere na druge procese sa manje regulatornih ograničenja, -Potrebno je prilagoditi inovacije zakonskim propisima na način da kompanije koriste anonimne (šifrirane) podatke umjesto ličnih podataka, -Novi propisi imaju pozitivan efekat na transparentnost na web stranicama
Da li implementacija propisa o privatnosti podataka utiče na poslovne modele i propise kompanija?	2 rada	(Buckley, *et al.*, 2021) (Frey i Presidente, 2024)	-Implementacija propisa može uticati na povećanje ili smanjenje rizika ulaganja u nove proizvode i poslovne modele, -Utiče na povjerenje i potražnju potrošača, -Potreba za dodatnim zaposlenicima u administraciji, dodatne obuke zaposlenika, -Propisi su najviše dobiti donijeli kompanijama koje pružaju pravne ili tehnološke savjete i usluge povezane sa sprovođenjem propisa, -Propisi utiču na kompanije na dva načina: sa razvojem novih procesa stvaraju se dodatni troškovi i smanjuje profit, te propisi i politike privatnosti mogu uticati na smanjenje online kupovine, a samim tim i smanjenja ukupne prodaje.

Izvor: Kreacija autor

4. DISKUSIJA I ZAKLJUČAK

U okviru sistematskog pregleda literature o propisima o privatnosti podataka, kroz istraživačke radove su analizirane razne pravne regulative tj. propisi, međunarodni standardi kao i pristupi mnogih organizacija prilikom usklađivanja sa tim propisima, te mijenjanje sistema i načina poslovanja koji su do sada praktikovali.

U svojim radovima autori nastoje definisati izazove sa kojima se organizacije susreću prilikom usklađivanja sa propisima. Jedan od značajnijih izazova sa kojima se susreću jeste promjena trenutnog načina skladištenja i obrade podataka, te potreba za izmjenama dosadašnjeg načina poslovanja i softvera koji su bili u upotrebi. Mnoge organizacije su istakle da je kontekst novih propisa nejasan, da su opširno napisani i da ih je prvenstveno potrebno dešifrovati. Neophodno je uložiti dosta truda i resursa kako bi se razumjeli svi zakoni novih propisa. Također organizacije trebaju utvrditi da li se ovi propisi odnose na njih i u kojoj mjeri, za koja područja vrijede i šta je sve potrebno izmijeniti kako bi ih se pridržavali.

Zaštita ličnih podataka predstavlja osnovno pravo svakog korisnika. Konstantne tehnološke promjene i globalizacija omogućile su jednostavno dijeljenje podataka i informacija , često bez znanja vlasnika, te ove informacije postaju globalno dostupne drugim kompanijama.

Analiza literature i istraživačkih radova je pokazala da su Evropska unija i Sjedinjene Američke Države lideri u kreiranju i razvoju propisa o privatnosti podataka sa tačno utvrđenim zakonima poput Opšte uredbe o zaštiti podataka (GDPR) i Zakona o privatnosti potrošača u Kaliforniji (CCPA). Propisi Evropske unije se ističu kao najstrožiji zakoni o privatnosti, čiji je glavni fokus zaštita ličnih podataka i obezbjeđivanje korisnicima veće kontrole nad vlastitim podacima, kao i mogućnost zahtijevanja od organizacija da se njihovi podaci obrišu, te da im se detaljno predoči svrha u koju će se njihovi podaci koristiti i obrađivati. CCPA je također veoma značajan propis koji ima nešto drugačiji pristup u odnosu na GDPR i koji se više fokusira na podatke potrošača i na njihova prava.

Namjera GDPR-a jeste doprinijeti postizanju slobode, sigurnosti, pravde, ekonomskog i socijalnog napretka unutar Evropske unije. GDPR se primjenjuje na bilo koju kompaniju, bez obzira na njenu lokaciju, a koja se bavi prikupljanjem i obradom podataka rezidenata EU. Glavna briga u današnjem digitalnom dobu jeste kako zaštititi podatke potrošača. Digitalne tehnologije i internet omogućili su organizacijama prikupljanje, prenos i upotrebu podataka o potrošačima u različite svrhe poput ciljanog oglašavanja i dizajniranja proizvoda u skladu sa preferencijama potrošača što je donijelo nove prihode kompanijama.

S druge strane sve ovo se može negativno odraziti na potrošače zbog prikupljanja i upotrebe njihovih podataka od strane organizacija, prvenstveno zbog gubitka privatnosti, neželjenog oglašavanja i sigurnosnih prevara.

S obzirom na to da potražnja potrošača za proizvodom neke kompanije zavisi i od toga kako kompanija tretira njihove lične podatke, veoma je važno da one konstantno ulažu u sisteme koji će obezbijediti sigurnost podataka, te da traže saglasnost potrošača za njihovo prikupljanje i korištenje.

Važnost razumijevanja brige potrošača o privatnosti njihovih podatka, te kreiranje načina na koji bi ublažili tu zabrinutost bi trebala biti veoma važna stavka svake organizacije. Većina organizacija svako uvođenje nekih novina i usklađivanja sa novim propisima doživljava kao trošak, međutim uvođenje novih propisa ne bi trebalo posmatrati kao neki problem ili prepreku, već kao novu priliku da unaprijede svoje poslovanje i poboljšaju utisak klijenata o kompaniji. Novi propisi zahtijevaju od organizacija da dobiju potvrdnu saglasnost za korištenje podataka, kao i da obavijeste potrošače o vrsti podataka koje će prikupljati i svrsi njihovog prikupljanja. Zapravo ovi propisi pomažu potrošačima da kontrolišu dijeljenje njihovih podataka, te da povuku odobrenje za njihovo korištenje u narednom periodu ukoliko to žele.

Jedan od problema sa kojima se potrošači susreću jeste to što su uslovi za prihvatanje i obavijesti često prilično duge i nerazumljive, jer sadrže zakonske uvjete koji nisu razumljivi prosječnom korisniku. Jedno od mogućih rješenja za ovaj izazov jeste pojednostavniti i što je moguće više skratiti obavijest kako bi korisnici lakše razumjeli zakonske uvjete i svrhu korištenja njihovih podataka.

Kompanije sve više koriste lične podatke kako bi pratile želje i potrebe određene ciljne grupe i na osnovu toga poboljšali svoje proizvode i kreirali nove poslovne modele. Većina često navodi da ih ovi stogi propisi stavljaju u nepovoljan položaj u odnosu na njihovu konkurenciju tj. kompanije koje se nalaze u zemljama sa blažom zakonskom regulativom, dok druge ističu da su strožiji propisi neophodni kako bi se vratilo povjerenje u digitalnu ekonomiju.

Provođenje novih propisa može utjecati na poslovanje organizacija i dovesti do toga da one odustanu od uvođenja inovacija zbog velikih troškova koje imaju prilikom usklađivanja i mijenjanja dosadašnjih procesa, te poslovanje usmjeriti na neke druge procese sa manje regulatornih ograničenja.

U današnjem dobu u kojem je zaštita i privatnost podataka sve važnija, GDPR je prisilio organizacije da poštuju privatnost svojih klijenata i da koriste njihove podatke samo uz odobrenje i na način na koji oni to žele. Također, uvođenje GDPR-a je natjeralo kompanije da poboljšaju svoje poslovne procese i da unaprijede upravljanje i obradu podataka. Ukoliko se kompanije odluče za to da se ne pridržavaju datih propisa, morat će se suočiti sa velikim kaznama koje ovi zakoni donose.

Aseri (2020) navode da je očuvanje privatnosti podataka podjednako važna kako za korisnike tako i za kompanije. Neprikladno ponašanje, nedozvoljeno dijeljenje kao i zlonamjerna upotreba podataka od strane kompanija koje svoje proizvode i usluge nude

putem interneta često dovode do povrede podataka i privatnosti korisnika, koji gube povjerenje u samu kompaniju, a samim tim utiču i na poslovanje kompanije (Alessi, et al., 2019).

Usklađenost organizacija sa propisima o privatnosti podataka je veoma važna kako bi se osigurala konkurentska prednost i sudjelovanje na tržištu (Aseri, 2020). Organizacije koriste prikupljene podatke u cilju boljeg razumijevanja potrošača, prepoznavanja njihovih preferencija i iskustava o proizvodima i uslugama koje oni nude (Ghorashi, et al., 2023). Pojedinci koji svjesno dijele lične podatke, ispunjavanjem ličnih i finansijskih podataka prilikom kupovine trebaju imati povjerenje u organizacije, da su njihovi podaci sigurni i da neće biti iskorišteni na njihovu štetu (Bauer, et al., 2022).

Jantti (2020) kao izazove prilikom sprovođenja propisa navodi potrebu za većim ulaganjem u komunikaciju i informisanje korisnika, zatim potrebno je izvršiti pažljivu pripremu i uložiti više sredstava za pripremu naročito u malim i srednjim preduzećima sa ograničenim resursima, potaknuti korisnike da se više brinu o sigurnosti i zaštiti vlastitih podataka. Pored navedenog, nedostatak obuke i potrebne edukacije predstavljaju izazov za kompanije prilikom usklađivanja sa propisima poput GDPR-a.

Lonzetta i Hayajneh (2021) u svom istraživanju ističu da je kontekst propisa nejasan, da su propisi opširno napisani, te da je prije svega potrebno utvrditi da li se propisi odnose na njihove kompanije i za koja područja ih je potrebno primjenjivati, zatim potrebno je dosta vremena kako bi se implementirali novi sistemi i prilagodili poslovanju.

Kompanije moraju izvršiti promjene dosadašnjih praksi oglašavanja i pohrane podataka. Problemi se javljaju i kod inostranih kompanija, jer pored propisa koje nalaže zemlja u kojoj se nalaze moraju ispoštovati i propise zemlje u kojoj pružaju svoje proizvode ili usluge (Li, et al., 2019).

Prije same obrade podataka korisnika potrebno je dobiti odobrenje od korisnika, ali prije toga potrebno je izvršiti izmjene i dopune aktuelnih obavještenja za dobivanje saglasnosti, jer su uslovi za njihovo dobivanje postali znatno strožiji (Politou, et al., 2018).

Miryala i Gupta (2022) kao izazove navode potrebu kompanija za kreiranjem sigurnosnih kopija, obezbjeđivanje obuka zaposlenika kako bi mogli ispoštovati sva pravila koje novi propisi nalažu, te kreiranje novih sistema kako bi se na vrijeme otkrile prijetnje, a sve sa ciljem kako bi se spriječili eventualni napadi, te kako bi se minimizirali njihovi uticaji na poslovanje kompanije i na njihove korisnike.

Korisnici obraćaju malo ili nimalo pažnje na prava koja im propisi o privatnosti omogućavaju, jer zahvaljujući njima korisnici imaju pravo uvida u informacije koje se prikupljaju, obrađuju i pohranjuju, te mogućnost ispravljanja grešaka i zahtijevanje njihovog brisanja. Također imaju pravo da kontrolišu u koje svrhe se koriste njihovi podaci, te da li se i na koji način dijele sa drugima (Presthus i Sorum, 2019).

Choi i Jerath (2022) navode da propisi o privatnosti podataka pomažu potrošačima prilikom sprječavanja dijeljenja njihovih podataka, ukoliko bi to dijeljenje moglo narušiti njihovu privatnost.

Kao mjere zaštite prava i privatnosti korisnika Fox *et al.* (2022) navode povećenje kontrole prilikom dijeljenja i obrade podataka, izgradnja povjerenja kod korisnika, te pružanje informacija potrošačima o praksama i politikama privatnosti organizacije, kao i eventualnim izmjenama koje se dešavaju.

Prema propisima koje nalaže GDPR vlasnik podataka mora biti informisan prije nego što se izvrši obrada njihovih podataka, o namjeri prikupljanja podataka i roku čuvanja podataka. U slučaju da obrada podataka ne bude u skladu sa zakonom, vlasnici podataka imaju pravo da traže od kompanije da se njihovi podaci izbrišu (Van Ooijen i Vrabec, 2019).

Kompanije sve više iskorištavaju lične podatke kako bi poboljšali svoje proizvode, te kreirali nove poslovne modele. Novi propisi mogu doprinijeti tome da kompanije odustanu od uvođenja inovacija jer se ne mogu prilagoditi propisima, pa svoje poslovanje preusmjeravaju na druge procese koji nemaju striktna ograničenja (Martin, et al., 2019).

Buckley *et al.* (2021) navode da implementacija propisa sa sobom donosi troškove, kao i potrebu za tehničkim i organizacijskim ulaganjem kako bi se omogućilo prenošenje podataka, ispravak kao i procesi brisanja. Potrebno je izvršiti revizije postojećih sistema i poslovnih modela kako bi se izvršilo usklađivanje sa GDPR-om. Ovi propisi najviše dobiti donose kompanijama koje se bave pružanjem pravnih ili tehnoloških savjeta i usluga koje su povezane sa sprovođenjem GDPR-a.

REFERENCE

1. Al-Abdullah, M., Alsmadi, I., AlAbdullah, R. & Farkas, B., 2020. Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. *Digital Policy, Regulation and Governance,* pp. 389-411.

2. Albahar, M. & Thanoon, M., 2022. Privacy Regulations in the Middle East: Challenges & Solutions. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies.*

3. Alessi, M. et al., 2019. A decentralized personal data store based on ethereum: Towards GDPR compliance. *Journal of Communications Software and Systems,* pp. 79-88.

4. Alves, P. H. et al., 2020. Permissioned blockchains: Towards privacy management and data regulation compliance. *In Legal Knowledge and Information Systems,* pp. 211-214.

5. Aseri, A. M., 2020. The implication of the European union's general data protection regulation (GDPR) on the global data privacy. *Journal of Theoretical and Applied Information Tehnology.*

6. Atlan, 2023. *Data privacy vs. Data Security: Definitions and Differences.*
Dostupno na: https://atlan.com/data-privacy-vs-data-security/
(Pristupljeno: 10. august 2024).

7. Baig, A., 2023. *7 Best Practices for Data Collection in 2023.*
Dostupno na: https://www.dataversity.net/7-best-practices-for-data-collection-in-2023/
(Pristupljeno: 10. august 2024).

8. Bauer, P. et al., 2022. Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. *Information, Communication & Society,* pp. 2101-2121.

9. Bertino, E. & Ferrari, E., 2017. Big data security and privacy. *In A comprehensive guide through the Italian database research over the last 25 years,* pp. 425-439.

10. Blakeley, C. J. & Matsuura, J. H., 2013. *Tips for protecting your organization's data.*
Dostupno na: https://store.legal.thomsonreuters.com/law-products/news-views/corporate-counsel/tips-for-protecting-your-organizations-data
(Pristupljeno: 10. august 2024).

11. Blesch, W., 2024. *Data Security vs Data Privacy.*
Dostupno na: https://www.termsfeed.com/blog/data-security-vs-privacy/
(Pristupljeno: 10. august 2024).

12. Blind, K., 2012. The influence of regulations on innovation: A quantitative assessment for OECD countries. *Research policy,* pp. 391-400.

13. Buckley, G., Caulfield, T. & Becker, I., 2021. " It may be a pain in the backside but..."Insights into the impact of GDPR on business after three years.".

14. BuiltIn, 2023. *Data Privacy: What You Need to Know.*
Dostupno na: https://builtin.com/articles/data-privacy
(Pristupljeno 3. decembar 2024).

15. California Attorney General's Office , 2024. *California Consumer Privacy Act (CCPA).* Dostupno na: https://oag.ca.gov/privacy/ccpa
(Pristupljeno: 23. august 2024).

16. ChinaBriefing, 2021. *The PRC Personal Information Protection Law (Final): A Full Translation.*
Dostupno na: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/
(Pristupljeno: 3. decembar 2024).

17. Choi, W. J. & Jerath, K., 2022. Privacy and consumer empowerment in online advertising. *Foundations and Trends in Marketing,* pp. 153-212.

18. Chojnowska, M., 2023. *Data Privacy and Security - Protecting Sensitive Data in a Data-Driven Organization.*
Dostupno na: https://sunscrapers.com/blog/data-privacy-and-security-protecting-sensitive-data-in-a-data-driven-organization/
(Pristupljeno 13. augsut 2024).

19. Cloudian, 2024. *Data protection and privacy: 7 ways to protect user data.*
Dostupno na: https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
(Pristupljeno: 3. decembar 2024).

20. Consentmo, 2024. *What is LGPD?.*
Dostupno na: https://www.consentmo.com/compliance/lgpd-compliance
(Pristupljeno: 3. decembar 2024).

21. Crutzen, R., Ygram Peters, G. J. & Mondschein, C., 2019. Why and how we should care about the General Data Protection Regulation. *Psychology & Health,* pp. 1347-1357.

22. DataGuard, 2024. *What is data protection and why is it important?.*
Dostupno na: https://www.dataguard.co.uk/blog/what-is-data-protection-and-why-is-it-important/
(Pristupljeno: 3. decembar 2024).

23. Dataversity, 2024. *Data Privacy vs. Data Security.*
Dostupno na: https://www.dataversity.net/data-privacy-vs-data-security/
(Pristupljeno: 3. decembar 2024).

24. Degeling, M. et al., 2018. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy.

25. Emeritus, 2022. *What is Data Collection? Why is it Important for Your Business?.*
Dostupno na: https://emeritus.org/blog/data-analytics-what-data-collection/
(Pristupljeno: 26. august 2024).

26. Fox, G., Lynn, T. & Rosati, P., 2022. Enhancing consumer perceptions of privacy and trust: a GDPR label perspective. *Information Tehnology & People,* pp. 181-204.

27. Frey, C. B. & Presidente, G., 2024. Privacy regulation and firm performance: Estimating the GDPR effect globally. *Economic Inquiry.*

28. GDPR, 2020. *What is GDPR, the EU's new data protection law?.*
Dostupno na: https://gdpr.eu/what-is-gdpr/
(Pristupljeno: 3. decembar 2024).

29. Ghorashi, S. R., Zia, T., Bewong, M. & Jiang, Y., 2023. An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing. *Applied Sciences.*

30. Hoofnagle, C. J., Van Der Sloot, B. & Borgesius, F. Z., 2019. The European Union general data protection regulation: what it is and what it means. *Information & Communications Tehnology Law,* pp. 65-98.

31. Imperva, 2024. What is data protection ? Dostupno na: https://www.imperva.com/learn/data-security/data-protection/.
(Pristupljeno: 3. decembar 2024).

32. Jain, P., Gyanchandani, M. & Khare, N., 2016. Big data privacy: a tehnological perspective and review. *Journal of Big Data*, pp. 1-25.

33. Jantti, M., 2020. Studying Data Privacy Management in Small and Medium-Sized IT Companies. *In 2020 14th International Conference on Innovations in Information Tehnology*, pp. 57-62.

34. Kabanov, I., 2016. Effective frameworks for delivering compliance with personal data privacy regulatory requirements. *In 2016 14th Annual Conference on Privacy, Security and Trust*, pp. 551-554.

35. Labadie, C. & Legner, C., 2023. Building data management capabilities to address data protection regulations: Learning from EU-GDPR. *Journal of Information Tehnology,* pp. 16-44.

36. Lame, G., 2019. Systematic literature reviews: An introduction. *Proceedings of the design society: international conference on engineering design*, pp. 1633-1642.

37. Layton, R. & Elaluf-Calderwood, S., 2019. A social economic analysis of the impact of GDPR on security and privacy practices. *In 2019 12th CMI Conference on Cybersecurit and Privacy (CMI),* pp. 1-6.

38. Li, H., Yu, L. & He, W., 2019. The impact of GDPR on global tehnology development. *Journal of Global Information Tehnology Management*, pp. 1-6.

39. Lonzetta, A. M. & Hayajneh, T., 2021. Challenges of Complying with Data Protection and Privacy Regulation. *EAI Endorsed Transactions on Scalable Information Systems.*

40. Martin, N., Matt, C., Niebel , C. & Blind, K., 2019. How data protection regulation affects startup innovation. *Information systems frontiers,* pp. 1307-1324.

41. Miryala, N. K. & Gupta, D., 2022. Data Security Challenges and Industry Trends. *IJARCCE International Journal of Advanced Research in Computer nd Communication Engineering,* pp. 300-309.

42. Netwrix, 2023. *International data privacy laws: A Guide.*
Dostupno na: https://blog.netwrix.com/2023/09/18/international-data-privacy-laws/
(Pristupljeno: 3. decembar 2024).

43. Pantelic, O., Jovic, K. & Krstovic, S., 2022. Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations. *Sustainability.*

44. Paul, J. et al., 2021. Scientific procedures and relationes for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies.*

45. Politou, E., Alepis, E. & Patsakis, C., 2018. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity.*

46. Presthus , W. & Sorum, H., 2019. Consumer perspectives on information privacy following the implementation of the GDPR.

47. Romansky, R. P. & Noninska, I. S., 2020. Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering,* pp. 5288-5303.

48. Rother, E. T., 2007. Systematic Literature review X narrative review. *Acta paulista de enfermagem.*

49. Sanchez, M., 2022. A general approach on privacy and its implications in the digital economy. *Journal Of Economic Issues,* pp. 244-258.

50. Sirur, S., Nurse , J. R. & Webb, H., 2018. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). *In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security,* pp. 88-95.

51. Spichtinger, D., 2024. *New data protection and privacy laws have changed the regulatory landscape for researchers in the Global North.*
Dostupno na: https://blogs.lse.ac.uk/impactofsocialsciences/2024/04/15/new-data-protection-and-privacy-laws-have-changed-the-regulatory-landscape-for-researchers-in-the-global-north/
(Pristupljeno: 26. august 2024).

52. Thomson Reuters, 2024. *Understanding California Consumer Privacy Act.*
Dostupno na: https://legal.thomsonreuters.com/en/insights/articles/understanding-california-consumer-privacy-act
(Pristupljeno:23. august 2024).

53. Tikkinen-Piri, C., Rohunen, A. & Markkula, J., 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review,* pp. 134-153.

54. TitanFile, 2023. *Top 5 Methods of Protecting Data.*
Dostupno na: https://www.titanfile.com/blog/5-methods-of-protecting-data/
(Pristupljeno 13. august 2024).

55. Trendmicro, 2024. *EU General Data Protection Regulation (GDPR).*
Dostupno na: https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr
(Pristupljeno: 3. decembar 2024).

56. Usercentrics, 2023. *Switzerland's Federal Act on Data Protection (FADP).*
Dostupno na: https://usercentrics.com/knowledge-hub/switzerland-federal-data-protection-act-fadp/
(Pristupljeno: 3. decembar 2024).

57. Usercentrics, 2024. *Brazil LGPD: General Data Protection Law Overview.*
Dostupno na: https://usercentrics.com/knowledge-hub/brazil-lgpd-general-data-protection-lawverview/#:~:text=The%20LGPD%2C%20or%20Lei%20Geral,personal%20data%20and%20provide%20transparency.
(Pristupljeno: 23. august 2024).

58. Van Ooijen, I. & Vrabec, H. U., 2019. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy*, pp. 91-107.

59. Wang, L. et al., 2019. Data capsule: A new paradigm for automatic compliance with data privacy regulations. *Springer International Publishing.*

60. Wolford, B., 2020. *What is GDPR, the EU's new data protection law.*
Dostupno na: https://gdpr.eu/what-is-gdpr/
(Pristupljeno:17. august 2024).

61. Yanamala, A. K. Y. & Suryadevara, S., 2023. Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Tehnologies and Innovations,* pp. 294-319.

62. Zaeem, R. N. & Barber , K. S., 2020. The effect of the GDPR on privacy policies: Recent progress and future promise. *" ACM Transactions on Management Information Systems (TMIS),* pp. 1-20.