https://doi.org/10.38190/ope.11.1.6 *Prethodno priopćenje / Preliminary communication*

OKVIR ZA UVOĐENJE I PROVJERU GDPR-a U MALIM I SREDNJE VELIKIM PODUZEĆIMA

mr. sc. **Sanja Penić**, v. pred.
Rapska 26/1, Zagreb, Hrvatska
Telefon: 098 326 301, E-mail: sanja.penic@digbiz.hr

mr. sc. **Kristian Saletović**, v. pred.
Miroševečki brijeg 33, Zagreb, Hrvatska
Telefon: 099 3657 538, E-mail: kristian.saletovic@gmail.com

SAŽETAK

Opća uredba o zaštiti osobnih podataka (Uredba (EU) 2016/697 poznata kao GDPR) počela se primjenjivati u svibnju 2018. godine te je imala znatan utjecaj na organizaciju poslovnih procesa u poduzećima. Posebno su to osjetila mala i srednje velika poduzeća za koje GDPR predstavlja dodatno opterećenje zbog ionako ograničenih resursa. Okvir za implementaciju i reviziju prethodno implementiranih zahtjeva definiranih GDPR-om predstavljen u ovom radu rezultat je informacija iz znanstvene literature i spoznaja dobivenih revizijom već implementirane Uredbe u dva mala poduzeća. Cilj je ovog rada je doprinijeti razumijevanju poteškoća s kojim se suočavaju mala i srednje velika poduzeća pri implementaciji GDPR-a. U radu je korištena studije slučaja. Dobiveni rezultati pokazali su da, iako je prošlo već dvije godine od prve implementacije, još postoji nerazumijevanje terminologije i obaveza u smislu svakodnevne primjene.

***Ključne riječi**: osobni podaci; mala i srednje velika poduzeća; GDPR; procesi; sigurnost*

1. UVOD

Prema službenoj web stranici Eurostata, mala i srednje velika poduzeća (eng. *Small and Medium-sized Enterprises - SME*) predstavljaju velik dio europske ekonomije te su velik potencijalni izvor poslova i potencijala za rast. Istraživanja su pokazala da mala i srednje velika poduzeća ne samo u Europi nego i u većini svjetskih ekonomija predstavljaju važan i dinamičan segment (Tarutėa, Gatautis, 2013). U europskom statističkom izvještaju za 2015. godinu (Eurostat - Statistics on small and medium-sized enterprises, 2015) mala i srednje velika poduzeća predstavljala su 99% ekonomije u Europi. Zapošljavaju gotovo dvije trećine od ukupno zaposlenih u EU te pridonose s 56% od ukupnog prometa (Eurostat - Basic structure: employment size class breakdown in Structural Business Statistics, 2015). U RH je, prema izvještaju za 2017. (CEPOR - Izvješće o malim i srednje velikim poduzećima u Hrvatskoj, 2018.), udio malih i srednje velikih poduzeća u ekonomiji 99,7%, "zapošljavaju gotovo tri četvrtine (73,2%) svih zaposlenih u poslovnim subjektima u Hrvatskoj u 2017. godini", a udio u ukupnom prihodu ostvarenom na razini Hrvatske iznosio je 59,6%.

Iz tih podataka jasno je da mala i srednje velika poduzeća imaju veliku ulogu u ekonomiji zemlje, no treba imati na umu da su to organizacije s ograničenim resursima, prvenstveno ljudskim i financijskim. U istraživanju o četvrtoj industrijskoj revoluciji (Matt, 2020) zaključeno je da ona obuhvaća individualizaciju korisničkih zahtjeva, a time i prikupljanje osobnih podataka, što posljedično obvezuje poduzeća na primjenu Opće uredbe o zaštiti osobnih podatka (dalje u tekstu koristit će se dobro poznata kratica GDPR prema engleskom nazivu *General Data Protection Regulation* – Uredba (EU) 2016/697 Europskog parlamenta).

Preduvjet za učinkovitu implementaciju GDPR-a je i visoka razina usvajanja informacijske i komunikacijske tehnologije (IKT) te ovladavanje vještinama potrebnim za njihovo korištenje. Usvajanje IKT-a u RH, prema izvještaju DZS-a (2019), na visokoj je razini: "Visok stupanj integracije IKT-a u poslovanju; 98% poduzeća upotrebljava računala, 98% poduzeća ima pristup internetu, a 69% poduzeća ima vlastitu internetsku stranicu." Visok stupanj digitalizacije poslovanja, a samim time i količina prikupljenih osobnih podataka, znači da i velik broj malih i srednje velikih poduzeća obvezuje primjena GDPR-a.

Rad je strukturiran tako da se u prvom poglavlju donose osnovne informacije o značenju malih i srednje velikih poduzeća, u drugom poglavlju napravit će se pregled dosadašnjih dostupnih spoznaja o implementaciji GDPR-a u mala i srednje velika poduzeća, a u idućim poglavljima bit će dan prijedlog okvira s empirijskim spoznajama o implementaciji u dva mala poduzeća. Rad je pisan u domeni kvalitativnih istraživanja te je primijenjena metoda studije slučaja. Izvori podataka za studije slučaja su otvoreni intervjui sa vlasnicama malih poduzeća, službeni dokumenti u poduzećima te dokumentacija vezana za Opću uredbu o zaštiti podataka (GDPR).

2. SPOZNAJE O IMPLEMENTACIJI GDPR-a U MALIM I SREDNJE VELIKIM PODUZEĆIMA

Prema provedenim istraživanjima (Freitas, 2019; Gilieron, 2018), mala i srednje velika poduzeća dočekala su nespremna uvođenje GDPR-a, tj. neki od njih nisu ni čuli za tu uredbu. Razumijevanje GDPR-a tada je bilo na iznimno niskoj razini. Uz nedostatak vještina i iskustava u upravljanju rizicima u poslovanju, pred mala i srednje velika poduzeća stavljeni su veliki izazovi - tumačenja i provođenja GDPR-a. Nedostatak iskustva u upravljanju rizicima poslovanja dodatno otežava i nerazumijevanje načina zaštite osobnih podataka. Uza sve već navedeno, dodatno ograničenje predstavljaju financijski i ljudski resursi koji stoje na raspolaganju malim i srednje velikim poduzećima.

Prema Ficheru (Fischer, 2020, 11), identificiran je osnovni problem implementacije GDPR-a, a to je činjenica da nije bilo službenih smjernica koje bi mala i srednje velika poduzeća mogla koristiti prilikom implementacije. Do tada dostupni materijali omogućili su općenito poznavanje GDPR-a, ali za razumijevanje je ipak potrebno dublje poznavanje novog pravnog okvira. Može se reći da je problem u tome što je zakonski okvir definiran, ali ne postoje službene smjernice zakonodavca kojima bi se omogućila implementacija regulatornog okvira u mala i srednje velika poduzeća. S obzirom na ograničene resurse, nepostojanje smjernica za implementaciju predstavlja veliku prepreku malim i srednje velikim poduzećima. Međutim, nedostatak standardiziranih uputa za implementaciju ne znači da ne postoje pokušaji da se one kreiraju. Prema dostupnim informacijama (Fischer, 2020, 12), u primjeni je nekoliko okvira koji pokušavaju standardizirati implementaciju:

- *Framework for Demonstrable GDPR Compliance A mapping of the Nymity's Privacy Management Accountability Framework to GDPR Compliance Obligations*
- *APSs GDPR FRAMEWORK*
- *IBMs GDPR framework*
- *Copenhagen Compliance framework*
- *Information commission offices framework.*

Nekoliko autora opisalo je implementaciju u mala i srednje velika poduzeća, a Fischer (2020) opisuje implementaciju *Nymity's Privacy Management Accountability Framework* u poduzeće koje nudi e-commerce platformu, a ima 37 zaposlenika i 3 milijuna eura prometa. Autor zaključuje da odabrani okvir obuhvaća najviše komponenti GDPR-a te je, empirijskom provjerom i uz manje modifikacije, uspješno implementiran u odabrano poduzeće.

Brodin (2019) u svom radu naglašava da GDPR ima vrlo rigorozne zahtjeve u obradi osobnih podataka koji mogu biti zahtjevni za mala i srednje velika poduzeća te je potrebna prilagodba, zbog čega predlaže okvir koji je ujedno testiran na nekoliko malih i srednje velikih poduzeća. Prema rezultatima zaključuje se da je predloženi implementacijski okvir efikasan te se predlaže daljnja razrada i nastavak testiranja.

U svom radu u kojem se opisuje implementacija GDPR-a u segmentu knjigovodstva malog poduzeća Šiškova i Lorinzova (2020) ističu fizičku i tehničku zaštitu kao najveće prepreke pri implementaciji zaštite osobnih podataka ponajviše zbog znatnog povećanja troškova.

Prema istraživanju provedenom u RH za potrebe diplomskog rada Stepan (2019) potvr-

đuje se nedovoljna informiranost o samoj Uredbi te se donosi zaključak kako je potrebno uložiti dodatne napore u edukacije kojima bi se podigla svijest o zaštiti osobnih podataka.

3. OKVIR ZA MALA PODUZEĆA

Za potrebe ovog rada analiziran je okvir za usklađivanje malih i srednje velikih poduzeća s GDPR-om koji je predložio Brodin (2019) u svom radu *A framework for GDPR Compliance for Small and Medium-Sized Enterprises*.

Usklađivanje s GDPR-om predstavlja velik izazov za sve vrste poduzeća (mala, srednja i velika) jer ih dodatno obvezuje na zaštitu osobnih podataka te zahtijeva od njih određene prilagodbe u odnosu na uobičajen način rada, što podrazumijeva razne logičke, tehnološke i funkcionalne promjene koje utječu na uobičajenu dnevnu rutinu poslovnih aktivnosti. Izazovi s kojima se susreću mala i srednje velika poduzeća uglavnom su vezani uz raspoloživost znanja u poduzeću te financijskih i ljudskih resursa koji se mogu posvetiti temi zaštite osobnih podataka. S obzirom na to da je novom regulativom napravljen određeni transfer odgovornosti o zaštiti osobnih podataka s državnih tijela na tvrtke te su propisane visoke kazne, one su obavezne u svakom trenutku moći dokazati svoju usklađenost s regulativom (Freitas, 2018; Kapoor, 2018).

U svom istraživanju Kapoor, Renaud i Archibald ističu kako je sektor malih i srednje velikih poduzeća u većini slučajeva izvršitelj obrade osobnih podataka te naglašavaju potrebu za uspostavom metodologije za usklađivanje malih i srednje velikih poduzeća s GDPR-om (Kapoor i sur., 2018). Jedan od okvira za usklađivanje predložio je u svom radu Brodin (2019).

U ovom radu provest će se analiza predloženog okvira za usklađivanje malih i srednje velikih tvrtki s GDPR-om autora Brodin (2019) na dva mala poduzeća u Hrvatskoj. Također, predložit će se upitnik za početnu analizu, a s ciljem doprinosa u nadogradnji predloženog okvira kako bi se povećala primjenjivost i efikasnost prilikom usklađivanja malih poduzeća.

3.1. Analiza predloženog okvira za mala i srednje velika poduzeća

Brodin, M. (2018) predložio je okvir za usklađivanje malih i srednje velikih poduzeća s GDPR-om. Okvir je prošao teorijsku evaluaciju, a empirijski je testiran u tri različita poduzeća u Švedskoj. Rezultat empirijskog dijela (usklađenost s GDPR-om) evaluirali su i odobrili stručnjaci u poduzećima i visoki menadžment. Autor predloženog okvira zaključuje da mala i srednje velika poduzeća često ne raspolažu s dovoljno znanja i ljudskih resursa kako bi se sama mogla uskladiti s GDPR-om. Do istih zaključaka došli su Schulze (2018), Lindqvist (2018) i Sirur (2018). Rezultati empirijskog testiranja pokazuju da predloženi okvir, uz male troškove, može znatno pomoći malim i srednje velikim poduzećima pri postupku njihova usklađivanja. Autor sugerira da je poželjno dodatno testirati predloženi okvir, što će se i provesti na dva mala poduzeća u kojima će se testirati njegova primjenjivost na malim poduzećima.

Nakon svakog projekta usklađivanja poduzeća sa zahtjevima propisanim u GDPR-u pravi test usklađenosti je zapravo audit koji provodi regulator (u Hrvatskoj je to Agencija za zaštitu osobnih podataka (AZOP)). U budućnosti bi bilo vrlo zanimljivo provjeriti stanje

usklađenosti u poduzećima te usporediti rezultate prije i nakon posjeta regulatora.

Predloženi okvir sastoji se od tri faze – analiza, dizajn i implementacija.

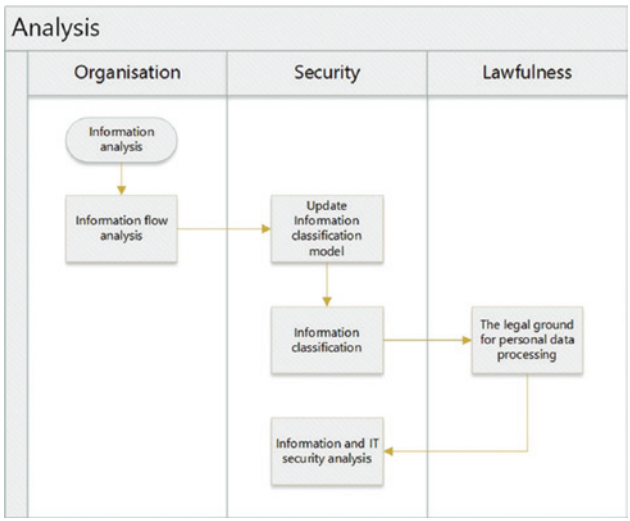
3.2. Faza analize

Predloženi okvir započinje analizom kako bi se utvrdilo trenutačno stanje u poduzeću u smislu upravljanja informacijama te njihovoj zaštiti. Prvenstveno se pod informacijama ovdje misli na osobne podatke, što se u početnoj fazi precizno definira. Početna analiza provodi se na jednoj ili više radionica u kojima sudionici definiraju osobne podatke i situacije u kojima poslovni proces dolazi u doticaj s njima. Zatim se definiraju lokacije tih osobnih podataka (baze podataka, razni poslovni programi, mape u ormarima, arhiva i sl.), a analiziraju se i obrade osobnih podataka koje se zbivaju u suradnji s vanjskim suradnicima (podizvršitelji obrade).

Prema članku 30. GDPR-a, mala poduzeća nisu obavezna voditi zbirke obrade osobnih podataka, ali to je korisno imati evidentirano pa se svakako preporučuje barem jednostavna tablica s osnovnim podacima.

U sljedećem koraku potrebno je utvrditi i razumjeti kretanje osobnih podataka unutar organizacije, njezinih poslovnih procesa i informacijskog sustava. Zatim treba razumjeti razloge obrade osobnih podataka kako bi se utvrdila pravna osnova (zakonski uvjetovana obrada, ugovorna osnova za obradu i sl.). Na kraju faze analize prikupljeni se podaci klasificiraju te se definiraju načini zaštite osobnih podataka (IT sustavi, fizička zaštita i sl.).

Slika 1: aktivnosti u fazi analize



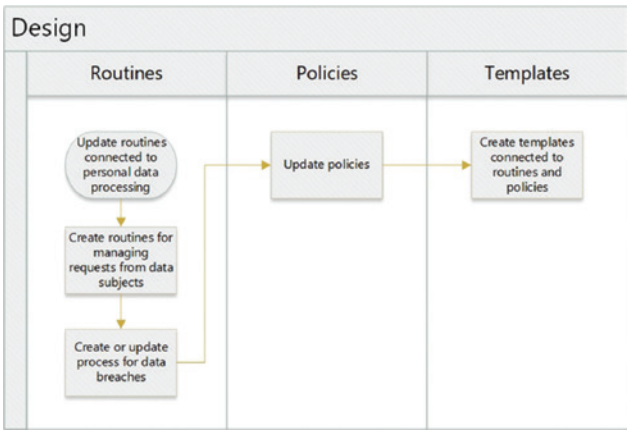
Izvor: Brodin, 2018.

3.3. Faza dizajna

Faza dizajna usmjerena je na procedure (*routines*), politike (*policies*) i predloške (*templates*). Procedure koje su direktno vezane uz GDPR kreiraju se tako da se bave pravima ispitanika (pravo na pristup osobnim podacima, pravo na brisanje itd.) i obvezama voditelja obrade (kako se provodi procjena učinka na zaštitu podataka, koraci koji se poduzimaju u slučaju gubitka osobnih podataka i sl.). Procedure su namijenjene svakodnevnoj upotrebi te se kreiraju i predlošci koji su vezani uz njih.

U sljedećim koracima treba ažurirati ili po potrebi kreirati krovni dokument (npr. politika ili pravilnik zaštite osobnih podataka) koji načelno opisuje postupanje s osobnim podacima, upotrebu i pohranjivanje osobnih podataka, prava ispitanika, pohranu te brisanje podataka.

Slika 2: aktivnosti u fazi dizajna



Izvor: Brodin, 2018

3.4. Faza implementacije

Prilikom implementacije u poduzećima fokus je na:

a) Uvođenju novih procedura i kreiranju sustava za izvještavanje o incidentima, čime se stvaraju uvjeti za trajnu usklađenost s regulativom.

b) Upoznavanju zaposlenika s njihovim novim ulogama i uvjetima u kojima obavljaju posao.

c) Pročišćavanju postojeće obrade osobnih podataka tako da se obrišu suvišni osobni podaci i uklone sve obrade osobnih podataka koje nisu u skladu s regulativom.

Prilikom implementacije novih procedura, politika i predložaka potrebno je to izvesti tako da se stvori sustav koji može dulje funkcionirati na taj način. U svemu tome iznimno je važna komunikacija kako bi svi zaposlenici bili upoznati s uvedenim novinama, ali i promjenama koje će se posebno zbivati tijekom adaptacije poduzeća.

Edukacija zaposlenika je iznimno važan dio zahtjeva GDPR-a pa poduzeća trebaju razviti

svojevrstan edukacijski program za zaposlenike (školovanje, prezentacija, e-learning i sl.) koji će se provoditi inicijalno pri zapošljavanju, ali i periodički (npr. godišnje).

3.5. Upitnik za početnu analizu

Predložena faza predanalize podrazumijeva upotrebu početnog upitnika kako bi se prikupile osnovne informacije vezane uz zaštitu osobnih podataka, a poslužit će kao polazna točka za fazu detaljnije analize u obliku radionica koje slijede u fazama kako je Brodin (2019) predložio u svom okviru za analizu malih i srednje velikih poduzeća (faze analize, dizajna i implementacije). Na taj se način prilagodio postupak malim poduzećima kako bi se brže i efikasnije provela analiza jer u većini slučajeva mala poduzeća raspolažu s vrlo ograničenim ljudskim resursima i znanjem koje se može primijeniti na temu zaštite osobnih podataka.

Upitnik je kreiran na osnovi stručnog znanja i iskustava autora te sličnih upitnika koje su predložili britanski regulator (ICO – *Information Commissioner's Office*; samoprocjena za mala poduzeća), irski regulatori (DPC – *Data Protection Commission*; lista za samoprocjenu) te nekoliko poduzeća koja su kreirala svoje upitnike uz pomoć drugih nacionalnih regulatora.

Tablica 1: Upitnik u fazi predanalize kojim se prikupljaju osnovne informacije vezane uz zaštitu osobnih podataka u malim poduzećima.

Rb	Pitanje	Da	Ne	Djelomično
1	Znate li koje osobne podatke posjedujete i za što ih koristite? Npr. osobni podaci vaših zaposlenika, korisnika, klijenata, poslovnih partnera i sl.			
2	Vodite li na sustavan način zbirke osobnih podataka? Npr. u tablicama ste zabilježili gdje se sve nalaze osobni podaci i o kojim je podacima riječ (imena i prezimena, e-mail adrese, adrese stanovanja i sl.).			
3	Znaju li pojedinci da imate njihove osobne podatke i kako ih koristite? Razmjenjujete li njihove osobne podatke s nekom drugom tvrtkom?			
4	Prikupljate li osobne podatke potrebne samo za obavljanje posla? Razmislite imate li, primjerice, OIB, kućnu adresu ili neke druge osobne podatke koji nisu nužni za pružanje usluge.			
5	Čuvate li osobne podatke dulje nego što je potrebno? Npr. zakonom je određeno razdoblje čuvanja određenih osobnih podataka (npr. 15 god.). Čuvanje osobnih podataka može biti vezano uz trajanje ugovorne obveze, jamstveni rok i slično.			
6	Čuvate li posebno osjetljive osobne podatke? Npr. medicinska dokumentacija, podaci o sudskim postupcima i drugo.			
7	Smatrate li da su osobni podaci koje posjedujete adekvatno zaštićeni od gubitka ili krađe?			

8	Ako osoba čije podatke posjedujete zatraži pristup ili brisanje osobnih podataka, znate li kako ćete postupiti?			
9	Imate li pravilnik ili sličan dokument u kojem propisujete načine ponašanja svojih zaposlenika s osobnim podacima? Jesu li svi zaposlenici upoznati s time?			
10	Regulirate li već na neki način u ugovorima sa svojim poslovnim partnerima upotrebu osobnih podataka? Npr. dodatak ugovoru o zaštiti i obradi osobnih podataka.			

Izvor: autori

4. PRIMJENA U MALIM PODUZEĆIMA (EMPIRIJSKA EVALUACIJA)

Prethodno opisan okvir valorizira se na dva mala poduzeća - jedno je u segmentu ICT usluga, a drugo u segmentu organizacije događanja.

Nakon donošenja Opće uredbe o zaštiti podataka (GDPR) 2018. godine napravljena je implementacije te uredbe u oba poduzeća. U nastavku će se opisati revizija postojeće dokumentacije, a kao temelj koristit će se predloženi okvir s posebnim naglaskom na upitnik za početnu analizu (faza predanalize).

4.1. Poduzeće 1 (IKT, Centar za podršku)

U prvom slučaju opisano je malo poduzeće koje daje usluge Centra za podršku neprofitne međunarodne organizacije.

U tvrtki se pružaju dvije razine usluga - sistemska podrška servisima namijenjenim članicama neprofitne organizacije te podrška članicama u primjeni servisa i korištenju standarda. Ne postoji poseban IT odjel jer su sami zaposlenici educirani u segmentu ICT-ja, a prisustvovali su i seminarima vezanima za Opću uredbu te su pohađali i online tečajeve.

Analiza

Prva procjena usklađenosti s GDPR-om provedena je 2018. godine kako bi se identificirale neusklađenosti. Procjena usklađenosti provedena je na temelju dokumenta "Vodič ICC-ja za informacijsku sigurnost u poslovanju" koji je 2015. izdao *International Chamber of Commerce* (ICC). Nakon analize dobivenih rezultata poduzete su potrebne aktivnosti - od edukacije zaposlenika do kreiranja zahtijevanih dokumenata i odgovarajućeg načina čuvanja podataka (npr. papirnata dokumentacija u posebno zaštićenom skladištu). Poduzeće je identificirano kao voditelj obrade podataka kada se obrađuju podaci o zaposlenicima. U odnosu s klijentom poduzeće je identificirano kao izvršitelj obrade, dok je klijent voditelj obrade osobnih podataka.

Za potrebe ovog rada napravljena je revizija postojećeg stanja, a kao polazna točka za analizu poslužile su informacije prikupljene u početnom upitniku i inicijalno kreirana dokumentacija 2018. godine.

Kako bi se dobila jasna slika o postojećoj zaštiti osobnih podataka te je li ona na odgovarajućoj razini, proveden je razgovor sa svim zaposlenicima u poduzeću te je pregledana

sva dokumentacija vezana uz GDPR. Utvrđeno je da svi zaposlenici imaju saznanja o osobnim podacima koje obrađuju - o zaposlenicima i klijentima, a tijekom prve implementacije Uredbe kreiran je i dokument (Kodeks ponašanja) na razini organizacije u kojemu se, između ostaloga, propisuje i ponašanje u radu s osobnim podacima.

Procesi su djelomično identificirani i dokumentirani - dokumentirani su procesi vezani uz prikupljanje i obradu osobnih podatka o zaposlenicima, ali nisu za obradu osobnih podataka klijenata. Iz dokumentiranog procesa o zaposlenicima vidljivo je da prikupljeni osobni podaci imaju zakonsku podlogu. Uočen je nedostatak dokumentiranog procesa vezanog za klijente. Zaposlenici su upoznati s informacijom da od osobnih podataka prikupljaju isključivo ime i prezime, e-mail adresu i telefonski broj. Upoznati su s činjenicom da se podaci koriste isključivo za poslovnu komunikaciju. Kako je dokumentiran samo proces o zaposlenicima, a ne i o klijentima, dodatno je kreiran i dokument pod nazivom Zbirka osobnih podataka za zaposlenike. Takav dokument nije formalno definiran za obradu podataka klijenata. U poslovnim procesima tvrtke nema potrebe za podacima koji se klasificiraju kao posebno osjetljivi podaci, npr. zdravstveni podaci, biometrijski podaci itd.

Prema dobivenim informacijama, podaci o zaposlenicima čuvaju se sukladno zakonskim odredbama i dobroj praksi u zaštiti osobnih podataka, dok se podaci koji nisu više relevantni za poslovnu komunikaciju brišu, pri čemu je uočeno da nije definirana procedura brisanja podataka na zahtjev.

Odgovorne osobe navele su da se podaci čuvaju na nekoliko načina - dokumenti u papirnatom obliku dijelom su u čuvanom skladištu (adekvatna primjena vatrodojave i protuprovale), a ostatak dokumentacije nalazi se u zaključanim ormaru, dok su podaci u digitalnom obliku na klijentskoj strani zaštićeni lozinkom (kontrola pristupa).

S knjigovodstvom postoji poseban ugovor o zaštiti podataka, kao i s klijentom.

Revizijom je utvrđeno da je napravljen velik inicijalni napor da se poduzeće uskladi s GDPR-om, no tek kada je bilo potrebno dati detaljne odgovore na pitanja u upitniku za početnu analizu, vidjelo se da još postoji dosta nerazumijevanja sadržaja uredbe, posebno terminologije.

Dizajn

Provedenom analizom utvrđeno je da najveći dio formalno potrebnih dokumenata u tvrtki već postoji te su redovito revidirani. S obzirom na trenutačno stanje, poduzeće je u visokom stadiju usklađenosti s GDPR-om. Uočen je prostor za napredak pri upotrebi zbirki osobnih podataka koje se odnose na podatke o klijentima, procedura za postupanje s podacima klijenata kada je poduzeće u ulozi izvršitelja obrade te nekoliko procedura vezanih uz obveze izvršitelja obrade (npr. brisanje osobnih podataka). Procedure je potrebno ažurirati ili kreirati kako bi svi zaposlenici na jednak način i s potrebnom pažnjom upravljali osobnim podacima.

Implementacija

U fazi implementacije ključno je izvršiti ono što je definirano u fazi dizajna (kreiranje potrebnih procedura za upravljanje osobnim podacima). Za ovaj slučaj implementacija je prepuštena upravi tvrtke. S obzirom na to da je poduzeće tijekom inicijalnog usklađivanja

s regulativom 2018. provelo veliku većinu obveza, u ovoj fazi provelo bi se testiranje operativne učinkovitosti pojedinih procedura.

4.2. Poduzeće 2 (organizacija događanja)

U drugom slučaju opisano je malo poduzeće čiji je osnovni proizvod organizacija događanja, prvenstveno okupljanje malih i srednje velikih poduzetnika te edukacije u području poduzetništva, upravljanja i marketinga. Edukacije se u razdoblju od početka pandemije odvijaju online, a okupljanja poduzetnika u manjem se broju odvijaju uživo.

Iako je poduzeće malo, obrađuje se velika količina osobnih podataka. Poduzeće koristi nekoliko kanala komunikacije s korisnicima i potencijalnim korisnicima – e-mail, Facebook, Twitter te portal na kojemu se objavljuju članci vezani uz područja koja se pokrivaju i edukacijama.

Ne postoji poseban IT odjel, koriste se usluge vanjskih poduzeća, a komunikaciju putem navedenih aplikacija vode zaposlenici poduzeća.

Analiza

U poduzeću postoje dokazi o nastojanju uvođenja Uredbe od 2018., što je vidljivo u postojanju, primjerice, dokumenta Zbirke osobnih podataka, a najviše informacija dobiveno je u odgovorima odgovorne osobe i zaposlenika na pitanja iz upitnika za početnu analizu.

Na temelju odgovora i uvidom u postojeću dokumentaciju uočeno je da nije provedena inicijalna procjena usklađenosti s GDPR-om, a ne postoji ni krovni dokument u kojem se definira postupanje zaposlenika pri obradi osobnih podataka.

Iako zaposlenici nisu polazili edukaciju vezanu uz obradu osobnih podataka, znali su identificirati osobne podatke koje posjeduju (informacije o zaposlenicima i korisnicima te dobavljačima). Napominju da su korisnici usluga upoznati s činjenicom da poduzeće obrađuje njihove osobne podatke (ime i prezime, e-mail, telefonski broj samo ako je nužno) - dani su dragovoljno, a upoznati su i s činjenicom da poduzeće ne razmjenjuje osobne podatke s trećim stranama. Prikupljeni osobni podaci koriste se isključivo u poslovnoj dokumentaciji. Na pitanje prikupljaju li posebno osjetljive podatke odgovoreno je negativno.

Kao što je navedeno, postoji Zbirka osobnih podataka vezana za zaposlenike, ali nije kreirana Zbirka osobnih podataka za korisnike usluga. Odgovorna osoba navodi da se podaci o zaposlenicima čuvaju sukladno zakonskim odredbama, a ostali podaci vremenski koliko je nužno za učinkovitu komunikaciju, no to nigdje nije dokumentirano. Osim toga, nigdje nije dokumentiran ni proces brisanja podataka iako zaposlenici tvrde da su upoznati s njime.

Dokumenti (podaci) u papirnatom obliku čuvaju se u sjedištu poduzeća, a podaci u digitalnom obliku na klijentskoj strani zaštićeni su lozinkom.

Dizajn

Nakon faze analize u kojoj su prepoznati određeni nedostaci u odnosu na regulatorne zahtjeve te dobru praksu u tehničkim i organizacijskim mjerama zaštite osobnih podataka, u fazi dizajna definirane su potrebne aktivnosti (npr. nužna dokumentacija kao podloga

za obradu osobnih podataka i sigurnosne mjere zaštite). Treba krenuti od krovnog dokumenta u kojem će se definirati opredjeljenje zaštite osobnih podataka i osnovne obveze koje poduzeće ima kad je riječ o zaštiti osobnih podataka kao voditelj obrade i kao izvršitelj obrade (npr. Pravilnik o zaštiti osobnih podataka). U poduzeću postoje definirani procesi vezani uz održavanje događanja okupljanja poduzetnika, ali ne i ostali procesi, primjerice oni vezani uz edukaciju. Jedan od prvih koraka koje treba poduzeti jest edukacija zaposlenika o zaštiti osobnih podataka, što je moguće provesti nabavom ili kreiranjem edukacijskih materijala o zaštiti osobnih podatka s kojima potom treba biti upoznat svaki zaposlenik.

Zatim treba ažurirati postojeće radne procedure tako da pri provođenju procesa uzimaju u obzir zaštitu osobnih podataka onako kako je definirano u GDPR-u.

Potrebno je kreirati procedure kako bi poduzeće bilo spremno osigurati prava ispitanika (pravo na pristup podacima, pravo na zaborav itd.) i obveze koje ima kao voditelj/izvršitelj obrade (npr. postupak u slučaju gubitka osobnih podataka).

S obzirom na to da poduzeće prikuplja i obrađuje znatnu količinu osobnih podataka, treba provesti i procjenu učinka na zaštitu osobnih podataka (DPIA – *Data Privacy Impact Assessment*). Sama procjena neće biti toliko kompleksna jer poduzeće ne provodi automatiziranu obradu osobnih podataka pojedinaca kojim bi izrađivala profile na temelju kojih se donose odluke s utjecajem na pojedinca.

Implementacija

S obzirom na to da je riječ o malom poduzeću s vrlo ograničenim resursima (zaposlenici, poznavanje područja zaštite osobnih podataka), angažiran je vanjski suradnik s kompetencijama u području zaštite osobnih podataka koji je zajedno s upravom poduzeća implementirao zahtjeve definirane u fazi dizajna.

5. ZAKLJUČAK

Uvođenje GDPR-a za mnoga je poduzeća predstavljalo velik napor, što je bilo uočljivo na primjerima malih i srednje velikih poduzeća prvenstveno zbog ograničenja ljudskih resursa, ali i kompetencija. U ovom radu predstavljen je okvir koji može pomoći malim i srednje velikim poduzećima u uvođenju GDPR-a, ali i u evaluaciji postojećeg stanja nakon uvođenja GDPR-a. U svojoj namjeni predloženi okvir nije predviđen kako bi se koristio u svrhu potvrde regulatorne usklađenosti.

Okvir je rezultat analize dobivenih rezultata opisanih u znanstvenim i stručnim časopisima, ali i spoznaja tijekom revizije uredbe u dva mala poduzeća. Smatra se kako predstavljeni okvir može pomoći malim i srednjim poduzećima da provedu jednostavniji (i jeftiniji) postupak uvođenja GDPR-a ili evaluaciju postojećeg stanja.

Provjera opisanog okvira napravljena je evaluacijom stanja u poduzećima dvije godine nakon prvog vala uvođenja GDPR-a. Primijenjen je na dva mala poduzeća iz različitih područja djelatnosti, a inicijalni rezultati primjene pokazuju njegovu efikasnost.

Rezultati su pokazali da, iako je prošlo već dvije godine od uvođenja GDPR-a, u malim i srednje velikim poduzećima još postoji određeno nerazumijevanje terminologije i obaveza

u smislu svakodnevne primjene. Tumačenja regulatora unose dodatnu dinamiku i kompleksnost u razumijevanje i primjenu Uredbe. Primjetno je da u poduzećima još nedostaju pojedini formalni dokumenti, posebno zato što treba kontinuirano pratiti aktualne preporuke i tumačenja regulatora te primijeniti odgovarajuće prilagodbe unutar poduzeća.

Dinamika i kompleksnost u razumijevanju i primjeni Uredbe podrazumijevaju kontinuiranu edukaciju zaposlenika te praćenje promjena, što malim i srednje velikim poduzećima može predstavljati dodatne troškove.

Rezultati sugeriraju da opisani okvir može biti od znatnije pomoći malim i srednje velikim poduzećima zbog jednostavnosti i lakoće primjene, no treba ga dodatno potvrditi u više poduzeća. Nakon primjene okvira i nadzora AZOP-a kao regulatora, bilo bi korisno ponoviti analizu primjene u svrhu unapređenja predloženog okvira.

FRAMEWORK FOR INTRODUCTION AND VERIFICATION OF GDPR IN SMALL AND MEDIUM-SIZED ENTERPRISES

Sanja Penić, MSc, senior lecturer
Rapska 26/1, Zagreb, Croatia
Phone: +38598 326 301, E-mail: sanja.penic@digbiz.hr

Kristian Saletović, MSc, senior lecturer
Miroševečki brijeg 33, Zagreb, Croatia
Phone: +38599 3657 538, E-mail: kristian.saletovic@gmail.com

ABSTRACT

The General Data Protection Regulation (Regulation (EU) 2016/697 known as GDPR) began its application in May 2018 and it had a significant impact on the organisation of business processes in companies. In particular, this was felt by small and medium-sized enterprises for which GDPR is an additional burden due to already limited resources. The framework for the implementation and revision of previously implemented GDPR requirements, presented in this paper, is the result of information obtained through scientific literature and knowledge obtained through the revision of the already implemented Regulation in two small enterprises. The obtained results showed that although it has been two years since the first implementation, there is still a misunderstanding of terminology and obligations in terms of daily application.

***Keywords**: personal data; small and medium-sized enterprises; GDPR; processes, security*

LITERATURA

1. Brodin, M. (2019): A Framework for GDPR Compliance for Small and Medium-Sized Enterprises. *European Journal for Security Research, 4, 243–264*; https://doi.org/10.1007/s41125-019-00042-z
2. CEPOR (2018). *Izvješće o malim i srednje velikim poduzećima u Hrvatskoj – 2018., uključujući rezultate GEM – Global Entrepreneurship Monitor istraživanja, 2017*
3. DPC – *Data Protection Commission* - irski regulator za zaštitu osobnih podataka; lista za samoprocjenu; Dostupno na: https://www.dataprotection.ie/en/organisations/self-assessment-checklist (20. 8. 2020.)
4. Eurostat (2015). *Basic structure: employment size class breakdown in Structural Business Statistics*. Dostupno na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises#Basic_structures:_employment_size_class_breakdown_in_Structural_Business_Statistics (30. 8. 2020.)
5. Eurostat (2015). *Statistics on small and medium-sized enterprises*. Dostupno na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises (30. 8. 2020.)
6. Eurostat (2020). *Small and medium-sized enterprises* (SMES). Dostupno na: https://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme (30. 8. 2020.)
7. Fisher, G.: (2020). Guidelines for SME adaption to GDPR, Case Study of Evalent. *Master Thesis, Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering*
8. Freitas, M. C., Silva, M. M. (2018). GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management, 3*(4), 30. doi: https://doi.org/10.20897/jisem/3941
9. Gilliéron, P. (2018). *Towards GDPR compliance as a best practice : a primer for Swiss SMEs. IAPP*. Dostupno na: http://www.communityresearch.org.nz/wp-content/uploads/formidable/8/Towards-GDPR-compliance-Primer-for-Swiss-SMES-Prof.-Philippe-Gilli--ron.pdf
10. Hashim, J. (2015). Information communication technology (ICT) adoption among SME owners in Malaysia, *Int J Bus Inf 2(2):221–240*
11. ICO – *Information Commissioner's Office* - britanski regulator za zaštitu osobnih podataka; samoprocjena za mikro i male tvrtke. Dostupno na: https://ico.org.uk/for-organisations/business/assessment-for-small-business-owners-and-sole-traders/ (20. 8. 2020.)
12. International Chamber of Commerce (2015). *Vodič ICC-a za informacijsku sigurnost u poslovanju*
13. Kapoor, K., Renaud, K., Archibald, J. (2018). Preparing for GDPR: helping EU SMEs to manage data breaches. In: *AISB 2018: Symposium on Digital Behaviour Interventions for Cyber-Securilty*. AISB, pp.13-20. Dostupno na: http://aisb2018.csc.liv.ac.uk/PROCEEDINGS%20AISB2018/Digital%20Behaviour%20Interventions%20for%20CyberSecurity%20-%20AISB2018.pdf
14. Lindqvist, J. (2018): New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *Int J Law Inf Technol 2018(26):45–63*
15. Matt, T. M., Modrak, V. Zsifovits H. (2020*). Industry 4.0 for SMEs, Challenges, Opportunities and Requirements. Palgrave Macmillan, str. 37.* doi: https://doi.org/10.1007/978-3-030-25425-4

16. Ostendo group - upitnik za procjenu usklađenosti sa zahtjevima Opće uredbe o zaštiti osobnih podataka. Dostupno na: https://ostendogroup.com/hr/wp-content/uploads/2017/10/Upitnik-za-samoprocjenu.pdf (20. 8. 2020.)
17. Schulze, H. (2018): GDPR compliance report. Dostupno na: https://crowdresearchpartners.com/portfolio/gdpr-compliance-report/ (1. 9. 2020.)
18. Sirur, S., Nurse, J. R. C., Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the general data protection regulation (GDPR). *In: MPS'18, pp 88–95*
19. Sprøgel, E. (2018). Information Security: The GDPR and SMEs in Denmark, *Master Thesis, Faculty of Governance and Global Affairs, Leiden University*
20. Stepan, T. (2019). Implementacija GDPR-a u malim poduzećima. *Diplomski rad br. 105/OJ/2018, Sveučilište sjever, sveučilišni centar Varaždin.* Dostupno na: https://repozitorij.unin.hr/islandora/object/unin%3A2463/datastream/PDF/view (1. 9. 2020.)
21. Šiškova, J., Lorinczova, E. (2020). Implementation of GDPR into Payroll Accounting in the Czech Republic. *Hradec Economic Days.* Dostupno na: https://digilib.uhk.cz/bitstream/handle/20.500.12603/291/%C5%A0i%C5%A1kov%C3%A1%20aj..pdf?sequence=1&isAllowed=y (1. 9. 2020.)
22. Tarutėa, A. Gatautis, R. (2013): ICT impact on SMEs performance, Contemporary Issues in Business, Management and Education. *Procedia - Social and Behavioral Sciences 110,* 1218 – 1225