



Branko Pavlović, predsednik Udruženja aktuara Srbije

■ **Otežavajuća okolnost za aktuarske analize predstavlja novo pravilo da osiguranik može da traži da se obrišu njegovi podaci, tj. da bude "zaboravljen" kada se završe međusobne obaveze iz ugovora o osiguranju. Dodatni izazovi se javljaju u vezi korišćenja ličnih podataka koji mogu dovesti do diskriminacije u određivanju cene rizika po pitanju pola, rase, religije**

Mogu li aktuari bez ličnih podataka osiguranika?

O pšta uredba o zaštiti podataka o ličnosti (engl. General Data Protection Regulation = GDPR), koja se primenjuje u svim državama članicama Evropske unije od 25. maja 2018. godine, detaljno je regulisala pravo na zaštitu podataka o ličnosti. Menja se način na koji kompanije rukuju ličnim podacima korisnika, uvode se nova pravila za korišćenje i brisanje ličnih podataka i uvodi davanje saglasnosti korisnika za obradu podataka.

Poznato je da se svi aktuarski obračuni zasnivaju na statističkim podacima, odnosno da su aktuari najveći korisnici podataka u osiguravajućoj kompaniji. GDPR zahteva od aktuara da promene način na koji čuvaju, obrađuju i modeliraju lične podatke. Otežavajuća okolnost za aktuarske analize predstavlja novo pravilo da osiguranik može da traži da se obrišu njegovi podaci, tj. da bude "zaboravljen" kada se završe međusobne obaveze iz ugovora o osiguranju. Dodatni izazovi se javljaju u vezi korišćenja ličnih podataka koji mogu dovesti do diskriminacije u određivanju cene rizika po pitanju pola, rase, religije, itd. U principu je zabranjena obrada takvih podataka, osim ukoliko je osoba dala eksplicitni pristanak na to, što dodatno komplikuje aktuarske poslove.

Evropsko udruženje aktuara (engl. Actuarial Association of Europe) je objavilo dokument o GDPR-u, u kome savetuje aktuare kako da postupaju u skladu sa novim regulatornim okvirom. Preporučuju se sledeći postupci:

1. Popis ličnih podataka u bazama sa kojima aktuar radi

Važno je prvo pažljivo identifikovati sve lične podatke osiguranika koje poseduje, a zatim definisati i da li je svaki od njih zaista potreban za analizu. Ukoliko nisu neophodni, najbolje ih je izbrisati i tražiti od kompanije da ne dostavlja više te delove baza.

2. Pribavljanje dozvole za obradu ličnih podataka

Ukoliko su lični podaci neophodni za konkretne analize, potrebno je pribaviti formalnu dozvolu za rad sa ličnim podacima osiguranika. Najbolje je obezbediti takvu dozvolu od nadležne funkcije za zaštitu podataka u kompaniji koju uvodi GDPR.

3. Gep analiza

Potrebno je napraviti gep analizu za utvrđivanje da li ima razlike između propisanog rada sa ličnim podacima u GDPR uredbi i rukovanja podacima koje aktuar

sprovodi u praksi. U slučaju utvrđenih razlika potrebno je zajedno sa osiguravajućom kompanijom revidirati procese pristupa i obrade ličnih podataka osiguranika.

4. Dokumentacija

Osiguravači imaju pravo da znaju šta konkretno aktuari rade sa ličnim podacima njihovih osiguranika, pa je potrebno da aktuari obezbede dokumentaciju u kojoj se to jasno vidi, i gde je objašnjena svrha svake takve obrade.

GDPR nudi mogućnost anonimizacije ličnih podataka, odnosno promene određenih podataka u bazi tako da se na osnovu preostalih originalnih podataka ne može identifikovati o kojoj osobi se radi. To je prihvatljivo rešenje za aktuarske analize, jer GDPR ne ograničava ni na koji način korišćenje anonimiziranih podataka. Na žalost, retko koja kompanija ima anonimizirane podatke koje može da ponudi aktuarima. Obično aktuari dobiju kompletne baze u kojima se nalaze imena, JMBG, adrese, itd. Naravno, proces anonimizacije ne treba da rade aktuari, ali mogu da pokušaju da se dogovore sa osiguravačem da dobijaju anonimizirane podatke, i ako uspeju ne moraju da brinu o GDPR-u.

Pored anonimizacije koja je nepovratan proces ukidanja veze između originalnih i anonimiziranih podataka, postoji i pseudoanonimizacija. To je proces u kome se menjaju određeni podaci u bazi, tako da se na osnovu preostalih originalnih podataka ne može identifikovati o kojoj osobi se radi, bez dodatnih šifarnika koji se drže odvojeno od pseudoanonimizirane baze podataka. S obzirom da je osiguravajuće kompanije mnogo lakše ubediti da izvrše pseudoanonimizaciju baze, jer u slučaju da im treba uvek mogu da vrate originalne podatke, za aktuarske analize je to kompromisno rešenje potpuno prihvatljivo, pod uslovom da ne dobiju i šifarnike od kompanije.

Nedostaci po pitanju obrade ličnih podataka, koju vrši bilo ko u kompaniji, uključujući aktuare, mogu da dovedu do toga da osiguravajuće kompanije u EU plate kazne koje su propisane do nivoa od 4% prihoda kompanije, ali ne manje od 20 miliona evra. Domaće zakonodavstvo za sada ne predviđa tako drastične kazne kao GDPR, ali kad se uskoro usvoji Zakon o informacionoj bezbednosti, aktuari koji rade za osiguravajuće kompanije u Srbiji, moraću da ispune sve zahteve iz zakona koji će biti prilično usklađen sa GDPR-om. ■

