



Branko Pavlović,
član Izvršnog
odбора Generali
osiguranja i
predsednik
Udruženja
aktuara Srbije

■ **Izdvađa se nekoliko osobina GDPR-a, koje će implementaciju prilično zakomplikovati. Uvodi se pravo klijenta da potpuno kontroliše prava pristupa svojim ličnim podacima i da zahteva potpuno brisanje podataka o njemu iz svih evidencija i informacionog sistema kompanije. Osiguravajuće kompanije u EU su naročito zabrinute zbog toga što buduće detaljne kontrole njihovih internih poslova i postupanja sa klijentima i poslovnim partnerima mogu da dovedu do toga da plate visoke kazne ako se otkriju nedostaci po pitanju zaštite ličnih podataka**

Opšta uredba o zaštiti podataka o ličnosti (engl. General Data Protection Regulation = GDPR), koja će se neposredno primenjivati na sve države članice Evropske unije od 25. maja 2018. godine, detaljno je regulisala pravo na zaštitu podataka o ličnosti. To ima dvostruki efekat: s jedne strane fizičkim licima daje punu kontrolu nad njihovim ličnim podacima u svakoj fazi obrade podataka, a s druge bi moglo da ima veliki uticaj na

Ima li osiguranja od nove regulative?

nove poslovne mogućnosti za pojedine kompanije. Novi režim zaštite podataka proširuje opseg zakona o zaštiti podataka i na sve strane firme koje se bave obradom podataka stanovnika EU i pruža okvir za usklađivanje propisa o zaštiti podataka u celoj Evropskoj uniji. Takođe, primenjivaće se i na domaće kompanije koje pripadaju grupama u Evropskoj uniji. Važiće za sva pravna lica, uključujući osiguravajuće kompanije.

Tri glavne institucije EU - Evropski parlament, Savet Evropske unije i Evropska komisija, sredinom 2015. godine, započele su pregovore o predloženoj Opštoj uredbi o zaštiti podataka, postupak poznat kao neformalni trijalog. Osnovu za trijalog činile su predlog Komisije iz januara 2012. godine, zakonodavna rezolucija Parlamenta iz marta 2014. i opšti principi Saveta usvojeni u junu 2015. godine. Tri institucije obavezale su se da će postupati prema GDPR-u kao delu šireg paketa reformi u području zaštite podataka koji uključuje predloženu direktivu za policijske i pravosudne delatnosti. Proces je zaključen formalnim donošenjem Uredbe u aprilu 2016. godine, nakon čega je određen dvogodišnji prelazni period.

Evropski regulator je ovom Uredbom promenio pristup - umesto popravljavanja štete nastale usled zloupotrebe ličnih podataka (Direktiva 95/46/EC), sada se preventivno štite osnovna prava i slobode klijenata. Nova Uredba obavezuje kompanije da primenjuju mere usmerene na zaštitu ličnih podataka klijenata i da garantuju efikasnost bezbednosnih mera za zaštitu ličnih podataka. To između ostalog omogućava uvođenje principa koji treba da podstaknu obradu ličnih podataka, odgovornog lica za zaštitu podataka, procene uticaja zaštite podataka i niz prava koja su data klijentima tokom obrade njihovih podataka.

Izdvađa se nekoliko osobina GDPR-a, koje će implementaciju prilično zakomplikovati. Uvodi se pravo klijenta da potpuno kontroliše prava pristupa svojim ličnim podacima i da zahteva potpuno brisanje podataka o njemu iz svih evidencija i informacionog sistema kompanije. Ovo pravo obećava puno dodatnog posla za advokate, koji već imaju puno posla u procesima protiv osiguravajućih kompanija. Dalje, u slučaju neovlašćenog pristupa ličnim

podacima klijenata, kompanija je dužna da obavesti nadzorni organ o tome u roku od 72 sata, što može da značajno naškodi reputaciji kompanije na tržištu. Na kraju, koncept odgovornosti je suština GDPR-a, i po njemu kompanija koja prikuplja lične podatke mora da dokaže da poštuje GDPR.

Osiguravajuće kompanije u EU su naročito zabrinute zbog toga što buduće detaljne kontrole njihovih internih poslova i postupanja sa klijentima i poslovnim partnerima mogu da dovedu do toga da plate visoke kazne ako se otkriju nedostaci po pitanju zaštite ličnih podataka koje su propisane do nivoa od 4 % prometa kompanije na globalnom nivou, ali ne manje od 20 miliona evra. Pojedine zemlje članice EU su u svoja zakonodavstva uvrstila novčane kazne do čak 5 % globalnog prometa. Zloupotreba ličnih podataka može imati i značajne posledice po ugled kompanije. Domaće zakonodavstvo za sada ne predviđa takve kazne, ali kršenje GDPR regulative u Srbiji u kompaniji koja pripada grupi iz Evropske unije može skupo koštati celu grupu. Takve kompanije treba da budu usklađene sa opisanom regulativom Evropske unije, ali i da ispunе sve zahteve domaćeg aktuelnog Zakona o informacionoj bezbednosti.

Ipak, za kompanije koje ga budu dosledno poštovalе, GDPR može biti dobra prilika da se dođe do novih klijenata s obzirom na to da će oni pre odabrati osiguravače koji pružaju bolju zaštitu ličnih podataka. Pored toga, na duži rok posmatrano, revidiranje politika i internih procesa dovelaće do dodatne operativne efikasnosti i smanjenja troškova, posle inicijalnog povećanja troškova zbog implementacije nove regulative, naravno. U velikim sistemima, zbog složenosti, očekuje da će se implementacija GDPR pretvoriti u kompleksne projekte čija će se vrednost meriti u milionima evra. Za male i srednje kompanije usklađivanje sa novom regulativom će koštati između 10 i 50 hiljada evra u prvoj godini, u slučaju korišćenja ključnog rešenja koja se već mogu naći na tržištu. Kada/ako Srbija postane članica EU, preko 100.000 pravnih lica će morati da primeni GDPR. Jednostavna računica kaže da će ukupni trošak usklađivanja za sve kompanije biti preko 2 milijarde evra. Bilo bi lepo kad bi to pokrilo neko osiguranje... ■

