MAJA ŠUTALO, odvjetnica

GDPR - OPĆA UREDBA O ZAŠTITI PODATAKA I OBVEZE POSREDNIKA U PROMETU NEKRETNINA

Malo koji od nacionalnih i europskih propisa je izazvao toliko kontroverzi kao Opća uredba o zaštiti podataka[1] (eng. *General Data Protection Regulation*, dalje u tekstu "GDPR"). Međutim, malo je poznato da je i nacionalno i europsko zakonodavstvo poznavalo pravila zaštite osobnih podataka još od devedesetih godina prošlog stoljeća. Štoviše, najveći broj načela sadržanih u GDPR-u je postojao i prije, a GDPR uvodi dvije znatne novosti:

- GDPR se primjenjuje izravno na području cijele Europske unije čime se postigao efekt ujednačenosti za razliku od prethodnog sustava u kojem je EU postavila samo ciljeve zaštite osobnih podataka, a na nacionalnim zakonodavstvima je bilo da konkretna pravila urede u skladu s tim ciljevima na način kako žele.
- GDPR predviđa iznimno visoke gornje granice kazni za nepoštivanje pravila i ta gornja granica je ujednačena za cijelo područje EU.

Kao posljedica iznimno visokih kazni i globalne primjenjivosti, najčešće komunicirani aspekt GDPR-a je upravo visina sankcija koja svojom rigoroznošću može uništiti poslovanje, a pogotovo poslovanje malih poduzetnika. Nažalost, manje eksponirani aspekti GDPR-a su vrijednosti koje stoje iza tako stroge zaštite. U takvoj atmosferi su, također nažalost, često nejasno komunicirana i nedovoljno shvaćena temeljna načela zaštite osobnih podataka i temeljne obveze koje poslovni subjekti moraju poštivati u okviru svakodnevnog poslovanja.

ŠTO NAM GOVORE TEMELJNA NAČELA I ŠTO TO ZNAČI U PRAKSI?

Svrha GDPR-a nije blokirati ni ograničavati poslovanje. Svrha je izbjeći manipuliranje osobnim podacima i u okviru poslovanja osvijestiti koje podatke je zbilja potrebno prikupljati, u koju svrhu, kome ih je u redu prenositi, a kome ih nije u redu odavati, uspostaviti interna pravila zaštite osobnih podataka u poslovanju te o svim bitnim okolnostima obavijestiti ispitanika samoinicijativno ili na njegov zahtjev, ovisno o slučaju.

Drugim riječima, ponašati se prema tuđim osobnim podacima kao prema vlasništvu te osobe, a ne kao prema svojem vlasništvu.

[1] puni naziv: Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46 EZ (Opća uredba o zaštiti podataka)

Kad bi se GDPR trebao sažeti u tri riječi, to bi bile transparentnost, neinvazivnost i sigurnost.

Transparentnost je vrlo jednostavna: ispitanik mora biti obaviješten tko prikuplja njegove podatke, u koju svrhu, na kojoj pravnoj osnovi, koliko dugo, kome ih prenosi, prenosi li ih izvan EU i slično. U praksi je načelo transparentnosti često zabludom zamijenjeno za ishođenje privole i baratanje privolama na nezakonit, ali i poslovno nelogičan način što je detaljnije objašnjeno u nastavku ovog članka.

Neinvazivnost jednostavnim rječnikom znači da se ne smije prikupljati i prenositi više osobnih podataka nego što je potrebno da se ispuni određena svrha. U radu agencija za posredovanje u prometu nekretnina ova obveza dolazi do izražaja kod fotografiranja nekretnina prilikom čega bi bilo poželjno izbjegavati fotografiranje nacionalnih i/ili vjerskih simbola vidljivih u prostoru jer se na taj način, najčešće nesvjesno, prikupljaju podaci o nacionalnoj i/ili vjerskoj pripadnosti vlasnika nekretnine koji predstavljaju posebnu kategoriju osobnih podataka, a istovremeno obrada tih podataka nije potrebna da bi se nekretnina mogla prodati, iznajmiti ili dati u zakup.

Sigurnost znači da su poduzete odgovarajuće mjere da se podaci zaštite od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja. Sigurnosne mjere ovise o tome na koji način poslovni subjekt organizira svoje poslovanje, a u svakom slučaju se u redovnom tijeku poslovanja odnosi na pravilno održavanje informatičkog sustava u kojem se pohranjuju osobni podaci, upotrebu lozinki i sl., a u određenim situacijama, kad se prikupljaju osjetljivi podaci ili posebne kategorije osobnih podataka (što najčešće nije riječ kod poslovanja posrednika u prometu nekretnina), sigurnost se postiže pseudonimizacijom i/ili enkripcijom. O sigurnosti treba voditi računa i u fizičkom prostoru u smislu kontrole nad tim tko ima pristup osobnim podacima te razmotriti je li određene podatke potrebno držati pod ključem, a posebno u slučajevima kad poslovni subjekt s nekim dijeli poslovni prostor.

Na gore navedenim načelima se temelji niz konkretnih pravila koje poslovni subjekti trebaju poštivati i radnji koje bi trebali izvršiti da bi bili usklađeni s GDPR-om kako slijedi:

- uspostavljanje evidencije aktivnosti obrade[2] što je svojevrsni pregled kategorija osobnih podataka, svrha i zakonskih temelja njihova prikupljanja, načina obrade, prijenosa trećim osobama i sl. u okviru redovnog poslovanja
- informiranje ispitanika - klijenata i zaposlenika, o obradi njihovih osobnih podataka[3]
- ishođenje privole u slučajevima kad je to primjenjivo[4]
- u određenim situacijama, sklapanje ugovora s vanjskim partnerima kojima se prenose osobni podaci[5], što će u slučaju agencija za posredovanje u prometu nekretnina često biti vanjski pružatelj knjigovodstvenih i/ili informatičkih usluga

[2] čl. 30. GDPR-a
[3] čl. 13. i 14. GDPR-a
[4] čl.6., st.1.(a) GDPR-a
[5] čl. 28. GDPR-a

i, u određenim situacijama, partnerske agencije za posredovanje u prometu nekretnina ako imaju ulogu podizvođača
- uspostavljanje internih pravila kojima se detaljnije definiraju mjere zaštite osobnih podataka, provedba načela GDPR-a u konkretnim situacijama, način postupanja u slučaju da ispitanik podnese zahtjev/pritužbu/upit i sl. glede prikupljanja i obrade njegovih osobnih podataka, način postupanja u slučaju povrede osobnih podataka, interna podjela zadataka glede zaštite osobnih podataka i sl.
- upoznavanje zaposlenika s temeljnim načelima i pravilima postupanja koja trebaju poštivati, potpisivanje izjave o povjerljivosti
- reguliranje zaštite privatnosti na web stranici što se prvenstveno odnosi na pravilno reguliranje "kolačića" i davanja potpune informacije posjetiteljima o obradi njihovih osobnih podataka prikupljenih putem web stranice

NEKE OD NAJČEŠĆIH ZABLUDA U PRAKSI

- **Ako mi je klijent dao privolu, zakonito prikupljam osobne podatke.**

Ovo je u najvećem broju slučajeva netočna tvrdnja. Naime, privola je dobrovoljna suglasnost za prikupljanje osobnih podataka koji se inače ne bi smjeli prikupljati. U poslovanju posrednika u prometu nekretnina, nije potrebno dobiti privolu za obradu osobnih podataka u svrhu izvršenja posredničkog posla ili izvršenja obveza glede sprječavanja pranja novca i financiranja terorizma ili vođenja posredničkih dnevnika. Naime, samim potpisom ugovora o posredovanju klijent je pristao da njegovi podaci budu obrađeni u svrhu ispunjenja tog ugovora, dok ispunjenje ostalih zakonskih obveza posrednika uopće ne ovisi o tome je li klijent na to pristao ili nije. Stoga je u takvim slučajevima dobrovoljna suglasnost u obliku privole bespredmetna.

Privola bi, na primjer, mogla biti potrebna za javnu objavu informacija o identitetu klijenta i detaljima o suradnji u marketinške svrhe, ako klijent nije sam ustupio te podatke u tu svrhu. Na primjer, ako je klijent sam, na upit ili samoinicijativno, sastavio i dostavio referencu o suradnji s agencijom za posredovanje u prometu nekretnina za potrebe objave na web stranici, taj njegov postupak implicira njegovu suglasnost. Međutim, ako posrednik to učini samoinicijativno, bez prethodnog znanja i sudjelovanja klijenta, takva obrada osobnih podataka bi, vrlo izgledno, bila nezakonita bez valjane privole.

U slučajevima kad se osobni podaci ne obrađuju na temelju privole, ispitanicima treba biti dana obavijest o obradi njihovih osobnih podataka, čime se ispitanicima ne ostavlja mogućnost dobrovoljnog biranja hoće li njihovi podaci biti obrađivani kao kod privole, nego im se na znanje daje informacija o svim bitnim okolnostima obrade njihovih osobnih podataka i o njihovim pravima glede te obrade.

Pogrešno poimanje privole i ishođenje privole u situacijama u kojima je ona bespredmetna i u kojima ispitaniku zapravo treba dati obavijest o obradi podataka je već u prvim mjesecima primjene GDPR-a prepoznato kao jednu od najčešćih zabluda na koju često ukazuju i nacionalna nadzorna i europska savjetodavna tijela, a u 2019.

godini je za pogrešnu primjenu privole izrečena prva novčana kazna u EU (u Grčkoj) u iznosu od 150.000,00 eura.

Nisam dužan odgovoriti na pitanje i/ili prigovor klijenta glede osobnih podataka jer nisam ja prikupio podatke već netko drugi, a meni su samo proslijeđeni, jer nemam znanje ni informacije o onome što me klijent pita, jer nije točno ono što klijent tvrdi, jer šalje upit i/ili prigovor iz obijesti ... (ili bilo koji drugi razlog za neodgovaranje na pitanje i/ili prigovor)

Također netočno. GDPR vrlo visoko pozicionira načelo transparentnosti koje se, između ostalog, ostvaruje mogućnošću ispitanika postaviti pitanje i/ili prigovor i/ili zahtjev glede obrade osobnih podataka. Na taj zahtjev se mora odgovoriti u roku od mjesec dana od dana primitka zahtjeva,[6] a svako suprotno postupanje predstavlja prekršaj. Zahtjev može biti neopravdan, temeljen na pogrešnim uvjerenjima, nerazumljiv ili na bilo koji način težak za odgovaranje, ali GDPR ne predviđa uvjete po kojima bi bilo opravdano i zakonito ignorirati taj zahtjev te je u svakoj situaciji moguće dati one informacije koje su dostupne, obrazložiti zašto zahtjev nije osnovan, informirati ispitanika koje su sve radnje poduzete povodom zahtjeva itd.

Štoviše, ako klijent smatra da posrednik krši njegova prava glede zaštite osobnih podataka, ispitanik se uopće nije dužan najprije obratiti posredniku, već može prigovor izravno uputiti Agenciji za zaštitu osobnih podataka koja poduzima daljnje korake radi utvrđenja povrede/prekršaja. Činjenica da je ispitanik upit uputio izravno posredniku znači da vjeruje u mogućnost mirnog rješenja situacije koja je uzrok njegova nezadovoljstva. U praksi su česte i situacije da ispitanik istovremeno pošalje upit ili prigovor na obje adrese. Svakako postoji razlika ako nadzorno tijelo, postupajući po takvom prigovoru, utvrdi da je posrednik već poduzeo sve moguće napore i poduzeo radnje u svrhu zaštite prava ispitanike, nego ako nadzorno tijelo utvrdi da je ispitanik bio izignoriran ili da je dobio površan ili nepotpun odgovor na svoj upit.

Mi ne radimo s fizičkim osobama i ne prikupljamo nikakve osobne podatke.

Ovo uvjerenje može biti točno u smislu da posrednik ne surađuje s fizičkim osobama ne prikuplja osobne podatke u velikom opsegu. Međutim, u onom manjem opsegu u kojem ih prikuplja, postoji jednak rizik neusklađenog ponašanja. Ovdje je bitno imati na umu da je osobni podatak svaki podatak koji se odnosi na određenu fizičku osobu[7], neovisno nastupa li ta osoba u poslovnom ili privatnom svojstvu. Drugim riječima, to znači da u područje primjene GDPR-a spadaju svi podaci direktora i/ili kontakt osoba nekog trgovačkog društva, ali i svi podaci obrtnika i samostalnih djelatnosti. Također, kad se malo analiziraju do sad izrečene kazne europskih nadzornih tijela, može se zaključiti da su najveće kazne izrečene multinacionalnim kompanijama koje raspolažu osobnim podacima milijuna korisnika - fizičkih osoba. Međutim, za najveći broj ostalih povreda za koje su izrečene kazne u vrlo maloj mjeri je relevantno je li riječ o poslovnim subjektima koji rade uglavnom s pravnim osobama ili uglavnom s fizičkim osobama.

[6] čl. 12., st. 3. GDPR-a

[7] definicija osobnog podatka sukladno čl. 4., st. 1. GDPR-a

POSTUPANJE, PRAVA I OBVEZE U SLUČAJU INSPEKCIJSKOG NADZORA

Agencija za zaštitu osobnih podataka (dalje u tekstu: AZOP) može izvršiti najavljeni i nenajavljeni nadzor.[8]AZOP može izvršiti nadzor po prigovoru ispitanika ili po službenoj dužnosti. Ovisno o situaciji, nadzor se može izvršiti samo u odnosu na jedan problematični element poslovanja ili u odnosu na cjelokupnu usklađenost poslovanja s GDPR-om.

Prilikom nadzora, poslovni subjekt ima pravo na prisutnost punomoćnika. Inspektori su tijekom nadzora ovlašteni napraviti preslike dostupnih dokumenata, presnimiti sve sadržaje sustava pohrane i prikupiti druge relevantne informacije. Ako iz tehničkih razloga nije moguće tijekom nadzora napraviti preslike potrebne dokumentacije, ovlaštene osobe će, prema potrebi, oduzeti potrebne sustave pohrane i opremu koja sadržava druge relevantne informacije i zadržati je koliko je potrebno za izradu preslika te dokumentacije, a najduže 15 dana od dana oduzimanja.[9]

Ovlašteni inspektor sastavlja zapisnik na licu mjesta ili ga dostavlja poštom nekoliko dana nakon izvršenog nadzora. Iznimno je bitno znati da, potpisivanjem zapisnika, poslovni subjekt nad kojim je izvršen nadzor potvrđuje točnost sadržaja navedenog u zapisniku - dakle, potvrđuje da je sve ono što je navedeno u zapisniku istinito, osim ako ne izjavi prigovor u odnosu na dio zapisnika ili cijeli zapisnik. To znači da, u slučaju utvrđenja povrede i izricanja sankcije na temelju onoga što je utvrđeno zapisnikom o nadzoru, poslovni subjekt ne može više naknadno isticati da ono što je navedeno u zapisniku nije točno ako je taj zapisnik potpisao i nije prigovorio na njegov sadržaj.

Treba voditi računa i o načinu izricanja kazni koji je Republika Hrvatska zakonski uredila na specifičan način. Naime, u slučaju utvrđenja povrede osobnih podataka, AZOP uz rješenje kojim se utvrđuje povreda može izreći i neku od posebnih mjera koje nisu novčana kazna. Na primjer, AZOP može izreći opomenu, dati nalog za ispunjenjem nekih od zahtjeva ili prava ispitanika (npr. da odgovore na upit/prigovor na koji nisu odgovorili ili da reagiraju na zahtjev za brisanjem podataka) kao i dati nalog za provođenjem određenih radnji za usklađivanje s GDPR-om.[10] Novčana kazna se nikad ne izriče zajedno s nekom od tih mjera, već naknadno donesenom odlukom nakon što odluka o utvrđenju povrede i izricanju neke od spomenutih mjera postane pravomoćna.[11]

Ovo sve, konkretno, znači da u trenutku kad poslovni subjekt zaprimi rješenje kojim mu se izriče novčana kazna, s određenim izgledom za uspjeh može pokrenuti postupak samo u odnosu na visinu kazne, a ne i u odnosu na odluku da je počinio povredu osobnih podataka. Naime, u odnosu na odluku o povredi osobnih podataka se pravni lijek mogao podnijeti kad je ta odluka bila donesena ili se, još ranije, mogao podnijeti prigovor protiv zapisnika o provedenom nadzoru ako su postojale primjedbe na njegov sadržaj, a u trenutku kad poslovni subjekt zaprimi odluku o izricanju novčane

[8] čl. 36., st.1 Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/2018)

[9] čl. 37. st. 1. i 2. Zakona o provedbi Opće uredbe o zaštiti podataka

[10] čl. 58., st. 2 GDPR-a

[11] čl. 45., st. 3. Zakona o provedbi Opće uredbe o zaštiti podataka

kazne, rokovi za poduzimanje tih radnji su već protekli. Stoga je od samog početka nadzora potrebno voditi računa o ovakvom tijeku postupka i o tome koja može biti krajnja posljedica, te u skladu s time donositi poslovne odluke o (ne)postupanju i (ne)podnošenju pravnih lijekova po zaprimljenom zapisniku o provedenom nadzoru ili po rješenju kojim se utvrđuje povreda, ali se ne izriče novčana kazna koja može biti izrečena naknadno.

KRITERIJI ZA IZRICANJE SANKCIJA I SANKCIJE IZREČENE DO SADA

Kao što je već poznato, GDPR za "lakše" prekršaje predviđa kazne do 10.000.000,00 eura ili do 2% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, a za "teže" prekršaje predviđa kazne do 20.000.000,00 eura ili do 4% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu.[12]

Procjena visine kazne koju će nadzorno tijelo izreći ovisi o prirodi, težini i trajanju kršenja, broju ispitanika obuhvaćenih povredom, je li prekršaj počinjen s namjerom ili nepažnjom, što je učinjeno naknadno kako bi se otklonila ili umanjila šteta koju su pretrpjeli ispitanici, o prijašnjim kršenjima GDPR-a, o stupnju suradnje s nadzornim tijelom, o načinu na koji je nadzorno tijelo dobilo saznanje o kršenju (je li poslovni subjekt sam izvijestio o povredi ili je nadzorno tijelo dobilo informaciju na drugi način), itd.[13]

U praksi, najviše kazne do sada su izrečene tehnološkim gigantima i predvodnicima u određenim industrijama s milijunima korisnika kako je i opisano u nastavku ovog teksta, dok je većina ostalih kazni višestruko niža od propisane gornje granice.[14]

Tijekom 2018. godine, europska nadzorna tijela su izrekla kazne u cjelokupnom iznosu od 56.000.000,00 eura[15] dok za 2019. statistike još uvijek nisu dostupne. Najveće pojedinačne kazne do sada su izrečene u 2019. godini, i to kazna u iznosu od 110.390.200,00 eura izrečena hotelskom lancu Marriott International Inc. i kazna u iznosu od 204.600.000.00 eura izrečena aviokompaniji British Airways Inc. Obje kazne je izreklo nadzorno tijelo Ujedinjenog Kraljevstva zbog zanemarivanja tehničkih i organizacijskih mjera sigurnosti osobnih podataka milijuna korisnika tih poslovnih subjekata što je u konačnici omogućilo hakerske napade u kojima su ukradeni podaci s kreditnih kartica ispitanika.

Od ostalih izrečenih kazni, u nastavku su neke od njih koje se odnose na povredu univerzalnih i širokoprimjenjivih načela zaštite osobnih podataka, uz napomenu da se

[12] čl. 83., st. 4 i 5 GDPR-a

[13] čl. 83., st. 2. GDPR-a

[14] sukladno javno dostupnim informacijama o izrečenim kaznama na web stranici www.enforcementtracker.com gdje je dostupno kratko objašnjenje slučajeva, službene statistike na razini EU dostupne na web stranici Europskog odbora za zaštitu podataka https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2018_-_digital_final_1507_en.pdf

[15] sukladno statističkim podacima koje je za 2018. godinu izrađivalo Međunarodno udruženje stručnjaka za privatnost (eng. *International Association of Privacy Professionals*)

u odnosu na znatan broj izrečenih kazni još uvijek vode postupci koji nisu pravomoćno okončani te stoga ovi podaci nisu nužno konačni i mogu poslužiti tek kao orijentir:[16]

- Španjolsko nadzorno tijelo je izreklo kaznu od 8.000,00 eura pružatelju usluga distribucije i opskrbe električnom energijom zbog ignoriranja obveze suradnje s nadzornim tijelom. Naime, nakon što je nadzorno tijelo dalo nalog pružatelju usluga da svoje korisnike detaljnije informira o načinu na koji se mogu obrađivati njihovi osobni podaci, pružatelj usluga se oglušio na takav nalog.
- Poljsko nadzorno tijelo je izreklo kaznu od 9.380,00 eura gradskoj upravi poljskog grada Aleksandrow Kujawski zbog nepostojanja pisanog ugovora o prijenosu osobnih podataka s pružateljem softverskih usluga.
- Grčko nadzorno tijelo je izreklo 150.000 eura poslodavcu za kojeg je utvrđeno da obrađuje osobne podatke svojih zaposlenika na temelju privole u slučajevima gdje privola nije odgovarajući pravni temelj za prikupljanje osobnih podataka.
- Mađarsko nadzorno tijelo je izreklo kaznu od 3.200,00 eura financijskoj instituciji zbog odbijanja prigovora ispitanika glede korištenja njihovih telefonskih brojeva radi kontaktiranja u situacijama kad ispitanici ne bi podmirili ratu kredita na vrijeme. Nadzorno tijelo je utvrdilo da je financijska institucija trebala udovoljiti zahtjevima ispitanika da se njihov telefonski broj ne koristi u te svrhe jer se isti cilj mogao postići manje invazivnim načinom, odnosno slanjem opomene poštanskim putem.
- Njemačko nadzorno tijelo je izreklo kaznu od 2.500,00 eura poslovnom subjektu koji je slao grupne emailove na način da su svi primatelji emaila vidjeli email adrese drugih primatelja, premda na to nisu pristali i premda nisu bili ni u kakvom poslovnom odnosu s drugim primateljima ili bilo kakvom odnosu koji bi opravdavao otkrivanje kontakt podataka.

Premda se nijedna od navedenih kazni ne odnosi konkretno na poslovanje agencija za posredovanje u prometu nekretnina, povrede zbog kojih su izrečene kazne nisu usko vezane uz jednu industriju te se odnose na postupanja koja su zajednička različitim djelatnostima i o kojima je bitno voditi računa neovisno o poslovnim aktivnostima kojima se bave.

AKTIVNOSTI AGENCIJE ZA ZAŠTITU PODATAKA

Prema službenom izvješću AZOP-a za aktivnosti poduzete u 2018. godini, AZOP je u toj godini zaprimio 5.424 predmeta na rješavanje što je za 238% više u odnosu na 2017. godinu.[17] Od toga se 383 predmeta odnose na pritužbe građana što je za 176% više u odnosu na 2017. godinu. [18]

AZOP je u 2018. zaprimio 486 predmeta koji su se odnosili na međunarodnu suradnju s nadzornim tijelima drugih država.[19] Naime, u slučajevima kad poslovni subjekt djeluje na području više država, nadzorna tijela država članica (na primjer, nadzorno tijelo

[16] pregled javno dostupnih informacija o do sada izrečenim kaznama od strane europskih nadzornih tijela na web stranici www.enforcementtracker.com

[17] Godišnje izvješće Agencije za zaštitu osobnih podataka za 2018., usvojeno Na 14. sjednici Hrvatskog sabora, održanoj 18. listopada 2019. godine

[18] ibid. 17

[19] ibid. 17

države članice EU u kojoj je poslovni subjekt registriran i nadzorno tijelo države članice EU u kojoj nadzorno tijelo sumnja na počinjenje povrede GDPR-a) mogu poduzimati zajedničke nadzorne aktivnosti i pružati jedna drugoj pomoć u provođenju tih aktivnosti.

U 2018. godini AZOP je izvršio ukupno 1.515 nadzora. Prema informacijama javno dostupnim u vrijeme pisanja ovog članka, u Republici Hrvatskoj od početka izravne primjene GDPR-a nije pravomoćno izrečena nijedna novčana kazna, a u tijeku je 18 sudskih postupaka pokrenutih protiv rješenja kojim se utvrđuju povrede osobnih podataka.[20]

Iz navedenog je vidljivo da AZOP bilježi znatan porast aktivnosti koji je u velikoj mjeri rezultat pojačane svijesti građana o njihovim pravima koji se tiču zaštite osobnih podataka. Također je vidljivo da je AZOP u dosadašnjem postupanju u najvećoj mjeri vodio računa o svojoj savjetodavnoj ulozi te time, prema javno dostupnim izvorima, spada u nadzorna tijela četiriju država članica EU koja do sada nisu donijela odluke o izricanju novčanih kazni.[21]

ZAKLJUČAK

Početno razdoblje primjene GDPR-a je obilježila iznimna medijska eksponiranost te poprilično raznovrsne reakcije obveznika GDPR-a koje se kreću od potpune nezainteresiranosti do iznimne osjetljivosti na tematiku zaštite osobnih podataka. U bližoj budućnosti se očekuje donošenje pravomoćnih sudskih odluka o izrečenim novčanim kaznama. Također se očekuje nastavak intenzivnog rada Europskog odbora za zaštitu podataka, kao tijela koje osigurava dosljednu primjenu GDPR-a, na donošenju smjernica za tumačenje i primjenu različitih aspekata zaštite osobnih podataka. Očekuje se da će te aktivnosti doprinijeti utvrđivanju ujednačenih standarda za primjenu pravila GDPR-a te je potrebno pratiti trendove u razvoju ovog područja i svakodnevno poslovanje uskladiti s načelima i dobrim praksama zaštite osobnih podataka.

[20] ibid. 17

[21] sukladno javno dostupnim informacijama o izrečenim kaznama na web stranici www.enforcementtracker.com