PROCESS MODELING FOR GDPR COMPLIANCE

MODELIRANJE PROCESA USKLAĐIVANJA S GDPR UREDBOM

KRAKAR, Ivan & ALIC, Marta

Abstract: *On May 25.2018. the General Data Protection Regulation (GDPR) or EU Regulation 2016/679 will be enforced in every EU country without transposing into national legislation. This Regulation was designed to harmonize EU data privacy laws, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. This is disruptive moment that will have a significant impact on every organization that gathers and uses personal data. Such organization have to harmonize theirs business processes and activities due to new Regulation such as collecting, gathering, processing and storing information and also harmonize their information security and business policy.*

Key words: *General Data Protection Regulation, Privacy impact assessment, GAP Analysis*

Sažetak: *Zaštita osobnih podataka postaje krucijalni problem gotovo za sve zemlje i sve poslovne sustave. S 25. svibnjem 2018. godine Opća uredba o zaštiti osobnih podataka (eng. General Data Protection Regulation; GDPR) Europske unije ili Uredba 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka, počinje se primjenjivati u svim državama članicama EU direktno, bez potrebe za dodatnim prenošenjem u nacionalno zakonodavstvo. Disruptivni je to moment koji utječe na sve organizacije unutar, ali i izvan EU, a koje prikupljaju i koriste podatke o građanima Unije, koje su pred velikim izazovom usklađivanja poslovnih procesa i aktivnosti s novom regulativom koja obuhvaća izmjene ne samo u prikupljanju, obradi, tijeku i pohrani informacija, već i na području informacijske sigurnosti te općih poslovnih politika*

Ključne riječi: *GDPR, zaštita podataka, PMI metodologija, analiza utjecaja na privatnost, analiza odstupanja*

Authors' data: Ivan **Krakar**, Tehničko veleučilište u Zagrebu, ikrakar@tvz.hr; Marta **Alić**, Tehničko veleučilište u Zagrebu, malic@tvz.hr

1. Uvod

Pravo na zaštitu privatnosti temeljno je ljudsko pravo. Ukoliko se ono ne poštuje, moguće su i dešavaju se mnogobrojne zlouporabe u više područja, između ostalog i s osobnim podacima. Zbog toga se potreba za normativnim uređenjem ovog područja razvija već duže vrijeme. Pravo na zaštitu privatnosti prvi je put propisano međunarodnim pravnim aktom Opće deklaracije o ljudskim pravima (UDHR) Ujedinjenih naroda (UN) 1948.g., u članku 12 [1]. Nakon toga pojedine zemlje počele su donositi propise o zaštiti osobnih podataka te su razvijani standardi i postupci zaštite privatnosti i podataka diljem svijeta, poput Smjernica za zaštitu privatnosti i prekograničnu razmjenu osobnih podataka Organizacije za ekonomsku suradnju i razvoj iz 1980. [2] te „Privacy framework" dokumenta organizacije Azijsko-pacifičke ekonomske suradnje iz 2005 [3]. Unatoč ovim nastojanjima, praksa kršenja prava privatnosti kontinuirano se događa u svim zemljama, što se može pratiti i kroz razne primjere europske sudske prakse [4].

Rapidni rast mogućnosti i primjene informacijske-komunikacijske tehnologije (IKT) stalno rađa nove ugroze osobnih podataka. Najsvježiji i najdramatičniji primjer koji je izbio u javnost, jest slučaj tvrtke Cambridge Analitics koja je koristila javno objavljene Facebook profile u razne svrhe koje nisu u skladu s načelima očuvanja privatnosti pojedinaca [5]. Upravo je sprječavanje takve zloupotreba osobnih podataka korisnika u fokusu nove europske uredbe, koja nastoji očuvati privatnost svih pojedinaca na svome teritoriju.

2. Razvoj potrebe za zaštitom osobnih podataka

Početak zaštite osobnih podataka u Europi u 1981. g., kada je Vijeće Europe prihvatilo Konvenciju za zaštitu pojedine osobe u pogledu automatske obrade osobnih podataka [6]. Taj akt bio je osnova za izradu Direktive 95/46/EZ Europskog parlamenta i Vijeća, od 24. listopada 1995. godine, o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnim protokom takvih podataka, koju izvan snage stavlja upravo Opća uredba o zaštiti osobnih podataka (eng. General Data Protection Regulation, GDPR).

U Hrvatskoj pravo na privatnost osigurano je člankom 37. Ustava [7]. Na temelju spomenute Direktive 95/46/EZ, Hrvatska je 2003. donijela Zakon o zaštiti osobnih podataka (NN 103 /03) kojim se uređuje zaštita podataka o fizičkim osobama, kao i nadzor nad prikupljanjem, obradom i njihovim korištenjem. Unatoč tome, praksa ukazuje na brojne primjere kršenja ustavnog prava svakodnevno, sudeći kroz brojne primjere i rješenja objavljena na mrežnim stranicama Agencije za zaštitu osobnih podataka [8].

Smatra se da su u svijetu vodeći motivi za ugrožavanje privatnosti: krađe osobnih podataka zbog ekonomskog interesa, politički marketing i loša namjera. Porastom trenda

digitalne transformacije sve više podataka prikuplja se i obrađuje posredstvom internata, no „ispod radara" prolazi činjenica da je svega 5 – 7 % informacijskog sadržaja na ovoj globalnoj informacijsko-komunikacijskoj infrastrukturi, sigurno [9]. Također, jedan od temeljnih razloga pojačane skrbi za zaštitom osobnih podataka jest i suvremeni način poslovanja u uvjetima globalizirane ekonomije. Takav vid poslovanja zahtijeva prekogranične tokove mnogobrojnih podatkovnih sadržaja, a time i osobnih podataka.

3. GDPR kao jedinstveni okvir zaštite osobnih podataka u EU

Nakon 4 godine debata, pregovora i lobiranja, Europska komisija donijela je 27. travnja 2016. konačnu verziju Opće uredbe o zaštiti osobnih podataka, koji nakon godine dana prilagodbenog perioda, unosi nova pravila i standarde u zaštiti osobnih podataka. GDPR uredba [10] sastoji se od 173 recitala ili općih načela, 11 poglavlja i 99 članaka. Uredba se odnosi se na sve tvrtke i organizacije koje posluju na teritoriju Europske unije, ali i na tvrtke koje raspolažu podacima europskih građana, bez obzira na njihovu lokaciju. Tvrtke koje su izvan Europske unije i nude svoje proizvode ili usluge unutar Europske unije, također su dužne poštovati odredbe GDPR-a, čime ova, izvorno europska regulativa, ima dalekosežan, globalni utjecaj, a njene značajke navedene su u nastavku.

- Uredba bitno proširuje definiciju osobnog podatka kao svaku informaciju koja se odnosi na identificiranu fizičku osobu koja se može identificirati i čiji se identitet može utvrditi izravno ili neizravno, na osnovi jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet, te osim osnovnih identifikacijskih podataka, kao osobne podatke definira i IP adresu, GPS lokaciju, RFID tagovi te kolačiće na web stranicama.
- Uredba propisuje mnogobrojne obveze koje dosadašnji propisi nisu tretirali, usmjerene prema osiguravanju prava pojedinca npr.; informacije koje treba dostaviti ispitaniku, pravo ispitanika na pristup svojim osobnim podacima, pravo na ispravak, pravo na brisanje, pravo na prenosivost, pravo na prigovor, ograničenja, obveze voditelja i izvršitelja obrada, sigurnost osobnih podataka itd.
- Uredbom se uvode načela prilikom obrade osobnih podataka: zakonitosti, poštenosti i transparentnosti obrade, ograničavanja svrhe i minimalizacije podataka, točnosti, cjelovitosti i povjerljivosti podataka, kao i ograničavanja roka pohrane podataka te pouzdanosti voditelja obrade, ali i izvršitelja obrade, da će poštivati sva načela i prava pojedinaca te, u protivnome, snositi odgovornost.
- Uredba također propisuje i vođenje registra osobnih podataka, obvezu postojanja službenika za zaštitu osobnih podataka, obvezu procjene učinaka na osobne podatke, kodeks ponašanja, obvezu obavješćivanja regulatora u slučaju proboja osobnih podataka i mnoge druge novine.

Kako bi osigurala provedba Zakona, Europska komisija odredila je složenu kaznenu strukturu koja prijestupnike penalizira s iznosima do 20 milijuna eura ili 4 % godišnjeg

prihoda tvrtke, ovisno koji je iznos veći, te je imenovala nacionalna regulatorna tijela u zemljama članicama za vršenje nadzora, a koja su ovlaštena provoditi audite i po drugim zemljama EU.

4. Model implementacije GDPR-a u praksu

Budući da GDPR tek ulazi u primjenu, ne postoji sustavno znanje, niti jedinstveni način o tome kako implementirati sukladnosti s Uredbom u sustave organizacija koji joj podliježu. Prema svom obujmu i djelokrugu, GDPR zahtjeva poznavanje slijedećih 5 aspekata: pravnih aspekata Uredbe, ali i niza drugih propisa koji se odnose na prikupljanje i obradu osobnih podataka, poznavanje organizacije poslovnog sustava i načina funkcioniranja u koji se ona uvodi, aspekte procjene rizika, sigurnosne aspekte i IKT potporu evidencijama osobnih podataka u konkretnom poslovnom sustavu. Iz svega toga proizlazi da je implementacija GDPR-a izrazito multidisciplinarno područje.

No, pristupajući uvođenju primjene Uredbe u poslovanje kao projektu, vremenski određenoj aktivnosti s ciljem ostvarivanja jedinstvenog rezultata, odnosno proizvoda, što svaka implementacija promjena i jest, moguće je pri tome postupku primijeniti i voditi se metodologijom za vođenje projekata. Iako je izgradnja infrastrukture privatnosti kroz organizaciju sustavan proces kojem treba pristupati holistički i kontinuirano, prilikom uspostavljanja sukladnosti sa zadanim regulativama, potrebno je, prije svega, izraditi osnovne resurse na temelju kojih će se struktura razvijati. To je jednostruk proces koji ima svoj početak i kraj, sa određenim potrebnim resursima (vremenskim, tehničkim, novčanim, ljudskim i dr.) koje treba uskladiti i organizirati u odnosu na ciljeve i rokove. Projektna metodologija predstavlja alate kojima se na sustavan način čini upravo ta potrebna harmonizacija i orkestracija potrebnih zahtjeva, tj. provodi se projekt.

Suvremeno vođenje projekata primjenjuje se u svim područjima poslovanja, uključujući i područja IKT-a, poput razvoja novog proizvoda, informacijskog sustava, programske opreme i mnogih drugih. Krovna institucija koja certificira stručnjake na području vođenja projekta naziva se Project Management Institute, a njena metodologija objavljuje se redovito kao Project Management Book of Knowledge (skraćeno PMBOK) [11], katalog znanja o upravljanju projektima, koji je postao i globalni standard upravljanja projektima. Metodologija obuhvaća sposobnosti i tehnike usmjerene na uspješnu realizaciju nekog projekta, podrazumijevajući odabir adekvatnih metoda za pojedine dijelove samog projekta te drugih pomagala ovisnih o tipu, veličini i ostalim značajkama projekta i njegove okoline. Tako projekt prema PMI metodologiji započinje fazom inicijalizacije, a završava zatvaranjem projekta. Između te dvije vremenske točke voditelj projekta definira, planira i upravlja svim segmentima projekta, kojih prema ovoj metodologiji ima 12 i čine ih: određivanje područja (scope) projekta, određivanje faza i aktivnosti projekta, određivanje organizacije projekta, upravljanje vremenom, upravljanje ljudskim resursima,

upravljanje rizicima, upravljanje troškovima, upravljanje kvalitetom, upravljanje komunikacijama, upravljanje nabavom i upravljanje odnosima s dionicima.

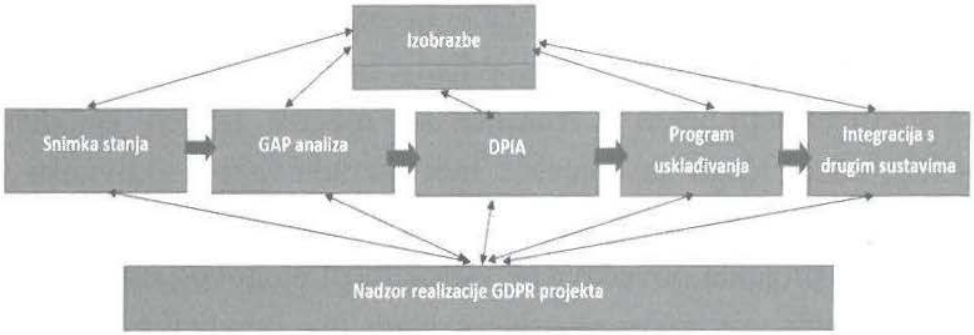
Svaki od ovih segmenata projekta je značajan za njegov uspjeh. Ishodište je odrediti područje projekta, nakon čega se najčešće radi razrada faza i aktivnosti te planiranje potrebnih ljudskih resursa i vremena. Potom slijede i drugi segmenti projekta. Primjerice, upravljanjem rizicima projekta povećava se vjerojatnost njegovog uspjeha, smanjivanjem mogućnosti štetnih djelovanja rizika na projekt. Nadalje, upravljati troškovima moguće je na razne načine i primjenom raznih modela zbog čega je u vođenju projekata važno i upravljanje nabavom. Naime, većina projekata zahtijeva različite materijalne resurse koji se nabavljaju relativno složenim procesima u kojima može sudjelovati više dobavljača, ugovaratelja i naručitelja. Također, i komunikacije u projektu identificirane su kao bitan čimbenik uspjeha, odnosno neuspjeha projekta, budući da iskustvo pokazuje kako voditelj nekog projekta provede gotovo 70% svog vremena u komunikaciji unutar ili izvan tima.

Radom se prikazuje primjena dijela PMI metodologije na slučaju uvođenja primjene odredbi Uredbe u poslovanje kao projektu na slijedeći način:

1. Područje vođenja projekta jesu zahtjevi same GDPR uredbe. Znači ovim projektom nužno je zadovoljiti sve što ona nalaže kao striktne zahtjeve ili preporuke. Za poslovni sustav koji uvodi GDPR to su prije svega obveze iz poglavlja 1 – 5 (Opće odredbe, Načela, Prava ispitanika, Voditelj i izvršitelj obrade, Prijenos osobnih podataka trećim zemljama i međunarodnim organizacijama).
2. Organizaciju GDPR projekta čine određeni ljudski resursi: pokrovitelj, voditelj i članovi tima. Budući da u poslovnim sustavima koje uvode GDPR nema još dovoljno znanja o ovom tipu projekata, za očekivati je angažman konzultanata, a od strane korisnika sudjelovanje rukovoditelja pojedinih organizacijskih cjelina.
3. Očekivane faze GDPR projekta su: snimka stanja, analiza odstupanja ili GAP analiza, procjena učinaka i rizika (DPIA), izrada programa usklađivanja, integracija s drugim sustavima i nadzor realizacije projekta.
4. Upravljanje vremenom postiže se izradom plana projekta. Prva konzultantska iskustva tvrtki koje su već realizirale ovakve projekte u praksi [12] pokazuju da za srednje veliki poslovni sustav takav projekt traje oko 3 mjeseca, pri čemu su očekivana trajanja pojedinih faza: snimka stanja 50 %, GAP analiza 15%, DPIA 15%, program poboljšanja 10% i integracija s drugim sustavima 10 %.

5. Prikaz konkretnog slučaja

Okvir za implementaciju GDPR uredbe, opisan u prethodnom poglavlju., ispitan je u praksi. Faze ovog procesa prikazane su na slici 1.



Slika 1 Proces implementacije GDPR-a u neki poslovni sustav

Ciljevi pojedinih faza, način njihove provedbe i rezultati koji pri tome nastaju, opisani su u nastavku.

5.1. Snimka stanja

Cilj ove faze je identificirati poslovne cjeline, njihove poslovne procese i IT servise koji uključuju osobne podatke i načine zaštite kroz izradu: organigrama, pravilnika, opisa poslovnih procesa, procedura, propisa, aplikacija i drugih evidencija osobnih podataka kroz radionice s predstavnicima svih ustrojbenih cjelina poslovnog sustava. Snimkom stanja potrebno je obuhvatiti i zaštitu podataka zaposlenika, ali i svih ostalih osoba u radnom ili poslovnom angažmanu, zaštitu podataka dobavljača, partnera i korisnika, ukoliko se radi o privatnim osobama. Kao rezultat ove faze korisniku se isporučuje *Izvješće o provedenoj snimci i analizi stanja*, kao i Registar evidencija osobnih podataka, koji je od posebnog značaja za usklađivanje s člankom 10 Uredbe. Dokument se dostavlja u elektroničkom obliku te sadrži sljedeće: oblik evidencije (elektronička, klasična), svrhu prikupljanja osobnih podataka (javne ovlasti, ispunjenje ugovora itd.), osobne podatke koji se prikupljaju (OIB, ime i prezime, slika, otisak prsta i sl.), izvore iz kojih se prikupljaju osobni podaci (web ili klasični obrazac, dokument..), pravne osnove prikupljanja osobnih podataka (zakon, pravilnik itd.), kada se osobni podaci prikupljaju i ažuriraju, tko smije vidjeti te osobne podatke, mjesto i period čuvanja osobnih podataka, vezu prema drugim evidencijama i/ili aplikacijama u poslovnom sustavu, kao i izvan poslovnog sustava, izvoze li se podaci u druge zemlje ili organizacije, provedene mjere zaštite podataka te druge podatke, prema potrebi.

5.2. Analiza odstupanja (GAP analiza)

Na temelju izvršene snimke stanja, za svaki zahtjev, članak Uredbe, u sljedećem koraku se procjenjuje stupanj njegovog zadovoljenja u poslovnom sustavu. U analizu ulaze sva dostupna dokumentacija organizacije, s ključnim Registrom iz prethodnog koraka, opisima poslovnih procesa, katalogom korištenih aplikacija te procedurama informacijske sigurnosti. Aktivnosti analize uključuju radionice s članovima implementacijskog tima, kao i sa zaposlenicima organizacije. Rezultat provedene analize je matrica GDPR obaveza i trenutnog stanja s preporukama za potrebna usklađenja.

5.3. Analiza utjecaja na privatnost (PIA - Privacy impact assessment)

Analiza utjecaja na privatnost bitan je korak sukladnosti s odredbama Uredbe. Njena svrha, s ciljem prevencije, je identificirati, razumjeti i odrediti bilo kakve probleme s osobnim podacima koji mogu proizaći u njihovim obradama ili razvoju novih proizvoda, usluga, te odrediti razine rizika. Ove rizike može se odrediti na niz načina, a najčešće se primjenjuje „princip semafora" kao kombinacija odnosa utjecaja rizika i vjerojatnosti njegovog ostvarenja, kao što je prikazano u tablici 2.

Utjecaj rizika	Vjerojatnost ostvarenja rizika				
	1-Vrlo niska	2-Niska	3-Srednja	4-Visoka	5-Vrlo visoka
1-Vrlo nizak	1	2	3	4	5
2-Nizak	2	4	6	8	10
3-Srednji	3	6	9	12	15
4-Visok	4	8	12	16	20
5-Vrlo visok	5	10	15	20	25

Tablica 1 Procjenjivanje razine rizika prema principu semafora

Potrebna dokumentacija za ovaj korak je Registar evidencija, tzv. Katalog rizika te postojeće sigurnosne mjere. Baš kao i u prethodnom koraku, aktivnosti se odnose na izvođenje radionica s članovima tima, ali i na samostalni rad člana tima, eksperata za procjene rizika. Rezultati su: matrica evidencije, mogući rizici, vjerojatnosti pojave, razine rizika, kao i prijedlozi dodatnih sigurnosnih mjera. Svaki identificirani rizik za svaku evidenciju promatra se kroz njegov utjecaj i vjerojatnost pojavljivanja te se u skladu s time pozicionira u matrici. Za rizike u zelenom području nije potrebno ništa dodatno poduzimati, dok se rizici u žutom području trebaju pažljivije analizirati i vidjeti mogu li izazvati veće posljedice u slučaju ugrožavanja osobnih podataka, tako da je za neke od njih očekivano poduzimanje dodatnih sigurnosnih mjera. Međutim, rizici pozicionirani u crvenom području, sigurno su takvog karaktera da je za njih obvezatno primijeniti dodatne kontrole (organizacijske i tehničke mjere), kako bi ih se svelo na prihvatljivu razinu.

5.4. Program usklađivanja

Na osnovi snimke stanja, analize odstupanja i procjene rizika za osobne podatke, radi se plan usklađivanja. Njega čine organizacijske, pravne i tehničke prilagodbe koje je nužno poduzeti da bi se poslovni sustav uskladio sa zahtjevima Uredbe. Tijekom ove aktivnosti stručnjak za pojedino područje analizira što je nužno još poduzeti da se postojeća razina podigne na onu koju nalaže GDPR. Od organizacijskih prilagodbi to su: izrada dodatnih

procedura, npr., za upravljanje rizicima u vezi s osobnim podacima, upravljanje privolama, način pristupa ispitanika njegovim podacima, pravo na ispravak, pravo na zaborav, izvješćivanje regulatora u slučaju incidenta, pravo na prenosivost itd. Pravne prilagodbe nalažu doradu postojećih internih normativnih akata (npr., ugradnju aspekata privatnosti u ugovore s dobavljačima, doradu ugovora o radu, doradu pravilnika) ili izradu novih (kodeksa privatnosti, procjene učinkovitosti sustava upravljanja privatnošću itd.).

6. Interpretacija rezultata i metodologije

Navedeni koraci implementacije sukladnosti s GDPR uredbom specifični su prilikom izgradnje arhitekture privatnosti. Prilagodba sustava organizacija može se sagledati sa operativnog i taktičnog sloja uvođenja potrebnih tehničkih mjera u poslovanje te sa strateškog sloja na razini uprave koji uključuje donošenja potrebnih pravila i dokumenata za provedbu mjera (politike privatnosti, politike sigurnosti i dr.). Tako neki poslovni sustavi već imaju implementirane određene politike ili standarde upravljanja, poput upravljanja kvalitetom (ISO 9001), upravljanja zaštitom okoliša (ISO 14001), upravljanja informacijskom sigurnošću (ISO 27001) te upravljanja uslugama (ISO 20000). GDPR upravljanje zaštitom privatnosti je novi sustav kojeg je nužno povezati s već postojećim sustavima ili ugraditi u njih integracijom zajedničkih politika, procedura i/ili internih procjena učinkovitosti od strane uprave poslovnih sustava i drugim povezujućim segmentima. Kako je tijekom bilo kojeg projekta, tako i GDPR projekta, nužno je provoditi nadzor njegovog napredovanja, potrebno je čvrsto definirane kontrolne točke u kojima se analizira učinjeno i u slučaju bilo kakvih većih poremećaja poduzimaju dodatne korektivne mjere. Prikaz primjene PMI metodologije na konkretnom slučaju prikazuje jasan slijed koraka i faza te međusobnu ovisnost „izlaza" jedne s „ulazima" druge faze ili koraka. Dokumentirani procesi i aktivnosti poduzeti prema sukladnosti s Uredbom, ujedno su i dokaz poduzetih „razumnih mjera" koji mogu biti presudni i prilikom vanjskog nadzora te izbjegavanja navedenih, vrlo visokih kazni. Izgradnja arhitekture privatnosti u organizacijsku okolinu stalan je i proces koji je potrebno vršiti kontinuirano, što je prikazano i PMRM modelom i metodologijom OASIS organizacije [13], koji izdvaja također postupke procjene rizika (PIA) te analize odstupanja, kao bitne elemente procesa. U odnosu na radom preloženi model ovaj model je iterativan i ciklički te se izvodi dok se ne uspostavi željena arhitektura privatnosti. No, postavljanje osnovne strukture privatnosti, opisane radom, kao temelja za daljnja unaprjeđenja, a u svrhu usklađivanja sa zakonskim okvirima GDPR uredbe, u čvrsto zadanim rokovima i datostima, linearan je proces za koji je prikazana PMI metodologija primjenjiva i sukladna.

7. Zaključak

Iako ima globalni, disruptivni efekt na poslovanje, Opća uredba ne donosi nove koncepte zaštite privatnosti, tog temeljnog ljudskog prava, budući da se ovo područje normativno uređuje duži niz godina. No, globalizacija i snažan tehnološki razvoj, osobito IKT-a, donijeli su nove probleme u zaštiti osobnih podataka koji su prerasli nacionalna zakonodavna tijela, otvarajući prostor upravo za jedan sveobuhvatni zakonodavni okvir i organizacijski standard koji bi mogao poslužiti kao primjer globalne zaštite privatnosti pojedinaca poput Opće uredbe o zaštiti osobnih podataka. Problem Implementacije Uredbe u poslovanje, stoga, zahtijeva interdisciplinarni pristup izgradnji sustava privatnosti, inženjeringa privatnosti koji je idejno vezan uz primjenu principa tzv. „privatnosti prema dizajnu" (eng. Privacy by Design) [14], pristupa koji privatnost stavlja u fokus tijekom cijelog procesa oblikovanja sustava. Svodeći zahtjeve za privatnošću pod okrilje projekta, ovim radom kroz primjenu PMI metodologije, opisan je tijek provedbe implementacije „dizajna privatnosti" na primjeru poslovnog modela izvedenog u praksi, opisujući pritom i druge alate koje se koriste prilikom usklađivanja s novom zakonskom odredbom, a s ciljem osiguranja daljnje „zadane privatnosti" (eng. privacy by default) nakon 25. svibnja 2018.

8. Literatura

[1] UN, *Opća deklaracija o ljudskim pravima*. 1948, pp. 1–7.

[2] OECD, "Organisation for Economic Cooperation and Development guidelines Annex to the recommendation of the Council of 23 September 1980: Guidelines governing the protection of privacy and transborder flows of personal data," no. September, 1980.

[3] Asia Pacific Economic Cooperation, *APEC Privacy Framework (2005)*, no. November. 2005.

[4] Vijeće Europe, *Priručnik o europskom zakonodavstvu o zaštiti podataka*. 2014.

[5] The Independent, "Cambridge Analytica." [Online]. Available: https://www.independent.co.uk/topic/cambridge-analytica.

[6] Council of Europe (COE), *Convention for the Protection of Individuals with regard to Automated Processing of Personal Data*, no. 108. 1981, pp. 1–9.

[7] Hrvatski Sabor, "Ustav Republike Hrvatske," 2010.

[8] "Agencija za zaštitu osobnih podataka." [Online]. Available: http://azop.hr/.

[9] N. Kuster and Q. Balzano, *Mobile Communications Safety*. 2014.

[10] EU, "Opća uredba o zaštiti podataka," no. 3, 2016.

[11] Project Management Institute Inc, *A guide to the project management body of knowledge (PMBOK® guide)*. 2000.

[12] ZIH, "Preporuke za planiranje GDPR projekata," 2018.

[13] J. Sabo, M. Drgon, and G. Magnuson, "Privacy Management Reference Model and Methodology (PMRM) Version 1.0," no. May, pp. 1–37, 2016.

[14] I. & P. C. Ann Cavoukian and C. Ontario, "Privacy by Design, The 7 Foundational Principles," pp. 7–8, 2011.