Uloga Agencije za zaštitu osobnih podataka kao nadzornog tijela u provedbi Opće uredbe o zaštiti podataka

Marija Pušić, Igor Vulje

Agencija za zaštitu osobnih podataka, Zagreb

Opća uredba o zaštiti podataka

Opća uredba o zaštiti podataka (u daljnjem tekstu Uredba) u cijelosti je obvezujuća i primjenjuje se izravno u svim državama članicama od 25. svibnja 2018. godine. Njezine odredbe moraju poštivati svi subjekti koji u sklopu svojih aktivnosti obrađuju osobne podatke fizičkih osoba u Europskoj uniji te u određenim slučajevima i subjekti izvan Europske unije. Dakle, iznimaka u smislu dodatnog perioda prilagodbe nema.

Uredba (General Data Protection Regulation – GDPR) se primjenjuje na sve tvrtke i tu nema iznimaka. Također se primjenjuje i na pojedince koji obavljaju određenu profesionalnu aktivnost, udruge, bolnice, klubove pa i na fizičke osobe kada obrađuju osobne podatke izvan okvira potreba kućanstva (npr. postavljanje video nadzora ispred ulaznih vrata kuće ili stana). Uredba se primjenjuje na sve državne institucije koje su dužne obrađivati osobne podatke u okviru svojih odredaba, osim u slučajevima kaznenopravnih aktivnosti poput sprečavanja kaznenih djela ili progona počinitelja tih djela te u područjima izvan nadležnosti prava EU-a.

Što se konkretno tiče zdravstvenog sektora i sustava zaštite u tom sektoru, nezaobilazno je naglasiti kako upravo Republika Hrvatska ima jedan od razvijenijih digitalnih zdravstvenih sustava, što svakako ima svoje prednosti, ali ostaje za utvrditi odgovaraju li sustavi pravnim, i tehničkim uvjetima, odnosno odredbama koje modernizacija zakonodavstva donosi. Budući da zdravstveni sustav (bolnice, klinike, laboratoriji, domovi zdravlja, zdravstveno osiguranje, liječnici opće medicine, stomatolozi te svi drugi subjekti) u velikoj, ako ne i najvećoj mjeri, zapravo obrađuje posebne kategorije osobnih podataka, konkretno podatke o zdravlju, nužno je da se Uredba u potpunosti ozbiljno shvati, da odgovorne osobe u ovim poslovnim subjektima što prije započnu s ulaganjima u svoj vlastiti sustav zaštite podataka. S aspekta obrade osobnih podataka nije isto bavi li se poduzeće kliničkim ispitivanjima, odnosno laboratorijskim analizama, kreditiranjem građana ili se bavi ugostiteljstvom ili pekarstvom. Također, nije isto ima li poduzeće program vjernosti za praćenje navika kupaca ili sustav nadzora zaposlenika. Sasvim je jasno da implementacija Uredbe nosi i određene troškove koji variraju i nemoguće je govoriti o jedinstvenim, odnosno jednakim troškovima, ali ono što je sigurno - prvo ulaganje je ono vremensko, točnije, upoznavanje sa samim propisom.

Ovlasti nadzornog tijela

U Republici Hrvatskoj kao nadzorno tijelo uspostavljena je Agencija za zaštitu osobnih podataka (AZOP). Među ostalim zadaćama, nadzorno tijelo prati i provodi primjenu Uredbe, promiče javnu svijest o pravilima, rizicima, zaštitnim mjerama i pravima u vezi s obradom te njihovo razumijevanje. Također promiče osviještenost voditelja obrade i izvršitelja obrade o njihovim obvezama, savjetuje Sabor, vladu i druga tijela o zakonodavnim i administrativnim mjerama u vezi s obradom podataka, rješava i istražuje pritužbe te podnositelja pritužbe izvješćuje o napretku i ishodu istrage. Surađuje s nadzornim tijelima drugih država članica EU-a s ciljem osiguranja konzistentnosti primjene i provedbe Opće uredbe o zaštiti podataka te sudjeluje u radu Europskog odbora za zaštitu podataka i prati razvoj u onoj mjeri u kojoj on utječe na zaštitu osobnih podataka - osobito razvoj informacijskih i komunikacijskih

tehnologija te komercijalnih praksi. Što se tiče ovlasti regulatora prilikom obavljanja zadaća oni mogu:

- izdati upozorenja i službene opomene voditelju obrade ili izvršitelju obrade,
- naložiti voditelju obrade ili izvršitelju obrade da poštuje zahtjeve ispitanika za ostvarivanje njegovih prava i da postupke obrade uskladi s odredbama Uredbe o zaštiti podataka,
- privremeno ili konačno ograničavati i zabraniti obradu podataka, pa i iznošenje podataka u treće zemlje, a u skladu s nacionalnim pravom, izreći upravnu novčanu kaznu.

Što se tiče nadzora obrade osobnih podataka i utjecaja Uredbe na ovlasti nadzornog tijela, one su proširene na istražne, korektivne i savjetodavne. Uvode se izričita pravila o obveznoj međusobnoj pomoći između tijela nadležnih za zaštitu osobnih podataka. Uvode se i mehanizmi koji propisuju ujednačeno postupanje koji obuhvaćaju više država članica, pri čemu se određuje i način postupanja prilikom rješavanja slučaja s međunarodnim elementima.

Uredbom je propisana i obveza tijela nadležnih za zaštitu osobnih podataka da budu ovlaštena za izricanje novčanih upravnih kazni osim ako pravnim sustavom države članice nisu predviđene novčane upravne kazne (to je slučaj s Danskom i Estonijom). Utvrđena su mjerila za utvrđivanje kazni kao i sama svrha tih kazni. To predstavlja bitnu novinu u odnosu na postojeći hrvatski Zakon o zaštiti osobnih podataka te će se u tom smislu morati poduzeti odgovarajuće zakonodavne promjene na nacionalnoj razini, u prvom redu odnosne na postupovne odredbe. Materijalne odredbe predviđene su Uredbom i na njih se ne može utjecati.

Što se tiče izricanja *upravnih novčanih kazni* napominjemo kako postoje dvije skupine povreda. Za jednu skupinu povreda Uredbom je propisana maksimalna kazna u iznosu od 10 milijuna eura ili 2% godišnjeg prometa na svjetskoj razini, a za drugu skupinu propisana je maksimalna kazna do 20 milijuna eura ili 4% godišnjeg prometa na svjetskoj razini, ovisno o tomu što je veće.

Minimalna kazna nije utvrđena, a što se tiče samog kažnjavanja, tijela za zaštitu osobnih podataka iz Europske unije donijet će odgovarajuće smjernice za ujednačenu primjenu kazni. Ono što je ključno, uloga regulatora (čitaj: AZOP) nije da svakom poslovnom subjektu nudi i/ili predlaže gotova rješenja jer *jedinstveno rješenje ne postoji*. Svaki poslovni subjekt ima svoje specifičnosti, a dužan je u okviru svog djelovanja uskladiti svoje poslovanje s Uredbom. Među ostalim, treba utvrditi:

- koje sustave pohrane ima,
- koja je pravna svrha za obradu,
- koliki je rok čuvanja podataka,
- zakonitost iznošenja u treće zemlje,
- prosljeđuju li se ti podaci trećim osobama i temeljem koje zakonske osnove,
- tko ima pristup tim podacima,
- jesu li tehničke mjere sigurnosti u skladu s čl. 32. Uredbe i drugim povezanim člancima i posebnim propisima.

Zaključak

Jedinstveni materijalni propis, eks-teritorijalna primjena, jasno utvrđene nadležnosti različitih nadzornih tijela u prekograničnim situacijama, pristup koji se temelji na rizičnosti i ukidanje administrativnih tereta te uspostavljanje krovnog europskog tijela, neke su od novosti Opće uredbe o zaštiti podataka koje utječu na sve dionike obrade podataka pa tako i na nadzorna tijela.

U tom smislu, proširuju se obveze nadzornih tijela, a jedna od posljedica je da će nadzorna tijela svoje resurse morati usmjeriti na nadzor rizičnih obrada. To je primjerice razvidno iz postupka prethodnog savjetovanja i povezane procjene učinka, izvješćivanja o povredama podataka (engl. *data breach*) te prilikom iznošenja podataka u treće zemlje.

Isto tako je nesporno da Opća uredba o zaštiti podataka propisujući opću nužnost izricanja upravnih novčanih kazni ostavlja vrlo malo mjesta za nekažnjavanje povreda što će zasigurno dovesti do vidnog povećanja angažmana nadzornih tijela u sudskim postupcima. Također, novim ili jačim pravilima bit će obuhvaćene one djelatnosti koje se bave obradom osobnih podataka visokog rizika u što svakako spada i zdravstveni sektor, odnosno obrade posebnih kategorija osobnih podataka, za koje će biti potrebno provesti procjenu učinka. To su obrade koje se odnose na sustavnu i opsežnu procjenu osobnih aspekata pojedinaca automatiziranim putem, opsežnu obradu posebnih kategorija podataka ili podataka o kaznenim osudama ili kažnjivim djelima te sustavno praćenje javno dostupnog područja u velikoj mjeri.