Ljuba Slijepčević

Pravosudna akademija

Novi Sad

Dostavljeno radno pravni savetnik 28.5.2022.

Obrada podataka o ličnosti zaposlenih shodno Zakonu o zaštiti podataka o ličnosti i GDPR uz domaću sudsku praksu i praksu ESLJP

Uvod

U Evropskoj uniji je, u 25.5.2018. godine,na snagu stupila Opšta uredba o zaštiti podataka , GDPR koja je podatke o ličnosti stavila pod zaštitu bez presedana. i od tog datuma obavezuje fizička i pravna lica sa prebivalištem, odnosno sedištem u Evropskoj Uniji, ali pod određenim uslovima GDPR ima primenu i u Srbiji. i obveznicima je ostavljeno dve godine da se usaglase sa novim propisima.

Iako se GDPR često predstavlja kao svojevrsna revolucija koja iz korena menja pravila zaštite podataka, nova regulativa ipak je prirodni naslednik EU Direktive 95/46 o zaštiti podataka o ličnosti Obrada podataka o ličnosti zaposlenih podrazumeva svaku radnju koja se preduzima u vezi sa podacima zaposlenih, a shodno Zakonu o zaštiti podataka o ličnosti, poslodavac je dužan da obavesti zaposlenog o obradi njegovih podataka, pre nego što ona i nastupi

Donošenjem i impelmentacijom GDPR regulative, odnosno Zakona o zaštiti podataka o ličnosti[1], Za usklađivanje i pripremu za ovaj zakon ostavljeno je devet meseci tako da zakon počinje da se primenjuje od 21.08.2019. godine. podignuti su standardi u poslovanju kompanija. Aspekt koji je veoma značajan, a kome se ne pridaje velika pažnja su zaposleni i njihovo pravo na privatnost na radnom mestu. Njime se postavljaju daleko viši standardi zaštite u Srbiji, po ugledu na Opštu uredbu EU o zaštiti podataka o ličnosti (dalje: GDPR).

Poseban osvrt zaslužuje obrada podataka o ličnosti zaposlenih od strane poslodavca, što je oblast koju domaće firme najčešće potpuno zanemaruju. Veliki broj poslodavaca ne zna:

da njihovo preduzeće vrši obradu personalnih podataka (zaposlenih, klijenata, kupaca, trećih strana)

da ne smeju instalirati video-nadzor po sopstvenom nahođenju

da je neophodno obavestiti zaposlene o njihovoj obradi podataka ili o instalaciji video nadzora

[1] ("Sl. glasnik RS", br. 87/2018)

da treba da postoji politika privatnosti kojom se detaljno regulišu svi aspekti zaštite podataka o ličnosti

da je njihov nadzor nad radom zaposlenih, ipak, ograničen

Obrada podataka zaposlenih

Iako primarna delatnost Društva ne podrazumeva obradu podataka, ipak u svakom preduzeću postoji obrada podataka o ličnosti.

Šta je to podatak o ličnosti

Shodno ZZPL (što, kako smo rekli predstavlja GDPR u Srbiji), podatak o ličnosti je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta.

Osim ovako određenog podatka o ličnosti Zakon posebno određuje određene kategorije podataka o ličnosti čija obrada je posebno uređena. Tu spadaju:

Genetski podatak:

podatak o ličnosti koji se odnosi na nasleđena ili stečena genetska obeležja fizičkog lica

podatak o ličnosti koji je dobijen analizom iz uzorka biološkog porekla

Biometrijski podatak:

podatak o ličnosti dobijen posebnom tehničkom obradom u vezi sa fizičkim obeležjima

podatak o ličnosti dobijen posebnom tehničkom obradom u vezi sa fiziološkim obeležjima

podatak o ličnosti dobijen posebnom tehničkom obradom u vezi sa ponašanjem fizičkog lica

Podatak o zdravlju:

Podatak o fizičko ili mentalnom zdravlju

Podatak o pružanju zdravstvenih usluga

Podatak kojima se otkriva informacija o zdravstvenom stanju

Ne smemo da zaboravimo zaposlene (pripravnike, lica na stručnoj praksi) i kandidate, čiji se podaci obrađuju prvim kontaktom sa poslodavcem. Budući da obrada podrazumeva svaku radnju koja se preduzima u vezi sa podacima, to dalje povlači da se obradom smatra bilo koja aktivnost: prikupljanje, beleženje, snimanje, analiziranje, korišćenje, prosleđivanje, uništavanje podataka i drugo. Svaki podatak koji ima cilj da identifikuje lice je lični podatak. Dakle, Ime i prezime zaposlenog ili kandidata, svi podaci iz radne biografije (stručna sprema, iskustvo, slika), broj bankovnog računa zaposlenog na koji se vrši isplata mesečne zarade i slično.

Obaveštenje zaposlenog o obradi

pod terminom zaposleni u smislu ovog teksta se smatra, ne samo lice koje je u radnom odnosu već i pripravnici, lica na stručnoj praksi i osposobljavanju, kao i lica koja obavljaju rad van radnog odnosa.

Sve se to smatra obradom podataka o ličnosti pa tako morate i poštovati određene obaveze koje novi Zakon o zaštiti podataka o ličnosti propisuje u tom smislu. Jedna od osnovnih obaveza jeste da sva lica obavestite o prikupljanju njihovih podataka o ličnosti pre nego što počnete sa obradom podataka o ličnosti.

Shodno Zakonu o zaštiti podataka o ličnosti, poslodavac je dužan da obavesti zaposlenog i sva druga lica (klijenti, kupci) o obradi njihovih podataka, pre nego što ona i nastupi. Najadekvatnije je da se obaveštenje za zaposlenog pripremi kao odvojeni dokument i da se priloži prilikom potpisivanja ugovora o radu sa svim neophodnim informacijama, vodeći računa da svi zakosnki uslovi budu ispunjeni. Neophodno je da zaposleni bude obavešten o tome koja je svrha obrade, pravni osnov, vrsta podataka koja se prikuplja, rok čuvanja, koja su njegova prava i drugo.

Podaci koji smeju da se prikupljaju zavise od pravnog osnova i svrhe obrade: naš zakon predviđa šest pravnih osnova za prikupljanje podataka, među kojima je najučestaliji pristanak, ali on nije sasvim adekvatan kad je reč o radnim odnosima jer pristanak podrazumeva dobrovoljnost i slobodu za njegovo davanje. Za to mora postojati ravnopravnost strana koje su u tom odnosu, a to se ne bi moglo reći za odnos poslodavca i zaposlenog. Tako je i davanje saglasnosti zaposlenog za podatke koje poslodavac želi da obrađuje upitno – da li je reč o pristanku ili o prinudi

Osnovi za obradu podataka o ličnosti zaposlenih:

Zakon je predvideo šest osnova za obradu podataka, pri čemu ćemo navesti one koji se najčešće koriste i saglasnost kao najneadekvatniji osnov:

Izvršenje zakonske obaveze – najčešće obrada podataka o ličnosti u vezi sa zakonskim obavezama propisanim Zakonom o radu ili Zakonom o evidencijama u oblasti rada, zakoni koji regulišu zdravstveno, penzijsko, invalidsko osiguranje.

Izvršenje ugovorne obaveze – izvršenje obaveza po osnovu ugovora o radu sa ograničenim brojem podataka koji se obrađuju u navedene svrhe (ime i prezime, broj telefona, e –mail, bankovni račun i sl.)

Legitiman Interes – retko ga treba koristiti kao osnov, a i kada se koristi najčešće je to u pogledu zaštite imovine i sigurnost poslodavca u pogledu poslovanja.

Pristanak – najneadekvatniji osnov. Prvo, u samom odnosu poslodavac – zaposleni postoji odnos suprematije, pri čemu se saglasnost ne bi mogla smatrati slobodnom. Sa druge strane, treba imati u vidu da se saglasnost zaposlenog u svako doba može povući, a to znači da više ne postoji osnov za dalje prikupljanje podataka. kada se daje saglasnost, ona se ne može dati uopšteno za sve obrade, već za tačno i precizno određene obrade. Na početku radnog odnosa sve vrste obrade nije moguće predvideti, pa i nije moguće dati saglasnost unapred.

postupak obrade podataka mora biti potpuno transparentan, a zaposleni mora da zna koje tačno podatke poslodavac obrađuje i u koje svrhe.

Kontrola rada od kuće

Kad je reč o špijunskim softverima koji prikupljaju informacije o zaposlenima, to naravno nije dozvoljeno ni jednim zakonom – čak se kosi i sa osnovnim ljudskim pravima, ali i sa Zakonom o zaštiti podataka o ličnosti i njegovim osnovnim načelima – transparentnošću, poštenjem i informisanošću: da biste nečije podatke obrađivali, ta osoba mora da bude informisana o tome bez obzira na to koji je razlog za prikupljanje podataka.

Kontrola zaposlenih / kandidata preko e maila i društvenih mreža

Poslovni mejl nije privatni, je ono što se obično čuje kao argument u prilog zabludi. Iako poslodavci mogu da nadziru komunikaciju koja se odvija putem poslovnog mejla, postavlja se pitanje da li je taj nadzor potpuno slobodan?

Tačno je da se mejlovi koji su poslati, odnosno primljeni preko mejl adrese poslodavca generalno ne smatraju privatnim. Poslodavac je slobodan da nadzire ovu komunikaciju, ali samo pod uslovom da postoji validan poslovni razlog za takvo postupanje.

U svakom slučaju, poslodavac bi trebalo da reguliše ova pitanja i da obavesti zaposlene, kako bi sve bilo transparentno.

Veliki broj kompanija praktikuje proveravanje kandidata, pa čak i zaposlenih putem društvenih mreža. Treba imati u vidu da sam GDPR, odnosno ZZPL ne regulišu ovo pitanje, ipak postoje tumačenja u kontekstu GDPR-a i javno dostupnih informacija koje zaposleni / kandidati sami učine javno dostupnim putem socijalnih medija (facebook, twiter, instagram.) U tim slučajevima, jedini mogući osnov za obradu mogao biti legitiman interes, s tim da bi postojala obaveza da se pomenutoj kategoriji lica čiji se podaci obrađuju, dostavi obaveštenje o obradi podataka sa svim informacijama propisanim zakonom, posebno ako profil sadrži relevantne informacije za obavljanje posla (karakteristike kandidata, veštine, sposobnosti), a sama lica bi imala pravo da podnesu prigovor na takvu vrstu obrade podataka. GDPR ne reguliše eksplicitno ovo pitanje. Ipak, telo koje se bavi tumačenjem GDPR-a je objavilo svoje mišljenje u kojem navodi da je moguće vršiti ovakve provere, ali pod sledećim uslovima:

1) Kandidati moraju biti obavešteni da ćete proveravati njihove profile na društvenim mrežama (čak iako su podešeni kao javni).

2) Da poslodavac ima zakonit osnov za obradu takvih podataka.

3) Da postoji verovatnoća da profil sadrži informacije o sposobnostima i karakteristikama kandidata koje mogu biti veoma važne za zaposlenje, odnosno obavljanje posla.

4) Poslodavac mora da bude usaglašen sa svim principima koje propisuje GDPR.

Naravno, ovo mišljenje nije obavezujuće. Međutim, preporuke ovog tela imaju značajan uticaj na sudove i druge institucije EU koje primenjuju i tumače GDPR. Kako kod nas još ne postoji relevantna sudska praksa, kao ni odgovarajuća tumačenja, verujemo da će se naši sudovi kao i nadležni državni organi rukovoditi ovim mišljenima i stavovima. Zato bi bilo najbolje da poslodavci počnu da usklađuju svoje postupanje, kako bi se osigurali da je njihovo ponašanje u skladu sa domaćom i evropskom regulativom.

Što se tiče zaposlenih, mogla bi se primeniti ista pravila kao i za kandidate za zaposlenje.

Sa druge strane, postavlja se i pitanje korišćenja društvenih mreža od strane zaposlenih. Najbolje bi bilo da donesete odgovarajući Pravilnik kojim ćete regulisati korišćenje društvenih mreža i naloga od strane zaposlenih, kako biste usmerili njihovo ponašanje.

Uvek morate imati na umu da bilo kakve zabrane nisu moguće i da jedino što možete jeste da pokušate na ljubazan način da usmerite ponašanje Vaših zaposlenih.

Sve je zastupljeniji trend BYOD (Bring your own device) koji podrazumeva da zaposleni koriste sopstvena sredstva za rad, na primer: telefon, laptop, tablet …

Tu se otvara pitanje suprotstavljenih intersa: zaštita poverljivih podataka poslodavca i nadzora rada zaposlenog, sa jedne strane i, zaštita podataka o ličnosti zaposlenog i članova njegove porodice, sa druge strane.

Sam GDPR ne vodi toliko računa o čijim se uređajima radi, tj. u čijem su vlasništvu – na prvom mestu je bezbednost i sigurnost podataka.

To ne znači da Vi kao poslodavac ne treba da brinete, budući da vlasništvo na uređaju može biti od velike važnosti, ako sadrži podatke za koje ste odgovorni. GDPR tretira podatke na računaru Vaše firme isto kao i kada se nalaze na personalnim uređajima zaposlenih – razmislite gde ćete pre čuvati Vaše poverljive podatke.

U svakom slučaju, ne može biti legitimno nadziranje putem uređaja koji mere broj otkucaja na tastaturi, aktivnost ekrana, snimanje preko web kamere i/ili praćenje zvuka putem mikrofona kako bi se pratile aktivnosti zaposlenih. Iako su ovakve tehnologije dostupne, zadiranje u privatnost je prevelika da bi se mogao opravdati ovakav nadzor, čak iako je oprema koju zaposleni koristi u vlasništvu poslodavca.

u svim ovim slučajevima morate voditi računa da ne zadirete u privatnost Vaših zaposlenih, kao i da obrađujete samo one podatke za koje postoji zakonski osnov. Potrebno je da zaposleni uvek budu unapred informisani o sprovođenju nadzora i obradi podataka, jer se u suprotnom, čak i u slučaju postojanja pravila zabrane upotrebe društvenih mreža, telefona i drugih sredstava komunikacije, poslodavac nalazi u opasnoj sferi narušavanja prava iz člana 8. Evropske konvencije o ljudskim pravima.

Video nadzor i zaposleni

Praksa je pokazala da poslodavci prema sopstvenom nahođenju uvode video- nadzor u svoje poslovne prostorije, pri čemu nisu u potpunosti informisani o nužnosti postojanja legitimnog interesa, obaveznosti izrade procene rizika, plana obezbeđenja sa planom tehničke zaštite, angažovanja eksterne organizacije sa licencom za projektovanje, instalaciju, puštanje u rad sistema tehničke zaštite.

Video nadzor je alat za prikupljanje (obradu) podataka o ličnosti kojim se u velikoj meri zadire u privatnost fizičkih lica, ali i druga prava i slobode koja su garantovane Ustavom RS, kao što su pravo na zaštitu podataka o ličnosti i pravo na poštovanje dostojanstva ličnosti na radu.

Da bi ovakva obrada podataka o ličnosti bila zakonita, mora da postoji i pravni osnov i opravdana svrha obrade koja je jasno određena i koja se ne može ostvariti bez poštovanja Zakona o zaštiti podataka o ličnosti kao i Zakona o privatnom obezbeđenju kojim je propisano da se planiranje sistema tehničke zaštite vrši na osnovu procene rizika u zaštiti lica, imovine i poslovanja.

Nadziranje hodnika i nadziranje kancelarija putem video nadzora nije isto. Da bi kancelarijski prostor bio pokriven kamerama, neophodno je da postoji imovina velike vrednosti ili da je u datoj kancelariji smešten glavni server. Postavljanje video nadzora u kancelarije u principu ne narušava privatnost zaposlenog, pod uslovom da su ispunjeni sledeći uslovi:

Da je uočljiv na prvi pogled i da zaposleni znaju za njegovo postojanje (neophodno je da postoji obaveštenje da je objekat pod video-nadzorom i ko vrši datu uslugu obezbeđenja, sa svim neophodnim elementima)

Da se ne nalazi na mestima kao što su svlačionice, toaleti, trpezarije, i slično

Da snima samo video signal

Da biste postavili video nadzor neophodno je da imate legitiman interes za tako nešto. Želite da obezbedite sigurnost Vaše imovine? To bi mogao biti legitiman osnov koji bi imao prevagu nad interesima privatnosti zaposlenog. Međutim, uvek morate postaviti pitanje da li postoji drugo sredstvo koje će manje ugrožavati privatnost zaposlenih, a kojim bi se postigli isti ciljevi. Na primer: postavljanje kamere tako da snima samo ulazna vrata, ali ne i radnu okolinu zaposlenih.

Ukoliko video nadzor za cilj ima isključivo nadzor nad ponašanjem i radnim aktivnostima zaposlenih, takva obrada podataka o ličnosti nije dozvoljena jer se na taj način narušava privatnost zaposlenih.

Saglasnost zaposlenih nije neophodna niti je izričito proklamovana, ali moramo imati na umu da bi saglasnost zaposlenog bila neophodna kada se obrada podataka koristi u svrhe koje nisu predviđene ugovorom, kao što je na primer, upotreba njihove snimljene slike u reklamne svrhe kompanije.

Imajući u vidu prethodno navedeno, neophodno je da kompanija ima legitimni interes. Nakon utvrđivanja legitimnog interesa za obradu podataka o ličnosti, rukovalac – kompanija, bi trebalo da utvrdi obim neophodnosti ličnih podataka. To znači da podaci o ličnosti moraju biti adekvatni, relevantni, i ograničeni samo na ono što je u vezi sa svhom zbog koje se obrađuju, čime se poštuje načelo minimizacije propisano Zakonom.

Video nadzor bi se trebalo koristiti samo ukoliko se svrha obrade podataka o ličnosti ne bi mogla ostvariti drugim sredstvima koja su manje invazivna prema osnovnim pravima i slobodama lica čiji se podaci obrađuju.

Pored video nadzora rukovalac može da preduzme i druge mere za zaštitu imovine i lica, poput angažovanja obezbeđenja, instaliranja boljeg osvetljenja, osnaživanja kapija, ulaznih vrata – odnosno da izvrši detaljnu analizu i procenu i utvrdi da li ove mere za zaštitu od krađa i provala mogu na adekvatan način zameniti video nadzor.

Kamera je bila usmerena direktno na sto tužilje tokom čitavog radnog vremena, kojim radnjama je prema tužilji postupao diskriminatorski u odnosu na druge radnike i čime je ista stavljena u nepovoljniji položaj. Naime, tužilja je ponašanjem direktora tuženog trpela zlostavljanje na radu koje se odvijalo učestalo i u dužem vremenskom periodu, a što je sve kod tužilje dovelo do produženog stresa usled nepodnošljivog radnog okruženja, do slabljenja motivacije, zamora i iscrpljenosti, narušavanja zdravlja, te ličnog ugleda i profesionalnog integriteta

Sudska praksa zaštita pojedinaca od zloupotreba podataka o ličnosti Apelacioni sud u Novom Sadu

“Prvostepeni sud je pravilno delimično usvojio tužbeni zahtev tužilje nalazeći da za rad ustanove, uspostavljanje i održavanje discipline odgovara direktor, te da je osnov odgovornosti tuženog, kao

poslodavca, prema tužilji, kao zaposlenoj, protivpravno postupanje direktora tuženog koje se ogleda u tome što se pored opravdanih opomena upućenih tužilji, obraćao tužilji povišenim glasom i vikanjem pred drugim zaposlenima što je omalovažavao tužilju, nakon čega joj je isključio internet čime je onemogućio da komunicira sa matičnom službom, oduzeo računar sa flet ekranom, tražio od tužilje da jedina dostavljanja nedeljne izveštaje o radu i rasporedio je na drugu lokaciju-drugo mesto rada tj. u izolovani radni prostor gde niko od zaposlenih kod tuženog nije boravio niti radio, te neopravdano prekomerno nadzirao tužilju u radu putem video nadzora (kamera je bila usmerena direktno na sto tužilje tokom čitavog radnog vremena), kojim radnjama je prema tužilji postupao diskriminatorski u odnosu na druge radnike i čime je ista stavljena u nepovoljniji položaj. Naime, tužilja je ponašanjem direktora tuženog trpela zlostavljanje na radu koje se odvijalo učestalo i u dužem vremenskom periodu, a što je sve kod tužilje dovelo do produženog stresa usled nepodnošljivog radnog okruženja, do slabljenja motivacije, zamora i iscrpljenosti, narušavanja zdravlja, te ličnog ugleda i profesionalnog integriteta, zbog čega je dolazilo do čestih odsustva sa rada, a koje je za krajnju posledicu imalo i davanje otkaza ugovora o radu od strane tužilje, pa su svi suprotni žalbeni navodi neosnovani…“ presuda Apelacionog suda u Novom Sadu, Gž1 651/2013 od 15. maja 2013. god.)

Praksa zaštita pojedinaca od zloupotreba podataka o ličnosti Evropskog suda za ljudska prava

Obezbeđivanje garantovanih prava pojedinaca, pa tako i prava na zaštitu podataka, ESLjP sprovodi kroz razmatranje predstavki podnetih od strane pojedinaca koji svoje pravo nisu mogli da ostvare pred nacionalnimpravosudnim i upravnim organima. Kada se ustanovi da je država prekršila jednoili više prava, ESLjP donosi presudu. Presude su obavezujuće, a država na koju se presuda odnosi je u obavezi da deluje u skladu sa odlukom.

ESLjP je do sada doneo niz presuda koje se odnose i na zaštitu pojedinaca od zloupotrebe podataka o ličnosti.

Član 8 EKLjP ima znatno širu primenu nego što je zaštita podatka o ličnosti, pa je ESLjP doneo i niz drugih presuda u vezi sa kršenjem prava na poštovanje privatnog i porodičnog života koje se odnose na zaštitu psihološkog i moralnog integriteta pojedinaca, kao i zaštitu identiteta i autonomije pojedinca.Engleski državljanin Džefri Denis Pek[2] podneo je tužbu protiv UK 1998.godine zbog ugrožavanja prava na privatnost. On je avgusta 1995. godine bolovao od depresije i na ulici je kuhinjskim nožem pokušao da iseče vene i izvrši samoubistvo. Nije znao da ga snimaju kamere za video nadzor instalirane na administrativnoj ustanovi u toj ulici. Na osnovu tog snimka objavljene su dve fotografije, u članku i na naslovnoj strani u lokalnim novinama, a kasnije i u drugim novinama, a lice podnosioca tužbe nije bilo sakriveno na fotografijama.Kasnije je deo video snimka objavljen na više televizija. Pošto je iscrpeo pravna sredstva unutar UK obratio se ESLjP, koji je konstatovao kršenje čl. 8 EKLjP.

Sud nije našao da su postojali opravdani razlozi koji bi dozvolili otkrivanje identiteta, a objavljivanje je izvršeno bez saglasnosti podnosioca tužbe. Sud je smatrao da je objavljivanje snimka predstavljalo nesrazmerno i neopravdano mešanje u privatni život.

[2] Peck v. The United Kingdom (Application no. 44647/98), ECHR, https:// hudoc.echr.coe.int/

eng-press?i= 003-687182- 694690

Državljanin UK Copland v. The United Kingdom [3] podneo je 2000. godine tužbu protiv UK ESLjP zbogkršenja prava privatnosti zbog nadzora korespondencije od strane poslodavca.Podnosilac tužbe je bio zaposlen na državnom koledžu, a tokom trajanja radnog odnosa njegovo korišćenje telefona, e-maila, i interneta bilo je podvrgnuto nadzoru u cilju da se utvrdi da li preterano upotrebljava sredstva u svojini koledža u privatne svrhe. ESLjP je u ovom slučaju došao do zaključka da je došlo do kršenja čl. 8 EKLjP. Podnosilac tužbe nije bio upozoren da će komunikacija koju ima biti praćena i osnovano je očekivao da će njegova privatnost biti zaštićena.

Prema stavu ESLjP za postojanje kršenja čl. 8 EKLjP nebitna je činjenica da podaci do kojih je kolež došao nisu javno objavljeni i nisu upotrebljeni u disciplinskom ili drugom postupku. Sud je zaključio da samo prikupljanje i čuvanje podataka o ličnosti koji se odnose na telefonske pozive, korišćenje elektronske pošte i interneta, bez znanja podnosioca tužbe predstavlja povredunjegovog prava na poštovanje privatnog života u smislu čl. 8 EKLjP.
Uvek se mora voditi po principima neophodnosti i srazmernosti u svakom slučaju obrade podataka. Znači da se mora voditi računa da mere koje se primenjuju budu zaista neophodne i u srazmeri sa svrhom koja se želi ostvariti.

Drugo, transparentnost i otvorenost je neophodna. Zaposleni moraju biti obavešteni o svakoj obradi podataka na jasan i razumljiv način.

Treće, obrada podataka mora biti fer prema zaposlenom. Da bi se prava pojedinaca na zaštitu ličnih podataka ostvarila, neophodno je da svi oni koji prikupljaju i obrađuju podatke u različite svrhe, kao rukovaoci i obrađivači, preduzmu sve neophodne mere kako bi uskladili svoje poslovanje sa najvišim standardima u oblasti zaštite podataka o ličnosti. Razlozi za ovakvo postupanje rukovalaca i obrađivača nisu samo ozbiljne posledice koje nastupaju zbog neusaglašenosti sa propisima o zaštiti podataka, već i potreba podizanja nivoa društvene odgovornosti. Delotvornost pravnih lekova meri se efikasnom primenom istih.

Literatura:

1.Diligenski Andrej, Prlja Dragan, Cerović Dražen, Pravo zaštite podataka- GDPR,

Institut za uporedno pravo, Beograd 2018.

2.Debeljački Milorad, “Zakon o zaštiti podataka o ličnosti: radna grupa za izradu

nacrta”, PravoIkt, online 2016., https://pravoikt.org/zakon-o-zastitipodataka-o-licnosti-radna-grupa-za-izradu-nacrta/

3.Jašarević Senad, Zaštita ličnih podataka zaposlenih u srpskom i evropskom pravu,

Zbornik radova Pravnog fakultet u Novom Sadu, br. 2/2009, Novi Sad, 2009.

[3] (Application no. 62617/00), ECHR, https://hudoc. echr.coe. int/