J. appl. health sci. 2020; 6(1): 159-167

Zaštita osobnih podataka

[1] Jasenka Surla
[2] Ivan Markotić
[2] Olja Vori

[1] Klinički bolnički centar Sestre milosrdnice
[2] Zdravstveno veleučilište Zagreb

Sažetak

Opća uredba o zaštiti podataka 2016/679 postavila je imperativ na zaštitu osobnih podataka u pravnim sustavima država članica Europske unije, propisujući načela kojih su se voditelji i izvršitelji obrade dužni pridržavati u obavljanju socijalnih i gospodarskih djelatnosti. Gospodarska i društvena integracija utjecala je na povećanje opsega razmjene osobnih podataka između država članica i trećih zemalja, u javnom i privatnom sektoru. U takvim okolnostima potreban je novi i jači pravni okvir koji propisuje jasna prava i obveze sudionika društvenih odnosa. Pritom je važno omogućiti daljnje ostvarivanje potreba modernog društva pod uvjetom očuvanja temeljnih ljudskih vrednota i zaštite prava osobnosti svakog pojedinca, bez obzira na nacionalnost i boravište. Neovisno o pravnoj osnovi obrade osobnih podataka, ispitanici uvijek zadržavaju pravo na informiranost, pristup svojim podacima, brisanje, mijenjanje i prijenos osobnih podataka te ograničenje svrhe obrade. Međutim, pravo na brisanje osobnih podataka nije apsolutno pravo, već ga je potrebno staviti u ravnotežu sa zakonskim obvezama voditelja obrade na čuvanje određenih vrsta podataka.

Ključne riječi: osobni podatak, osjetljivi podaci, obrada, ispitanik, voditelj i izvršitelj obrade, privola, legitimni interes, javni interes, zdravstvo

Datum primitka: 24.01.2019.

Datum prihvaćanja: 15.02.2020.

https://doi.org/10.24141/1/6/1/15

Adresa za dopisivanje:
Ivan Markotić, Zdravstveno veleučilište Zagreb
E-pošta: ivan.markotic@zvu.hr

Uvod

Zaštitom osobnih podataka teži se poštivanju temeljnih prava i sloboda bez obzira na nacionalnost i boravište pojedinca. U vremenu kada je neograničena količina informacija pojedincu dostupna putem interneta, a razvoj tehnologije i sve kompleksnije djelovanje javnog i društvenog života zahtijevaju razmjenu velike količine podataka, pravo na zaštitu osobnih podataka postalo je jedan od instrumenata ostvarenja prava na poštivanje privatnog i obiteljskog života i prava osobnosti.

Temeljni je akt zaštite osobnih podataka na području Europske unije od 25. svibnja 2018. Opća uredba o zaštiti podataka 2016/679 (dalje u tekstu: Uredba), koja se izravno i u cijelosti primjenjuje u Republici Hrvatskoj. Općom uredbom dosadašnja je regulativa zaštite osobnih podataka jedinstveno uređena za sve države članice, s propisanim načelima za obradu osobnih podataka, pravima ispitanika, obvezama voditelja i izvršitelja obrade te predviđenim sankcijama za prekršitelje. Pravni sustav Republike Hrvatske svojim posebnim zakonima uređuje pojedina područja društvenog života te utvrđuje pravnu osnovu za pojedine obrade osobnih podataka u cilju ispunjenja zakonom propisanih svrha. Primarni cilj strože zakonske regulative na ovom području predstavlja iskorak prema uspostavi područja slobode, sigurnosti, pravde i dobrobiti pojedinaca.

U odnosu na obradu podataka o zdravlju ispitanika, Uredba uređuje okolnosti u kojima nije potrebna privola ispitanika, s obzirom na to da je obrada osobnih podataka nužna kako bi se ispunila prava ispitanika zajamčena posebnim propisima na području zdravstva, odnosno kako bi pružatelj zdravstvene usluge ispunio svoju zakonsku obvezu. Uredba također ostavlja prostor za razmatranje postojanja ravnoteže između prava pojedinca i javnog interesa posebice u pogledu zaštite od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanje visokih standarda kvalitete i sigurnosti zdravstvene skrbi, lijekova i medicinskih proizvoda te svrhe provođenja znanstvenih ili povijesnih istraživanja i statističkih svrha.

Zakonski okvir

Zaštita osobnih podataka u međunarodnom pravu i pravu Europske unije prisutna je dugi niz godina putem pravnih akata poput Opće deklaracije o ljudskim pravima proglašene na Općoj skupštini Ujedinjenih naroda 1948., Konvencije za zaštitu ljudskih prava i temeljnih sloboda iz Rima 1950. te Povelje Europske unije o temeljnim pravima proglašene 2000. godine. Temeljna namjera međunarodne zajednice, bez na to je li riječ o narodima Europske unije ili svijeta, bila je zaštiti pravo svakog pojedinca na poštivanje njegova privatnog i obiteljskog života, prava na osobnost, prava na dostojanstvo i zaštitu osobnih podataka. Imajući u vidu da osobni podaci neposredno ukazuju na strogo osobna stanja, karakteristike, vjerovanja i stavove fizičke osobe, razvidno je da zaštita osobnih podataka čini jedan od sastavnih dijelova zaštite i ostvarenja pojedinih drugih prava čovjeka i građanina. Uslijed pojave sve bržeg razvoja tehnologije i industrijskog društva u proteklih nekoliko desetljeća, susrećemo se s izazovima zaštite osobnih podataka u uvjetima gotovo neograničene i brze razmjene podataka putem interneta, što postavlja sve zahtjevnije kriterije za kontinuirano povećanje standarda informacijske sigurnosti na svim područjima privatnog i javnog života.

U Republici Hrvatskoj člankom 37. Ustava zajamčena je sigurnost i tajnost podataka, a njihovo prikupljanje, obrađivanje i upotreba bez privole ispitanika mogući su samo uz uvjete predviđene posebnim zakonima. Kao država članica Europske unije, RH je dužna u svoj pravni sustav implementirati uredbe EU-a izravno i u cijelosti. Stoga je od 25. svibnja 2018. u našem zakonodavstvu, kao i na području cijele Europske unije, u primjeni Uredba 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka – engl. *General Data Protection Regulation* – GDPR). Uredba je na snagu stupila u svibnju 2016., no zbog niza administrativnih postupaka koje su fizičke i pravne osobe privatnog i javnog sektora u državama članicama obvezne primjenjivati u svojem poslovanju, predviđen je rok od dvije godine za prilagodbu. Zbog brojnih praktičnih iskustava, presuda Europskog suda za ljudska prava, mišljenja radnih skupina Europske komisije i mišljenja nadzornih tijela za zaštitu osobnih podataka u državama članicama, jasno je da

razdoblje od dvije godine nije dovoljno za temeljitu primjenu Uredbe ta da je njezina implementacija zahtjevan proces koji se trajno nastavlja.

U odnosu na pravni sustav RH, Uredba je opći akt, dok su pojedini zakoni posebni akti koji uređuju pojedina područja društvenog života. Jednaku snagu Općoj uredbi u RH ima Zakon o provedbi Opće uredbe o zaštiti podataka te zajedno čine povezanu cjelinu. Spomenuti Zakon detaljnije uređuje pojedina prava i obveze iz Uredbe te utvrđuje nadzorno tijelo u RH – Agenciju za zaštitu osobnih podataka, kao i njezin djelokrug. Od posebnih propisa to su primjerice:

- Zakon o radu
- Zakon o zaštiti prava pacijenata
- Zakon o obveznom zdravstvenom osiguranju i zdravstvenoj zaštiti stranaca u Republici Hrvatskoj
- Pravilnik o načinu vođenja, čuvanja, prikupljanja i raspolaganja medicinskom dokumentacijom pacijenata iz obveznog zdravstvenog osiguranja u Centralnom informacijskom sustavu zdravstva Republike Hrvatske
- Zakon o podacima i informacijama u zdravstvu
- Zakon o psihološkoj djelatnosti
- Zakon o osobnoj iskaznici
- Zakon o zaštiti na radu
- Zakon o državnim službenicima
- Kazneni zakon itd.

Naime, sudionici pojedinih društvenih odnosa moraju poštivati pravne obveze na području zaštite osobnih podataka koje proizlaze iz relevantnih zakona i podzakonskih propisa koji uređuju djelatnost kojom se bave. To znači da Uredba postavlja opća načela zaštite osobnih podataka, a pravnim sustavima država članica dozvoljava da svojim posebnim propisima utvrđuju kada je obrada osobnih podataka zakonita bez privole ispitanika, odnosno koja su prava i obveze sudionika pojedinih djelatnosti u vezi s obradom osobnih podataka.

Što je osobni podatak?

Osobni podaci jesu podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Pojam kojim Uredba oslovljava pojedinca jest **ispitanik**. Pojedinac, tj. ispitanik čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.[1]

U svakodnevnim životnim situacijama ponekad se čini dvojbenim smatraju li se ime i prezime osobnim podatkom, posebice ako uzmemo u obzir da su neka imena vrlo česta, npr. Ivan Horvat, pa iz samog imena nije moguće utvrditi o kojem je točno Ivanu Horvatu riječ. No valja imati na umu da su situacije u kojima osobno ime nije dovoljan identifikator iznimno rijetke, a svrha upotrebe tog podatka gotovo je uvijek dio šireg konteksta. Pojedini podaci samostalno ne moraju imati nikakvo značenje, ali u kombinaciji s drugim podacima izravno upućuju na identitet određene osobe. Primjerice, ako je samo osobno ime Ivan Horvat navedeno na komadiću papira, tada nije moguće identificirati točno određenu osobu pod tim imenom. Međutim, ako se na istom papiru nalazi informacija da je zaposlenik određenog poslodavca odnosno godina rođenja, karakteristika fizičkog izgleda, kućna adresa, broj telefona, adresa e-pošte, OIB ili bilo koji drugi podatak koji upućuje na određenu osobu, tada ime i prezime svakako čine osobni podatak u smislu Uredbe. Nadalje, određeni iznos plaće, čak bez ijednog drugog podatka, predstavlja osobni podatak u situaciji kad taj iznos možemo upisati u COP sustav konkretne zdravstvene ustanove. U tom trenutku prikazat će se imena svih radnika te zdravstvene ustanove koji primaju plaću u tom iznosu, a osim toga istodobno će biti vidljivi i ostali njihovi osobni podaci koji su na zakonskoj osnovi uneseni u sustav. Shvaćanje osobnog podatka u smislu Uredbe ide toliko daleko da je, primjerice, komentar rukovoditelja napisan u dosje radnika osobni podatak tog rukovoditelja. Prema tome, preporučljivo je da se pojam osobnog podatka razumije i primjenjuje u što širem značenju. Neovisno o eventualnim posljedicama identifikacije, pravo je svakog ispitanika zaštita i tajnost njegovih osobnih podataka. To znači da bez obzira na bezazlenost uvida u određene osobne podatke u danom trenutku, kao što su ime i prezime i go-

dina rođenja bez OIB-a ili broja tekućeg računa osobe, svaka upotreba, tj. obrada osobnog podatka jednako potpada pod kriterije obrade i zaštite u skladu s odredbama Uredbe.

Osobni podaci ne moraju uvijek izravno ili neizravno identificirati određenu osobu, već mogu biti pseudonimizirani ili anonimizirani. **Pseudonimizacija** je obrada osobnih podataka tako da se više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija. Tehničkim (npr. enkripcija) i organizacijskim mjerama osigurava se nemogućnost upotrebe dodatnih informacija i njihovo povezivanje sa pseudonimom određene osobe koje bi moglo rezultirati utvrđivanjem ispitanikova identiteta. Dakle, za reidentifikaciju osobe potrebne su dodatne informacije koje se obično čuvaju na odvojenim sustavima pohrane. Tako se, primjerice, u kliničkim ispitivanjima lijekova koja provode zdravstvene ustanove podaci o zdravstvenom stanju pojedinog ispitanika prosljeđuju naručiteljima kliničkih ispitivanja, tj. farmaceutskim tvrtkama, pod određenim kodom – pseudonimom. Tako naručitelj ispitivanja dobije relevantnu informaciju o djelotvornosti lijeka na ispitanika, ali identitet tog ispitanika može utvrditi samo zdravstvena ustanova jer mu je u svojem informatičkom sustavu dodijelila pseudonim.

U slučaju **anonimiziranih** podataka nitko nema informacije s pomoću kojih je moguća identifikacija ispitanika, čak ni osoba koja prikuplja podatke od ispitanika. Takav primjer predstavljaju anonimne ankete ili upitnici u čijem se sadržaju ne nalaze pitanja koja jasno upućuju na karakteristike s pomoću kojih je moguće identificirati ispitanike. Za primjenu Uredbe nužno je razlikovati ove pojmove, budući da obuhvaća pseudonimizirane podatke, dok se na anonimizirane podatke ne primjenjuje.

Obrada osobnih podataka znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.[2] Dakle, sam uvid liječnika ili medicinske sestre u dokumentaciju ili karticu zdravstvenog osiguranja pacijenta predstavlja obradu osobnog podatka prema slovu Uredbe. S tim u vezi, Izjavom o povjerljivosti i internim aktima poslodavac će obvezati radnike na čuvanje poslovne tajne.

Subjekti obrade

Za obradu su odgovorni **voditelji obrade**, tj. fizičke i pravne osobe, tijela javne vlasti, agencije ili druga tijela koja samostalno ili zajedno s drugima određuju svrhe i sredstva obrade osobnih podataka.[3] Zdravstvena ustanova, fakultet, ministarstvo, porezna uprava, policijska uprava, telekomunikacijski operator, trgovina, poslodavac, pošta, radijska ili televizijska postaja samo su neki od voditelja obrade. Osim njih, osobne podatke obrađuju i **izvršitelji obrade**. To su pravne ili fizičke osobe koje osobne podatke obrađuju za voditelja najčešće pružajući uslugu *outsourcinga* te ne određuju svrhu obrade samostalno. Primjeri su izvršitelja obrade informatičke tvrtke, knjigovodstveni servisi, pravne osobe ovlaštene za pružanje privatne zaštite i sl. Važno je da se obrada koju provodi izvršitelj obrade uredi ugovorom ili drugim pravnim aktom. Tako voditelj obrade osigurava da izvršitelj poštuje odredbe Uredbe te jamči zaštitu i povjerljivost obrade osobnih podataka. S obzirom na to da za propust izvršitelja obrade prema ispitaniku odgovara voditelj obrade, ako su međusobna prava i obveze voditelja i izvršitelja jasno definirani u ugovoru, u slučaju propusta izvršitelja obrade voditelj će biti obvezan nadoknaditi štetu ispitaniku, ali u tom slučaju imat će mogućnost regresne naplate od izvršitelja obrade.

Privola

Privola je jasna potvrdna radnja kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu osobnih podataka koji se na njega odnose. Privola može biti usmena ili pisana izjava, uključujući i elektroničku. Na internetskim stranicama privola se može sastojati od označavanja određenih polja kvačicom, npr. odabirom određenih vrsta tzv. kolačića i biranje tehničkih postavki usluga informacijskog društva. Unaprijed kvačicom označeno polje ne bi se smjelo smatrati privolom. Također, korisnici moraju moći odabrati koju vrstu oglasne e-pošte žele primati od pojedinog pružatelja usluge i sl. Osim toga, privola može biti i druga izjava i ponašanje kojim ispitanik u tom kontekstu jasno pokazuje da prihvaća predloženu

obradu osobnih podataka. U tom smislu šutnja ili manjak aktivnosti ispitanika ne znače privolu na obradu.[4]

U slučaju postojanja više svrha obrade koje su u trenutku prikupljanja privole identificirane i predvidive, tada privola mora jasno obuhvatiti svaku od tih pojedinih svrha. Privola se ne smije odnositi na nedefinirane potencijalne i buduće svrhe obrade koju provodi konkretan voditelj obrade. Isto tako, ako tekst privole sastavlja voditelj obrade, mora biti jasan, lako razumljiv i bez nepoštenih uvjeta. Identitet voditelja obrade i svrhe obrade moraju biti jasno naznačeni. Privola se ne može smatrati dobrovoljnom ako ispitanik nema slobodan izbor ili ako nema mogućnost odbiti ili povući privolu bez posljedica. Kada se govori o djelatnosti zdravstva, obveze bolnice u pružanju zdravstvene usluge propisane su Zakonom o zdravstvenoj zaštiti, Zakonom o zaštiti prava pacijenata i dr. S tim u vezi, privola pacijenta na obradu osobnih podataka ne može biti pravni temelj njihove obrade koja se obavlja u procesu pružanja zdravstvene usluge. Naime, medicinsko osoblje bolnice dužno je na temelju spomenutih pravnih propisa pružiti pacijentu uslugu te izvršiti za to potrebnu obradu osobnih podataka. Pisana privola u ovom bi slučaju bila nepotrebna administrativna mjera koja nije pravna osnova obrade osobnih podataka, s obzirom na to da zakonska obveza pružanja zdravstvene usluge postoji i u slučaju da pacijent odbije potpisati obrazac privole za obradu osobnih podataka.

Osjetljivi podaci

Obrada određene vrste osobnih podataka može uzrokovati znatan rizik za temeljna prava i slobode ljudi pa su iz tog razloga tzv. **osjetljivi podaci** svrstani u posebnu kategorija osobnih podataka. Zabranjena je obrada podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu, genskih i biometrijskih podataka te podataka koji se odnose na zdravlje, spolni život i spolnu orijentaciju osobe. Kada je riječ o podacima o zdravlju, Uredba predviđa slučajeve u kojima je obrada dopuštena bez privole ispitanika:

1. obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju prava Unije ili prava države članice ili u skladu s ugovorom sa zdravstvenim radnikom
2. obrada je nužna u svrhu javnog interesa u području javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanje visokih standarda kvalitete i sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda, na temelju prava Unije ili prava države članice kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda ispitanika.[5]

Zdravstveni podaci osjetljivi su podaci, a čine ih svi podaci o prijašnjem, trenutačnom i budućem fizičkom i mentalnom zdravstvenom stanju pojedinca, uključujući i broj i oznaku koji su dodijeljeni radi jedinstvene identifikacije za zdravstvene svrhe te ostale informacije prikupljene prilikom registracije za pružanje zdravstvenih usluga ili tijekom pružanja zdravstvenih usluga pojedincu. Također, osjetljive podatke čine i broj, simbol ili oznaka koja je pojedincu dodijeljena u svrhu njegove jedinstvene identifikacije u zdravstvene svrhe, kao i informacije izvedene iz testiranja ili ispitivanja dijela tijela ili tjelesne tvari, među ostalim iz genskih podataka i bioloških uzoraka, te bilo kakva informacija o, na primjer, bolesti, invalidnosti, riziku od bolesti, medicinskoj povijesti, kliničkom tretmanu ili fiziološkom ili biomedicinskom stanju ispitanika neovisno o njegovu izvoru, kao na primjer od liječnika ili drugog zdravstvenog djelatnika, bolnice, medicinskog uređaja ili dijagnostičkog testa *in vitro*.[6]

Obrada podataka u svrhe povezane sa zdravljem trebala bi se obavljati samo radi ostvarivanja tih svrha u korist pojedinaca i društva u cjelini, pogotovo u kontekstu upravljanja uslugama i sustavima zdravstvene ili socijalne skrbi, u što se ubraja i obrada takvih podataka koju u svrhu kontrole kvalitete, informacija o upravljanju i općeg nacionalnog i lokalnog nadzora sustava zdravstvene ili socijalne skrbi provode uprava i središnja nacionalna tijela nadležna za zdravlje i u svrhu osiguravanja kontinuiteta zdravstvene ili socijalne skrbi i prekogranične zdravstvene skrbi ili u svrhu zdravstvene zaštite, nadzora i uzbunjivanja ili u svrhu arhiviranja u javnom interesu, u svrhu znanstvenih ili povijesnih istraživanja ili u statističke svrhe utemeljene na pravu Unije ili pravu države članice i čime treba ostvariti cilj od javnog interesa, kao i za studije koje se provode u javnom interesu u području javnog zdravlja.[7]

Načela obrade osobnih podataka:

- zakonitost, poštenost i transparentnost
- ograničavanje svrhe
- smanjenje količine podataka
- točnost
- ograničenje pohrane
- cjelovitost i povjerljivost
- pouzdanost.

Osobni podaci ne smiju se obrađivati bez opravdanog razloga ni u prekomjernoj količini. Stoga obrada osobnih podataka u svakom pojedinom slučaju mora biti zakonita, tj. udovoljavati barem jednom od uvjeta predviđenih člankom 6. Uredbe. Prema tome, obrada je zakonita ako postoji privola ispitanika odnosno ako je nužna za:

- izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora – npr. *Ugovor o kreditu*
- poštivanje pravnih obveza voditelja obrade – npr. obveze poslodavca povezane s *mirovinskim i zdravstvenim osiguranjem radnika; pružanje zdravstvene usluge prema Zakonu o zaštiti prava pacijenata itd.*
- zaštitu ključnih interesa ispitanika ili druge fizičke osobe – npr. *nužno pružanje hitne pomoći pacijentima bez svijesti*
- izvršavanje zadaća od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade – npr. *godišnje podnošenje podataka Hrvatskom zavodu za javno zdravstvo na propisanim obrascima*
- potrebe legitimnih interesa voditelja obrade ili treće strane – *obrada osobnih podataka osoba zaposlenih u zoni zračenja kako bi se obavile mjesečne provjere stanja dozimetra na zaštitnim odijelima; videonadzor radi zaštite imovine i ljudi itd.*[8]

Obrada osobnih podataka također mora biti transparentna. Pojedinac mora biti upoznat s identitetom voditelja obrade te svakom od svrha radi koje će se njegovi podaci obrađivati. Ako sve potencijalne svrhe nisu u početku poznate, ispitaniku voditelj obrade mora omogućiti da se naknadno o svakoj novoj svrsi posebno izjasni pristaje li na nju ili ne. Obrađivati se moraju samo oni osobni podaci koji su potrebni za određenu svrhu – **smanjenje količine podataka**. Često se susrećemo s pojavom prekomjernog prikupljanja osobnih podataka koji nisu potrebni u pojedinom slučaju. Primjerice, u svrhu vođenja evidencije radnog vremena dovoljno je da radnik prisloni karticu ili utipka dodijeljeni kod u uređaj za prijavu, bez potrebe za istodobnim biometrijskim skeniranjem, tj. izradom i prikupljanjem fotografija u bazu podataka evidencije. Za takvu obradu biometrijskih podataka radnika u svrhu evidentiranja radnog vremena potrebna je izričita privola radnika.[9] Ako se radnik protivi takvoj obradi, poslodavac je dužan pronaći alternativno rješenje.

Nadalje, jedan od čestih primjera prekomjerne obrade osobnih podataka jest i ako voditelj obrade fotokopira osobnu iskaznicu ispitanika te pohrani kopiju u dosje ispitanika nakon provjere da su OIB i drugi podaci točno uneseni u informatički sustav, ako to nije obvezno na temelju pravnog propisa za pružanje određene usluge u konkretnoj djelatnosti. Kada zakon ne propisuje obvezu čuvanja kopije osobne iskaznice, trebalo bi je uništiti nakon provjere točnosti podataka. Prema tome, voditelji obrade dužni su voditi računa o opsegu obrade osobnih podataka, razdoblju pohrane i mogućnosti dokazivanja njezina pravnog temelja.

Pravo voditelja obrade na obradu osobnih podataka pojedinca može, osim iz privole, proizlaziti iz ugovora s ispitanikom, zakona ili legitimnog interesa voditelja. U praktičnom iskustvu legitimni interes predstavlja pojam koji otvara najviše pitanja. Naime, riječ je obvezi obrade osobnih podataka kako bi se provela zadaća povezana s poslovnim aktivnostima. Obrada osobnih podataka u tom slučaju ne mora biti izričito opravdana pravnom obvezom ili provedbom uvjeta ugovora s pojedincem. Voditelj obrade u slučaju pozivanja na svoj legitimni interes nikako ne smije ozbiljno utjecati na prava i slobode pojedinaca čije osobne podatke obrađuje. U suprotnom, voditelj osobnih podataka mora pronaći drugi pravni temelj za obradu osobnih podataka. Primjer obrade u legitimnom interesu bilo bi osiguranje mrežne i informacijske sigurnosti IT sustava konkretnog voditelja obrade.[10]

Prava ispitanika:

- pravo na informiranost
- pravo na pristup podacima
- pravo na ispravak
- pravo na brisanje ili zaborav
- pravo na ograničenje obrade
- pravo na prenosivost podataka
- pravo na prigovor
- pravo na izuzeće pravnih odluka prilikom automatskog donošenja odluka i izrade profila.

Prilikom prikupljanja osobnih podataka voditelj obrade mora ispitaniku pružiti informacije o svojem identitetu, podatke za kontakt, informacije o svrhama obrade i pravnoj osnovi za obradu podataka, roku obrade, mogućnosti povlačenja privole, iznošenju osobnih podataka u treće zemlje, podatke o drugim primateljima osobnih podataka, pravu na podnošenje pritužbe nadzornom tijelu, uputu o pravima ispitanika itd.[11]

Ispitanik ima pravo na pristup podacima, tj. uputiti voditelju obrade upit o tome obrađuju li se i kako se obrađuju njegovi osobni podaci, u koju svrhu i po kojoj pravnoj osnovi. Osim toga, ispitanik ima pravo obratiti se voditelju obrade podnošenjem zahtjeva za povlačenje privole ili mijenjanje osobnih podataka kojima voditelj raspolaže (npr. promjena prezimena ili adrese). Također, ispitanik ima pravo prenijeti osobne podatke od jednog voditelja obrade drugome. U svakom trenutku ispitanik ima pravo podnijeti voditelju obrade prigovor na obradu njegovih osobnih podataka. Iz navedenih razloga, voditelj obrade obvezan je omogućiti ispitaniku ostvarenje svakog od tih prava na jednostavan način, primjerice objavom potrebnih informacija, uputa i podataka za kontakt na svojoj mrežnoj stranici.

Ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose, a voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja u slučaju, primjerice, prestanka svrhe obrade, nezakonite obrade, nepostojanja pravne osnove za obradu ili nepostojanja legitimnih interesa koji su jači od interesa pojedinca. Pravo na brisanje nije apsolutno pravo ispitanika, već ga treba staviti u ravnotežu s drugim pravima koja su relevantna u odnosu između ispitanika i pravne obveze odnosno legitimnog interesa voditelja obrade. Prema Zakonu o podacima i informacijama u zdravstvu, u CEZIH-u se medicinska dokumentacija za fizičke osobe čuva deset godina nakon smrti fizičke osobe, a nakon isteka tog roka s dokumentacijom se postupa u skladu s propisima o arhivskom gradivu i arhivima.[12] Slijedom navedenog, pravno utemeljeno bit će odbijanje zahtjeva ispitanika podnesenog zdravstvenoj ustanovi kojim traži brisanje svojih zdravstvenih podataka sadržanih u sustavu CEZIH. Također valja napomenuti da pravo ispitanika na povlačenje privole i brisanje podataka ne utječe na zakonitost obrade učinjene prije takvog povlačenja ili podnošenja zahtjeva za brisanje.

Kako bi se osobni podaci ispitanika zaštitili od povreda u smislu nezakonite obrade, neovlaštenog pristupa i mogućih zlouporaba, dužnost je voditelja i izvršitelja obrade da poduzmu tehničke, kadrovske i organizacijske sigurnosne mjere. To će se postići uvođenjem politike informacijske sigurnosti u redovito poslovanje, čuvanjem dokumentacije koja sadrži osobne podatke u zaključanim ormarima u trenucima kada se ne upotrebljava za obavljanje redovnih radnih zadataka, redovitim mijenjanjem lozinki za pristup informatičkom sustavu, zaključavanjem zaslona računala prilikom udaljavanja od radnog mjesta, unošenjem Izjava o povjerljivosti u ugovore o radu itd.

Pritužbe nadzornom tijelu

Pritužbu na obradu osobnih podataka ispitanik može podnijeti Agenciji za zaštitu osobnih podataka, koja je u Republici Hrvatskoj samostalno i nezavisno nadzorno tijelo te za svoj rad odgovara Hrvatskom saboru. Ustrojstvo i djelokrug Agencije utvrđeni su Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/18). Agencija na svojoj mrežnoj stranici objavljuje mišljenja, preporuke i odgovore na pitanja zainteresiranih o primjeni Uredbe na konkretne slučajeve.

Agencija za zaštitu osobnih podataka u Republici Hrvatskoj izriče upravne novčane sankcije voditeljima i izvršiteljima obrade za povredu osobnih podataka u skladu s Uredbom. Propisane novčane kazne iznose do 10.000.000,00 eura ili do 2 % ukupnoga godišnjeg prometa na svjetskoj razini. Kršenje osnovnih načela za obradu, uključujući sadržaj privole, prava ispitanika, prijenos osobnih podataka i treće zemlje, nepoštivanje naredbe ili predviđenog ili trajnog ograničenja obrade, povlači za sobom novčanu kaznu čak u iznosu koji može dosegnuti 20.000.000,00 eura ili do 4 % ukupnoga godišnjeg prometa na svjetskoj razini. Cilj drakonskih novčanih kazni zasigurno je odvratiti voditelje i izvršitelje obrade od protuzakonitog poslovanja u pogledu odnosa prema osobnim podacima klijenata i korisnika njihovih usluga. Prilikom određivanja iznosa upravne novčane kazne uzima se u obzir jedanaest kriterija kao što su težina, trajanje, priroda kršenja, vrsta krivnje, poduzete mjere ublažavanja štete, prijašnja kršenja, tehničke i organizacijske mjere primijenjene u obradi osobnih podataka i sl.[13]

Zaključak

Zdravstvene ustanove voditelji su obrade osobnih podataka na dva načina. Nastupaju kao poslodavci dužni zaštititi osobne podatke svojih radnika te njih istodobno obvezati na poštivanje prava na zaštitu osobnih podataka drugih osoba čije osobne podatke obrađuju tijekom izvršavanja svoje radne obveze. Prema trećima i pacijentima zdravstvena ustanova nastupa i kao voditelj posebne kategorije osobnih podataka koja uživa pojačanu zaštitu prema slovu Uredbe.

Obrada podataka u svrhe povezane sa zdravljem trebala bi se obavljati samo radi ostvarivanja tih svrha u korist pojedinaca i društva u cjelini, pridržavajući se općih načela zaštite kao što su zakonitost, poštenost i transparentnost, smanjenje količine podataka i dr. Rezultat primjene predviđenih načela mora se odraziti u pouzdanosti voditelja obrade koji može dokazati da sustavno i ažurno provodi tehničke, organizacijske i kadrovske mjere sigurnosti. Dosljedan rad na implementaciji Uredbe pridonosi jačanju povjerenja te osvješćivanju svih ljudi o važnosti ispravnog ponašanja prema vlastitim i tuđim osobnim podacima, a tijekom kontinuiranog procesa prilagodbe, stav prema osobnim podacima kao predmetu zaštite temeljnih prava i sloboda svakog čovjeka postat će i dio kulture svakog društva.

Reference

1. Opća uredba o zaštiti podataka 2016/679, članak 4. stavak 1.
2. Opća uredba o zaštiti podataka 2016/679, članak 4. stavak 2.
3. Opća uredba o zaštiti podataka 2016/679, članak 4. stavak 7.
4. Opća uredba o zaštiti podataka 2016/679, Uvodna odredba broj 32
5. Opća uredba o zaštiti podataka 2016/679, članak 9. stavak 2. točke i) i j)
6. Opća uredba o zaštiti podataka 2016/679, Uvodna odredba broj 35
7. Opća uredba o zaštiti podataka 2016/679, Uvodna odredba broj 53
8. URL https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
9. Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/2018, članak 22.
10. URL https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_hr
11. Opća uredba o zaštiti podataka 2016/679, članci 13. i 14.
12. Zakon o podacima i informacijama u zdravstvu, NN 14/19, Članak 28. stavak 4
13. Opća uredba o zaštiti podataka, 2016/679, članak 80.

PROTECTION OF PERSONAL DATA

Abstract

The General Data Protection Regulation 2016/679 set out the imperative to protect personal data in the legal systems of the European Union Member States, stipulating the principles which the data processing directors and administrators are obliged to adhere to in carrying out their social and economic activities. Economic and social integration has led to an increase in the volume of exchange of personal data between the Member States and third countries in the public and private sectors. In these circumstances, a new and stronger legal framework prescribing the clear rights and obligations of participants in social relations is needed. At the same time, it is important to enable further fulfillment of the needs of the modern society, while preserving basic human values and protecting the rights of the individual's personality, irrespective of their nationality and place of residence. Regardless of the legal basis for personal data processing, respondents always retain the right to be informed, access to their data, to delete, modify and transfer personal data, and limit the purpose of the processing. However, the right to erase personal data is not an absolute right, but it must be balanced against the legal obligations of the processing manager to keep certain types of data.

Keywords: personal data, sensitive data, processing, respondent, processing manager and administrator, consent, legitimate interest, public interest, health care