UDC: 343.45:340.134 Info M str. 11-16

OSVRT NA GDPR UREDBU I SUGESTIJE ZA RAZVOJ APLIKATIVNE PODRŠKE
REVIEW OF THE GDPR REGULATION AND SUGESTIONS FOR THE DEVELOPMENT OF SUPPORT APPLICATION

Nenad Badovinac, student doktorskih studija, nenad.badovinac@gmail.com
Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, Srbija

REZIME: Uredba Evropske unije o zaštiti podataka o ličnosti (GDPR) primenjivaće se neposredno u svim zemljama članicama Evropske unije počevši od 25. maja 2018. godine. Ova regulativa definiše propise o zaštiti podataka ličnosti u Evropskoj uniji, ali uredba će se primenjivati i na kompanije sa sedištem u zemljama izvan Evropske unije. Ukoliko srpske kompanije na bilo koji način poseduju lične podatke građana Evropske unije, tada moraju da se usklade sa GDPR regulativom. Iz toga proizlazi da se GDPR neće primenjivati na sve kompanije koje imaju sedište u Srbiji, nego isključivo na one koje obrađuju podatke o ličnosti rezidenata Evropske unije. U radu su predstavljeni okviri sa naglaskom na pravne i tehničke aspekte koji su neophodni za proces usklade kompanije sa GDPR-om. S obzirom na potrebnu implementaciju tehnoloških rešenja, u radu su predstavljene sugestije za razvoj aplikativne podrške koje će biti primenjive tokom usklade kompanije sa GDPR-om.

KLJUČNE REČI: GDPR regulativa, aplikativna podrška, usklađivanje sa GDPR.

ABSTRACT: The European Union's Act for General Data Protection Regulation (GDPR) will be applied directly in all EU member states starting from May 25, 2018. This regulation defines principles on the protection of individuals personal data in the European Union, but it will apply to companies based in countries outside the European Union. If Serbian companies in any way have personal data of citizens of the European Union, then they have to comply with GDPR regulation. It follows that the GDPR will not apply to all companies that have headquarters in Serbia, but exclusively to those who process personal data of the European Union residents. This paper presents frameworks focusing on the legal and technical aspects that are necessary for the process of synchronizing the company with GDPR. In view of the necessary implementation of technological solutions, the paper presents suggestions for the development of application support that will be applicable during the company's synchronization with GDPR.

KEY WORDS: GDPR regulations, application support, synchronization with GDPR.

1. UVOD

Opšta uredba o zaštiti ličnih podataka (GDPR) definiše propise o zaštiti ličnih podataka fizičkih lica koji su rezidenti Europske unije [1]. Srbija je zemlja u kojoj posluju fizička lica iz Europske unije i ona treba takođe da primenjuje ovu uredbu [4]. Po članku 3, GDPR regulative [5] nastoji se uskladiti zaštita osnovnih prava fizičkih lica u vezi sa aktivnostima obrade ličnih podataka. GDPR uredba primenjuje se na sve organizacije koje prikupljaju ili obrađuju lične podatke pojedinaca rezidenata Europskoj unije, bez obzira na to gde su sedišta pojedinih kompanija. Kompanije će imati obavezu da se usklade sa GDPR regulativom. Pravovremeno pravno, procesno i tehnološko prilagođavanje olakšaće uskladu kompanije sa GDPR. U Srbiji je na snazi Zakon o zaštiti podataka o ličnosti iz 2009. godine [16], koji će se i dalje primenjivati bez obzira što se radi na nacrtu novog zakona o Zaštiti podataka o ličnosti koji bi trebalo da bude usklađen sa GDPR, počevši od maja 2018. godine. Uredba propisuje za slučaj neusklađenosti poslovnih procesa sa ovom direktivom, kaznu u visini do 20 miliona eura ili do 4% ukupnog godišnjeg prihoda za pravna lica [4]. Mogući način usklade sa GDPR uredbom je da kompanija uvede službenika za zaštitu podataka (*Data Protection Officer* - DPO) [5], koji može da bude ili zaposlen u kompaniji ili treće lice iz vanjske agencije. Sve kompanije koje će angažovati DPO službenika za zaštitu podataka imaće jasno definisanu osobu koja će biti odgovorna za usklađivanje rada kompanije sa GDPR-om.

Uloge DPO službenika u kompaniji biće: podizanje svesti zaposlenih o GDPR i o drugim zakonskim, organizacionim, bezbednosnim promenama koje ova regulativa donosi. DPO službenik upoznaće zaposlene sa GDPR regulisanim procesima upravljanja ličnim podacima. Između ostalog, DPO službenik usaglasiće sve procedure upravaljanja sa podacima.

Potrebno je pravovremeno edukovati poslovne subjekte o važnosti implementacije GDPR regulative. Da bi se postigla usklada sa GDPR regulativom potrebno je uskladiti definisati poslovne, organizacione i tehnološke procese. Na lokalnom tržištu manje IT kompanije treba da ponude aplikativna rešenja koja će pomoći velikom broju malih i srednjih kompanija da upravljaju procesom prilagodbe i kasnije da po pravilima GDPR upravljaju svojim poslovnim procesima.

2. PRINCIPI GDPR REGULATIVE

GDPR regulativa obezbeđuje pojedincima veću kontrolu nad ličnim podacima i nameće mnoge obaveze kompanijama koje prikupljaju i analiziraju lične podatke. Regulativa pod privatnim podacima podrazumeva sve one podatke iz kojih se može utvrditi identitet lica, zatim podatke o političkoj, seksualnoj orijentaciji, rasi, imovnom stanju, ali i podaci kao što su istorija pretraga, meta podaci na fajlovima koje je napravilo fizičko lice, a koji mogu da otkriju identitet, podaci o zdravlju, kretanju, navikama. Pod lične podatke podrazumeva se bilo koja kombinacija ličnih činjenica koja tačno određuje jednog pojedinca, to su, između ostalog, ime i prezime, JMBG, podaci o lokaciji,

fizički, fiziološki, genetski, mentalni, ekonomski, socijalni, kulturni ili bilo koji drugi faktori. Na upravljanje ličnim podacima GDPR regulativa temelji se na sledećim principima:

- Potrebna je zakonita i transparentna obrada ličnih podataka rezidenata Evropske unije.
- Prikupljanje ličnih podataka u posebne, tačno određene svrhe. Kompanija ne sme obrađivati podatke na način koji nije u skladu sa navedenom svrhom. Čuvanje samo minimalno potrebnih podataka.
- Kompanija nema ovlašćenje da od pojedinca traži dodatne informacije koje izlaze van definisane svrhe prikupljanja i obrade podataka.
- Kompanija nema ovlašćenje podatke čuvati duže nego što je definisano.
- Potrebno je da kompanija implementira određene sigurnosne mere,
- Lični podaci moraju biti tačni i ažurirani.
- Na adekvatan način potrebno je osigurati odgovorajući nivo sigurnosti ličnih podataka uključujući zaštitu od neovlaštene obrade. Potrebno je obezbediti poverljivost podataka [6].

GDPR regulativa zahteva reviziju poslovnih modela u kompaniji koja svoje robe i usluge nudi fizičkim licima rezidentima Evropske unije. Kompanija koja prikuplja lične podatke pre obrade mora dobiti saglasnost pojedinca za njihovo korišćenje i neophodno je da fizičko lice koje daje saglasnost bude obavešteno o svrsi prikupljanja ličnih podataka [2].

Jedan od jednostavnijih načina prilagodbe kompanije GDPR regulativi je angažovanjem trećih lica – agencije koja imaju pravna i tehnička znanja za bezbednost i zaštitu podataka. Oni će moći da adekvatno i stručno ispune obaveze kompanijama u pogledu efikasne zaštite privatnosti.

3. PRAVA I OBAVEZE SUDIONIKA KOJE PROPISUJE GDPR REGULATIVA

Korisnici i institucije na koje se odnosi GDPR regulativa su: pojedinac (fizičko lice) na kojeg se odnose prava zaštite ličnih podataka definisana GDPR regulativom, kontrolor koji prikuplja lične podatke u cilju ostvarivanja profita, distributer je firma koja vrši obradu ličnih podataka za kontrolora, i nadzorno telo koje vrši proces nadgledanje provođenja regulative [5].

Kontrolor prema pojedincu ima sledeće obaveze:

– Dokazivanje usklađenosti sa GDPR,
– Garantovanje sigurnosti ličnih podatka,
– Definisanje sa distributerom jasna pisana uputstva za obradu ličnih podataka.
– Vođenje evidencije o svim obradama podataka
– Obaveštenje pojedinca o eventualnom kršenju sigurnosti.

Kompanija, kao kontrolor obrade ličnih podataka ima obaveze i prema Nadzornom telu koje će biti zaduženo za sprovođenje GDPR regulative. Kompanija mora da imenuje službenika za zaštitu ličnih podataka i da obavesti Nadzorno telo o provođenju svih potrebnih procesa usklade sa GDPR uredbom. Važno je da kontrolor u slučaju "curenja" podataka obavesti Nadzorno telo u roku od 72 sata od trenutka kada je otkrilo da je došlo do incidenta i kompromitovanja podataka [5].

Kontrolori angažuju distributere i ovlašćuju ih da oni obrađuju lične podatke za njih. Kompanija kao kontrolor u procesu rada sa ličnim podacima treba jasno sa distributerima ugovorom definisati mere sigurnosti koje distributer mora implementirati u svoje poslovne procese obrade ličnih podataka. Distributer može biti treće lice kao poslovni subjekt koji će, na primer, obračunati platu zaposlenima u kompaniji koja je kontrolor, tj. koja prikuplja podatke. Distributer mora da osigura provedbu odgovarajućih tehničkih i organizacionih mera. Njegova dužnost je da izveštava kontrolora o planiranim aktivnostima obrade podataka koja se definiše ugovorom.

Pojedinac ima pravo da od kompanije zatraži detaljne informacije o tome kako čuva lične podatake. Potrebno je da kompanije traži saglasnost pojedinaca za prikupljanje i obradu podataka, tek potpisom pismene saglasnosti pojedinac daje pravo kompaniji da ona može da obrađuje lične podatke. Prava pojedinca su jasno definisana GDPR regulativom i dele se na:

Pravo pristupa – pojedinci mogu tražiti da znaju u koju svrhu se lični podaci obrađuju, mogu da traže uvid u podatke, i da im se predstave metode koje kompanija koristi za proces čuvanja podataka.

Pravo na zaborav – pojedinac, može da zatraži brisanje ličnih podataka koje kompanija vodi o njemu. Međutim neki podaci se ne mogu brisati, jer su vezani nekim drugim zakonskim aktima. Pojedinac može od kompanije tražiti da ga se ne obaveštava, na primer putem mejling liste. U tom slučaju od kompanije se zahteva da se podaci koriste u druge svrhe.

Pravo na ispravku – pojedinac može da traži od kompanije da se njegovi netačni podaci isprave.

Pravo na prenosivost – pojedinci mogu tražiti da kompanija koja obrađuje podatke prenese lične podatke, u sigurnom obliku i sigurnim putem, trećim licima.

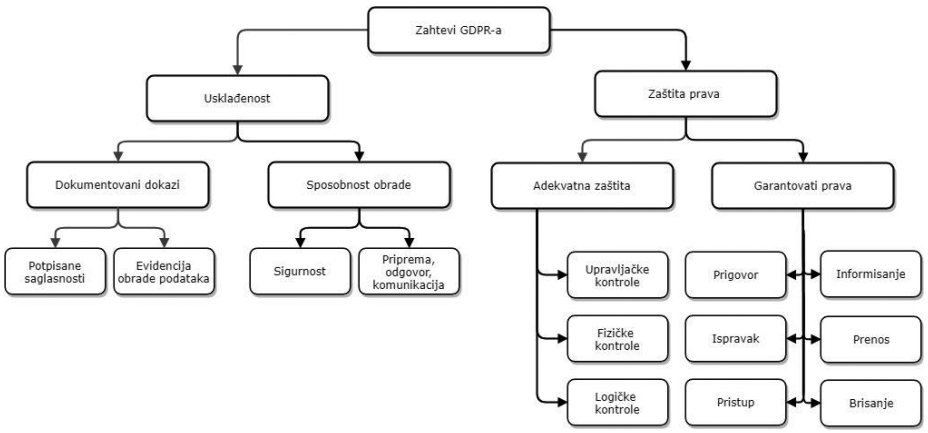
Povreda privatnosti – Ukoliko dođe do "curenja" ličnih podataka, kompanija ima obavezu da u roku od 72 sata od saznanja o incidentu, obavesti fizičko lice.

Pojedinac pre ostvarnje svojih prava, mora potpisati Saglasnost na temelju koje omogućava da kompanija koristi njegove lične podatke. Međutim u slučaju da postoji zakon koji obavezuje davanje podataka ili ugovor između kompanije i pojedinca, to podrazumeva da je fizičko lice već pristalo na korišćenje određenih podataka i u tim slučajevima kompanija ne mora da pribavlja saglasnost pojedinca. Isto tako u slučaju da se podaci nalaze negde javno objavljeni, ni u tom slučaju kompanija ne mora imati potpisanu saglasnost od pojedinca.

4. ZAHTEVI GDPR

Kompanija može internim aktima organizovati uskladu poslovnih procesa sa GDPR regulativom, a DPO službenik vodiće provedbu tih akata. Uredbom je definisana mogućnost izbora, tako da će kompanija moći da imenuje službenika kao osobu koja je već zaposlena u kompaniji ili kao osobu koja će biti zaposlena u vanjskoj agenciji. Službenik će pratiti propise sa kojima će upoznati zaposlene u kompaniji i sprovodiće interne akte tako da im zaposleni pristupe stručno i odgovorno.

DPO Službenik je osoba koja će podići svest zaposlenih da se koliko je to moguće u najvećem meri spreče incidenti.



Slika 1. *Zahevi GDPR regulative [6]*

Sigurnost ličnih podataka zavisiće o angažmanu DPO službenika, tako da kompanija mora dobro da proceni soluciju imenovanja idealne osobe za obavljanje ove dužnosti.

Internim aktima kompanija može da definiše poslovne procese koji će biti usklađeni sa GDPR-om, i tako nad podacima obezbedi korišćenje tehničkih i organizacionih mera, uz obavezno kriptiranje podataka i uz ostale tehničke kategorije. Na slici 1 prikazani su zahtevi GDPR koji se dele na ukupnu usklađenost i zaštitu prava pojedinca. Ukupna usklađenost treba da se dokumentuje dokazima o potpisanim saglasnostima uz evidentiranje svih vrsta obrade podataka. Sposobnosti obrade podataka odnosi se na tehničke komponente sigurnosti u samim procesima obrade podataka. Sa druge strane u segment zaštite prava kompanija treba da vodi brigu o adekvatnoj zaštiti podataka i garantovati prava pojedinca tj. fizičkog lica. Adekvatna zaštita podataka osigurana je upravljačkim i fizičkim kontrolama procesa obrade podataka, dok se prava pojedincima moraju garantovati kroz sistem definisanih mera.

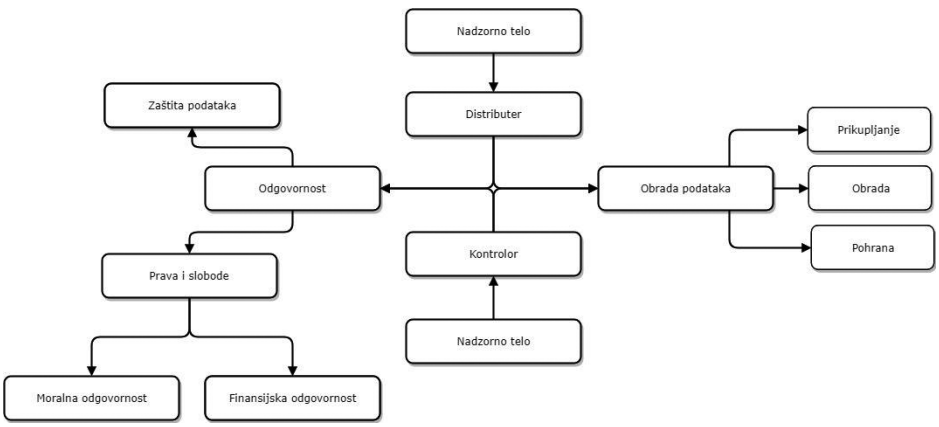
5. UPRAVLJANJE PROCESOM USKLADE PRAVNOG SUBJEKTA SA GDPR UREDBOM

Kao prvi korak usklade kompanije sa GDPR uredbom, predlaže se inventura aktuelnih poslovnih procesa. Nakon toga potrebno je evidentirati poslovne procese po zaposlenima koji ih obavljaju. Kada se tačno evidentiraju procesi po zaposlenima tada će implementacije potrebnih promene poslovnih procesa biti jednosavnija. Poslovne procese definišu se na razini aplikacije koju zaposleni koristi, ali i na razini IT infrastrukture, koja je ključna tačka u pogledu neometanog korišćenja aplikativne podrške. Osim toga, ne treba zaboraviti lične podatke koji se arhiviraju u papirnom obliku, kao na primer – ugovori. Korisno je da kompanija napravi procenu rizika za slučaj narušavanja sigurnosti ličnih podataka [6]. Uz to, potrebno je definisati kontrolne mehanizme koji će se implementirati.

Kada kompanija odredi ove korake, moćiće na osnovu analize rezultata da proceni rizik uz definiciju kontrolnih mehanizama i da uz konsultaciju sa pravnim stručnjacima i stručnjacima za IT sigurnost definiše interne akte. Sa internim aktima DPO službenik mora upoznati sve zaposlene koji će se pridržavati novih poslovnih procesa.

Koristeći interne aktve u slučaju bilo kakvih incidenata ili kontrole od strane nadzornog tela biće vidljivo da kompanija edukuje ljude sa razrađenim postupcima u slučaju incidenta. Na taj način kompanija će ostaviti utisak profesionalnog odnosa prema ličnim podacima koje obrađuje. U slučaju kažnjavanja, činjenica da se zaposleni pridržavaju internim aktima usklađenim sa GDPR, imaće uticaj na smanjenje kazne.

Na slici 2 predstavljen je proces obrade podataka iz perspektive odgovornosti kontrolora i distributera. U internim aktima potrebno je definisati odgovornosti kojih se kontrolori i distributeri moraju pridržavati.



Slika 2. *Odgovornosti sudionika GDPR uredbe [6]*

Nadzorno telo kontroliše rad distributera i kontrolora. U slučaju da se njihova odgovornost prema poslovnim procesima zaštite podatka i odgovornost prema pravima ispitanika neće adekvatno sprovoditi, oni mogu imati moralnu i finansijsku odgovornost. Sa druge starne, njihova odgovornost su i aktivnosti vezane za adekvatno prikupljanje, obradu i pohranu ličnih podatka.

Procesno GDPR ide do najniže razine u strukturi zaposlenih unutar kompanije, do svih zaposlenika koji moraju biti upoznati sa izmenama u poslovnim procesima. Važno je istaći da svi procesi moraju biti podložni promenama, a radnici moraju biti edukovani na nove tehnologije koje će se primenjivati.

Cilj celokupne aktivnosti usklade su višestuke, prvenstevno jer će se stvoriti baza podataka o trenutnim poslovnim procesima i mogućnostima njihovih poboljšanja [18]. Odluka o izboru načina usklade sa GDPR regulativom je na timu kompanije. Postoje više načina da se izvrše procesi usklade. Korisno je usklađu napraviti pomoću pravnih i IT stručnjaka, jer oni će predložiti pravna i optimalna tehnološka rešenja koja će biti primenjiva u procesima usklade kompanioje sa GDPR regulativom.

6. PRIMENA APLIKATIVNE PODRŠKE ZA IMPLEMENTACIJU GDPR-A

Kako bi poboljšali zaštitu ličnih podataka, kompanije će unaprediti svoju IT infrastrukturu, implementirajući potrebne zaštitne mere za proces fizičke kontrole pristupa podacima, pohrani i procesu arhiviranja podatka. Uredba spominje potrebu arhiviranja i evidencije pristupa podacima. To će naveti kompanije da se fokusiranju na procesima zaštite podataka.

Potrebna usklada domaćih kompanija sa GDPR regulativom povećaće zahteve tržišta za specijalizovanom aplikativnom podrškom. Uredba eksplicitno ne navodi koja tehnologija mora biti korišćena za aktivnosti zaštite podataka. Uredba spominje obavezan kontinuiran nadzor nad ličnim podacima i potrebne aktivnosti pretraživanja, upravljanja, zaštite, nadzor nad ličnim podacima i aktivnosti izveštavanja [5].

Tehnologija koja bi pomogla kompanijama u procesu usklade sa GDPR može biti proizvoljna. U Tabeli 1 navedene su aktivnosti usklađenih procesa sa predlogom aplikativne podrške [6].

Aktivnost	Problemi kojeg je potrebno rešiti	Predlog ponude rešenja
Pretraga	Strukturisani i nestrukturisani podaci	Automatizacija - *e-discovery*
	Podaci na serveru	
	Podaci na *Cloud-u*	
	Pretraživanje mejlova	
Upravljanje	Prenos ličnih podataka	Klasifikacija ličnih podataka
	Označavanje podatkovnih medija	
Zaštita ličnih podataka	Ovisno o vrsti korišćenja	Šifriranje podataka
	Ovisno o pretanjama	Maskiranje podataka
Nadzor i izveštavanje	Sistemski zapisi i log fajlovi	*Security Incident & Event Management (SIEM)*
	Curenje poverljivih podataka	

Tabela 1. *Ciklus aktivnosti u radu sa ličnim podacima sa predlogom ponude rešenja [6]*

Prva i osnovna faza implementacije GDPR uredbe je faza pretrage postojećih ličnih podataka. Potrebno je omogućiti pretragu kompetnog opsega ličnih podataka. Uz to, neophodno je odrediti identifikatore koji će jasno definisati lični podatak, kao na primer: ime, prezime, email, adresa, telefon, JMBG i sl. Nakon određivanje ovih identifikatora ličnih podataka, podatke koji će se pretraživati podeliće se na strukturirane i nestrukturirane.

Strukturirani podaci nalaze se u tabelama u kojima su strukturno navedena imena, prezimena, JMBG brojevi i sl. Potrebno je pretražiti kompletne baze podataka da bi se odvojili oni fajlovi koji u sebi imaju strukturirane podatke sa definisanim identifikatorima ličnih podataka. Aplikativna podrška pomoćiće kompanijama da na temelju određenih pravila pretraživanja u što većem procentu pronađu lične podatke.

Kada se podaci odrede, tada ih je potrebno klasifikovati. Lične podatke moguće je označiti po vrsti (strukturirane/nestrukturirane), po tajnosti (javni podaci, tajni podaci). Svaki korisnik baze ličnih podataka treba da dobije pristup ovakvom alatu. On će ručno ili strojno da klasifikuje podatke (datoteke, office dokumente, fotografije, video, audio, email). Klasifikacija podataka omogućiće da se unutar kompanije odrede vrste podataka koje obrađuju poslovni procesi: da li je podatak uopšte lični podatak, da li mu je potrebna enkripcija, digitalni potpis i slično.

Da bi otkrili što veći procenat ličnih podataka koje kompanija ima u svojim bazama podataka, potrebno je definisati – šta sve treba pretraživati. Alat za pretraživanje treba moći pretražiti fotografije, kao važan identifikator ličnih podataka, isto tako i podatke sa društvenih mreža, razne online identifikatore: kao što su korisničke prijave, MAC podaci, i GPS podaci o korisnikovim geolokacijama. Da bi sistem za pretraživanje podataka mogao pronaći veći procenat ličnih podatka, potrebno je definisati veći spektar identifikatora koje GDPR uredba prepoznaje kao lične podatke.

Potrebno je definisati način pretraživanja podataka. Moguće je pretraživati strukturirane podatke u kojima je lakše prepoznati identifikatore kao što su: ime, prezime broj telefona, JMBG i sl. Ti podaci se pronalaze u bazama kao što su računovodstveni ERP sistemi ili sistemi za upravljanje odnosima sa kupcima CRM. Unutar organizacije potrebno je definisati da su i IP i MAC adrese takođe lični podaci. Da bi sistem za pretraživanje mogao da radi i sa takvim podacima, potrebno je primetiti da ovi podaci imaju kontrolne znamenke i po njima se može zaključiti da neki niz brojeva (JMBG, MAC adresa ili sl.) pripada ličnom podatku [6]. Predlaže se korišćenje sistema za strojno učenje (Machine learning), jer oni će samostalno unutar sličnih dokumenata prepoznati da li je nešto specifično za organizaciju. Tako će optimalna aplikativna podrška sistem moći iz velikog broja dokumenata i ugovora prepoznati šta je lični podataka.

Potrebno je koristiti aplikativnu podršku sa mehanizmima za pretragu kako bi kompanija odredila gde se lični podaci nalaze. Potrebno je pretražiti sve hardverske jedinice za pohranu podatka, jer moguće je da se kopije ličnih podataka nalaze na više jedinica za pohranu. Strukturirane podake biće lakše pro-

naći, ali za nestrukturirane podatke potrebno je razviti nove algoritme za pretragu unutar mejlova ili cloud-a.

Aplikativna podrška treba da sadrži mehanizme za izveštavanje. Mehanizmi izveštavanja koristiće se prilikom izrade detaljne analize trenutnog stanja kompanije tokom usklade sa GDPR. Faze izveštavanja biće aktuelna konstantno tokom rada sa ličnim podacima. Na primer, analiziraće se koliko je zahteva došlo od fizičkih lica, za uvid u njegove lične podatke.

Šifriranje	Maskiranje
Promena ličnih podataka u oblik nerazumljiv neovlašćenim licima	Promena ličnih podataka na način oduzimanja atributa identifikacije određene osobe.
Zaštita putem transformacije	Zaštita putem zamene
Reverzibilnost je neophodna	Reverzibilnost može biti potrebna
Matematički algoritam + ključ	Bez matematičkog algoritma (zamena putem određenih pravila)
Neupotrebljivi podaci	Podaci upotrebljivi
Promena veličine podataka	Bez promene veličine podatka
Neupotrebljivo pre dešifrovanja	Iskoristivo za obradu (testiranje, stat. analize)
Korišćenje: zaštita fajlova, mrežni promet	Korišćenje: kada je potrebna daljnja obrada podataka

Tabela 2. *Nadzor i zaštita podataka sa aspekta šifriranja i maskiranja podataka [6]*

Uredba koristi pojmove šifriranja i maskiranja podataka. Metode se razlikuju zavisno o tome šta želimo da radimo sa podacima nakon primene jedne od ovih metoda. Karakteristike ovih metoda prikazane su u Tabeli 2. Šifriranje će pretvoriti podatke u nečitljivi oblik i kao takav, podatak se više neće moći koristiti. Maskiranje kao metoda vrši zamenu podatka koji ostaje čitljiv, ali je netačan. Jedna i druga metoda će postići da podatak gubi sposobnost da identifikuje neku osobu i samim tim koristeći neke od ovih metoda podaci više ne podležu GDPR regulativi. U slučaju da dođe do "curenja" ovih podatka kompanija neće biti dužda da obaveštava nadzorno telo u roku 72 sata.

Maskiranje se koristi kada se želi obavljati daljnju obradu nad ličnim podacima. Podaci će biti prepoznatljivi kao lični podaci, ali neće biti tačni.

Procese zaštite podataka i kontrolu pristupa podacima GDPR uredba spominju kao obavezne. Drugim rečima, tehnička zaštita podataka mora biti implementirana i mora se evidentirati svaki pristup podacima. S obzirom da većina kompanija nemaju IT infrastrukturu sa ovakvim funkcionalnostima, potrebno je da IT firme tržištu ponude optimalnu aplikativnu podršku. To su centralizovana rešenja koja prikupljaju sistemske zapise logove iz baza podataka svih podatkovnih repozitorija koje koristi kompanija. U tu svrhu može da se koristi *Security incidente & Event managemetnt (SIEM)* rešenje. To je tehnološki termin koji je prepoznat u finansijskom sektoru, ali očito je sada potrebno proširiti opseg njegovog korišćenja na manje firme različitih delatnosti. Nije za očekivati da će manje firme moći implementirati rešenja koja su namenjena velikim firmama. Stoga je potrebno da IT firme prepoznaju potrebu razvoja aplikativne podrške i u ovom segmentu.

Osobni računari i pametni uređaji takođe trebaju proći nivo zaštite, jer i oni se konektuju na IT infrastrukturu. Da li preko enkriptiranih podatka ili putem VPN-a osobni računari i pametni telefoni biće sastavni deo IT infrastrukture koja će biti podložna GDPR uredbi. U tabeli 3 su prikazane aplikativne podrške koje će biti potrebno ponuditi kompanijama i tako pomoći proces njihove usklade sa sa GDPR regulativom.

Prevencija	Enkripcija i maskiranje podataka
	Upravljanje update-ovima softvera
	Sistem identifikacije i sigurne prijave u sistem
	Testiranje sigurnosti sistema
Konstantna upotreba	Secure mail, Web gateway
	Anti-malware rešenja
Detekcija i korekcija	Analiza DNS prometa
	Upravljanje logovima sistema (SIEM)

Tabela 3. *Konstantne aktivnosti zaštite podataka unutar kompanije [6]*

Kompletna usklada pravnog subjekta sa GDPR zahteva uskladu svih postojećih poslovnih procesa. Kako bi se maksimalno osigurali podaci tokom procesa usklade, proces može da se obavlja postupno kroz transfer jednog po jednog poslovnog podsistema i može biti fokusiran na određeni broj ključnih procesa [8]. Strukturirani pristup procesu usklade može pomoći kompaniji da standardizuje i automatizuje svoje poslovne procese i da poveća efikasnost svojih zaposlenih kroz efikasnije poslovne procese. Osim što može sačuvati vreme i smanjiti troškove usklade, integrisani pristup upravljanja poslovnim procesima može da obezbedi da zaposleni rade na istim podacima i upravljaju procesima na osnovu istih indikatora [9]. Korisnici baze podataka koje službenik treba da osposobi za rad sa ličnim podacima su: administratori, dizajneri i krajni korisnici [10].

U domeni rada sa procesima postoje različiti sistemi i alati koji mogu da usklade procese sa određenim promenama. U tu svrhu moguće je koristiti *Process mining* koncept, koji iako pripada relativno mladoj istraživačkoj disciplini može pomoći u cilju otkrivanja, posmaranja i poboljšanja stvarnih poslovnih procesa. *Process mining* podrazumeva automatizovano otkrivanje neusklađenih procesa, proveru odstupanja od uobičajenog ponašanja korisnika, proširivanje i popravku tih modela [11]. *Process mining* se najčešće koristi za kreiranje optimalne veze između procesa i podatka koje oni kreiraju [9] i kao takav može da pomogne boljem analiziranju toka ličnih podataka u kompaniji.

Unutar kompanije posluju različita ERP rešenja koja pomažu korisnicima kontrolisati funkcionisanje kompanije. ERP sistemi obrađuju podatke za samo izvršenje poslovnih proce-

sa i čuvaju zapise *(logove)* o izvršenim aktivnostima. Analiziranje ovakvih zapisa daje uvid u način izvršavanja procesa i može poslužiti za prikazivanje razlike između planiranih (GDPR usklađenih) i aktuelnih procesa. Koncept *process mininga* može da se primeni nad zapisima događaja (*event logs*) iz poslovanja informacionih sistema. Međutim u poslovnim sistemima, podaci koji se odnose na poslovne procese čuvaju se u često ne direktno povezanim tabelama. Ova činjenica predstavlja izazov za istraživače budući da je za primenu *process mining* potrebno prevesti nestrukturirane u strukturirane podatke [12].

7. ZAKLJUČAK

Implementatori aplikativne podrške imaće procedure za uskladu sa GDPR regulativom. Međutim, od korisnika će zahtevati jasno definisanje promena poslovnih procesa. Kompanije moraju biti svesne da IT firme neće preuzimati rizik i odgovornost na sebe. IT firme polaziće od pretpostavki da izbegavaju preuzimanje rizika zbog velikih kazni i zbog često nejasnih tačaka unutar GDPR regulative.

IT firme implementaciju aplikativne podrške radiće po primljenim zahtevima od klijenata i na taj način izbeći će rizik koji se odnosi na GDPR regulativu. Stoga je važno da menadžeri kompanija prođu potrebne obuke kako bi se osposobili za implementaciju usklade sa GDPR regulativom. IT firma koja razvija aplikativnu podršku, mora biti svesna da njeni klijenti podležu GDPR i da sama činjenica da kompanije koriste njihovu aplikativna podršku za unos ličnih podataka, stvara i njima obavezu usklade sa GDPR regulativom.

Neki od principa kojih se mora pridržavati aplikativna podrška su: potrebno je u aplikativnu podršku implementirati potrebne postavke za zaštitu ličnih podataka kao i mogućnosti kompetnog brisanja ličnih podataka. Potrebno je da se svi interfejsi prema trećim sistemima usklade sa pravilima zaštite ličnih podataka. Potrebno je pojednostaviti procese izmene ličnih podataka kupaca, na način da se sa jednog mesta izmena reflektuje na svim mestima u bazama podataka kompanije. Potrebno je u aplikaciji ponuditi štampanje Saglasnosti koje će ispitanici potpisati. Menja se i proces logovanja korisnika u sistem. Važno je da svaki korisnik pristupa sistemu sa svojim prepoznatljivom korisničkom prijavom koju isključivo samo on koristi.

Velike IT firme uskladile su svoje aplikacija sa GDPR-om. *SAP* je procenio potrebu imlementacije novih procedura u svoj *SAP SuccessFactors HCM Suitea*. SAP je uzeo u obzir da će za usklađenost sa GDPR-om morati posebno evidentirati lične podatke zaposlenika komapnije koje uključuje: lične podatke, bankovne podatke, podatke o ljudskim resursima, kvalifikaciju zaposlenih, detalje o obrazovanju, podatke o visini plate i podatke o socijalnoj sigurnosti, o svim detaljima pristupa sistemu od zaposlenog, kao i sva njegova ovlašćenja u sistemu. Ovaj će paket biti postavljen u *SAP Cloudu*, uz maksimalnu sigurnost podataka koji će se kriptirati.

Oracle je primetio da će usklađenost sa GDPR-a zahtevati koordinaciju mnogih entiteta organizacije, kao što su: pravni, kadrovski resursi, marketing, sigurnost i IT. Biće potrebno analizirati mnoge tačke u IT infrastrukturi da bi se pronašli lični podaci, kao što su: nestrukturirani podaci, različite vrste fajlova, MAC ili IP adrese i metapodaci. Iz *Oracle* saznajemo da će biti potrebno poboljšati sigurnosne kontrole [7].

LITERATURA

[1] GDPR portal: *Site Overview. This website is a resource to educate the public about the main elements of the General Data Protection Regulation* (GDPR), 2018. https://www.eugdpr.org/

[2] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* 1995. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en

[3] *Data Protection Act*, 1998. https://www.legislation.gov.uk/ukpga/1998/29/contents

[4] *Uredba (EU) 2016/679 Evropskog Parlamenta i Saveta od 27. aprila, 2016. o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i o slobodnom kretanju takvih podataka i o stavljanju Direktive 95/46/EZ van snage.* (Opšta uredba o zaštiti podataka) 2016. http://esigurnost.org/wp-content/uploads/2018/01/GDPR-Uredba-2016.679.pdf

[5] *EU General Data Protection Regulation* (EU-GDPR) 2018. http://www.privacy-regulation.eu/

[6] Marinković, N., Kladar, D., Kleković, I.: "*Webinar: Jeste li usklađeni sa GDPR-om*" 2018. https://www.youtube.com/watch?v=RD7TW5_6wOY&

[7] Paul Sheldon Foote and Sumantra Chakravarty: *"EU GDPR biometric compliance systems"*, 21.03.2018. https://www.biometricupdate.com/201803/eu-gdpr-biometric-compliance-systems

[8] Anne N. Parr, Graeme Shank, *A Taxonomy of ERP Implementation Approaches, Proceedings of the 33rd Hawaii International Conference on System Sciences*, 2000.

[9] Malić, J., Pantelić, O., Pajić, A., *Analiza modela podatka sistema "MS NAV" na primeru procesa nabavke*", InfoM, ISSN 1451-4397, str. 38-46. br 64/2017 .

[10] Ramez Elmasri, Shamkant B. Navathe: *Fundamentals of database systems*, Addison-Wesley, 2011.

[11] Rafael Accorsi, Ernesto Damiani, Wil M.P. van der Aalst: *Unleasing Operational Process Mining*, Izveštaj sa Dagstuhl seminara, 2013.

[12] Ana Pajić, Dragana Bečejski-Vujaklija, *Metalodel of the Artifact-Centric Approach to Event Log Ectraction from ERP Systems*, International Journal to Decision Support System Technology, 2016.

Nenad Badovinac, student doktorskih studija, Fakultet organizacionih nauka, Univerzitet u Beogradu
Kontakt: nenad.badovinac@gmail.com
Oblasti interesovanja: biometrijski sistemi, e-payment, DMS (dealership management system)