VODIČ KROZ ZAKON O ZAŠTITI PODATAKA O LIČNOSTI I GDPR

TUMAČENJE NOVOG PRAVNOG OKVIRA

SHARE FOUNDATION

OEBS Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

Шведска
Sverige

VODIČ KROZ ZAKON O ZAŠTITI PODATAKA O LIČNOSTI I GDPR

TUMAČENJE NOVOG PRAVNOG OKVIRA

VODIČ KROZ ZAKON O ZAŠTITI PODATAKA O LIČNOSTI I GDPR
TUMAČENJE NOVOG PRAVNOG OKVIRA

UREDNIK
DANILO KRIVOKAPIĆ

AUTORI
DANILO KRIVOKAPIĆ
JELENA ADAMOVIĆ
DUNJA TASIĆ
ANDREJ PETROVSKI
PETAR KALEZIĆ
DR ĐORĐE KRIVOKAPIĆ

IZDAVAČI
MISIJA OEBS-A U SRBIJI
SHARE FONDACIJA

OBRADA TEKSTA
MILICA JOVANOVIĆ

DIZAJN
OLIVIA SOLIS VILLAVERDE

PRELOM
UNDERDOG

ŠTAMPA
FIDUCIA 011 PRINT D.O.O.

TIRAŽ
200 PRIMERAKA

ISBN 978-86-6383-084-4

Publikacija je izrađena uz finansijsku podršku Švedske agencije za međunarodnu razvojnu saradnju, u okviru projekta Konsolidovanje procesa demokratizacije u sektoru bezbednosti u Republici Srbiji.

SADRŽAJ

INDEKS POJMOVA I SKRAĆENICA

Kolačići - eng. *cookies*, komadići podataka koje internet sajtovi razmenjuju sa korisničkim uređajem za kratkoročno pamćenje aktivnosti korisnika na sajtu.

Kolačići trekeri - eng. *tracker cookies*, posebna vrsta kolačića koja se koristi za dugoročno pamćenje aktivnosti korisnika, njihovo profilisanje na osnovu ponašanja, posebno preko trekera treće strane. Spadaju u vrste kolačića koji nisu neophodni za korišćenje onlajn servisa i kao takvi podložni su odredbama GDPR o informisanom pristanku.

Opt in - Predefinisani model odnosa sa korisnicima koji podrazumeva aktiviranje usluge tek pošto korisnici izraze izričitu saglasnost.

Opt out - Predefinisani model odnosa sa korisnicima koji podrazumeva da automatski aktivirana usluga prestaje tek pošto korisnici to izričito zatraže.

Podrazumevana privatnost - eng. *privacy by default*, privatnost po difoltu, predefinisana privatnost; pristup prodaji ili distribuciji koji podrazumeva da su standardna podešavanja proizvoda ili usluge postavljena tako da štite privatnost.

Policijska direktiva - Direktiva EU 2016/680 o zaštiti pojedinaca u vezi s obradom podataka o ličnosti od strane nadležnih organa u svrhe sprečavanja, istrage, otkrivanja ili progona krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka.

Politike privatnosti – eng. *privacy policy*, dokument o privatnosti, izjava ili pravni dokument koji sadrži informacije o načinu i svrsi prikupljanja i obrade ličnih podataka, obavezama rukovaoca i pravima građana.

Poverenik - Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti.

Radna grupa 29 - Radna grupa za zaštitu pojedinaca u vezi sa obradom podataka o ličnosti.

Ugrađena privatnost - eng. *privacy by design*, privatnost po dizajnu; pristup izgradnji, programiranju, oblikovanju, razvoju, itd. hardvera ili softvera, koji podrazumeva da je zaštita privatnosti korisnika integralni deo uređaja, programa ili sistema.

CJEU - Court of Justice of the European Union, Sud pravde Evropske unije

EDPB - European Data Protection Board, Evropski odbor za zaštitu podataka

EDPS - European Data Protection Supervisor, Evropski supervizor za zaštitu podataka o ličnosti

EU – European Union, Evropska unija

GDPR – General Data Protection Directive, Opšta uredba o zaštiti podataka

ICO - Information Commissioner's Office, Služba poverenika za informacije (UK)

IMEI - International Mobile Equipment Identity, međunarodni identitet mobilnog uređaja

IP – internet protokol

JMBG – jedinstveni matični broj građana

ZSPIJZ - Zakon o slobodnom pristupu informacijama od javnog značaja

ZZPL – Zakon o zaštiti podataka o ličnosti

PREDGOVOR

Sveprisutno računarstvo, umreženost, Veliki podaci, primena senzora, 3D štampa i digitalna fabrikacija, IoT, roboti, veštačka inteligencija, blokčejn, virtuelna realnost... samo su neka od rešenja u kojima mnogi vide razlog za proslavu uveliko prisutne Četvrte industrijske revolucije. Tehnologija je osvojila sve sfere našeg života, obećanjem da će nam unaprediti kvalitet života, pomoći nam da optimizujemo korišćenje resursa, smanjiti troškove, povećati produktivnost, obezbediti više slobodnog vremena, podići nivo bezbednosti.

Industrija 4.0 ide korak dalje, obećava eksponencijalni rast i zamućuje granice „fizičkog, digitalnog i biološkog sveta, utičući na sve discipline, ekonomije i industrije, pa čak i osporavajući ideje o tome šta znači biti čovek".[1]

Za razliku od prethodnih, Četvrta se industrijska revolucija razvija munjevitom brzinom, bez presedana u istoriji. Njen radikalni uticaj na gotovo svaku industriju, u svakoj državi sveta, menja čitave sisteme proizvodnje, poslovanja i javne uprave, što jasno govori da smo zakoračili u nepoznate vode – a da jedva imamo vremena da se osvrnemo oko sebe.

Poslovne organizacije pokrenute na ovim osnovama ubrzo su postale tehnološki giganti i najvrednije svetske kompanije. *Amazon*, *Apple*, *Facebook* i *Google* su po svojoj vrednosti i moći prestigle stare transnacionalne kompanije iz sektora finansija, energetike i automobilske industrije. Iako je deo poslovanja ovih kompanija vezan za proizvodnju i prodaju hardvera i licenciranje softvera, poslovni modeli koji su im omogućili ubrzani rast, uz razarajući efekat na postojeća tržišta, značajno su evoluirali. Neki od najvrednijih proizvoda ovih kompanija, poput Fejsbukove društvene mreže i Gugl pretraživača i mapa, kojima se svakodnevno služe milijarde ljudi, "besplatni" su za korišćenje i praktično se ne mogu platiti novcem.

Inovativni poslovni modeli zasnovani su na primeni informacionih tehnologija za korišćenje velikih količina prikupljenih ili generisanih podataka. S druge strane, jedan od bitnijih činilaca Industrije 4.0 jeste i koncept koji prožima gotovo sve oblasti savremenog društva – digitalna transformacija (DX). Kao oličenje susreta novih poslovnih vrednosti i vrhunskih tehnoloških mogućnosti, DX predstavlja najavu da svet nije prepušten samo inovativnim i brzorastućim kompanijama, rođenim u digitalnoj eri. DX pruža viziju u kojoj i tradicionalni biznisi, uključujući čitave industrije ali i javni sektor, imaju šansu da se prilagode promenama i ostanu (ili postanu) relevantni u 21. veku.

Kao poseban akter u oblasti digitalne transformacije javlja se i sama država koja je, zahvaljujući galopirajućem razvoju tehnologija i njihovom uticaju na tržište i društvo, već izgubila deo suvereniteta u korist tehnoloških giganata. Kako bi povratila moć i ostala relevantna u čitavom nizu društvenih sfera, država se na svim nivoima digitalizuje i transformiše. Mada sa zakašnjenjem, suveren ubrzano stvara glomazne sisteme za elektronsku upravu i pružanje usluga građanima elektronskim putem.

Industrija 4.0 ne bi bila moguća bez upotrebe velikih količina podataka u poslovanju. Posebno su značajni oni podaci koji nastaju tokom upotrebe svih raspoloživih digitalnih rešenja. Obrada podataka se vrši sa ciljem kreiranja novih vrednosti, koje mogu da pomognu da odluke u okviru organizacije budu smislenije, da optimizuje i poboljša postojeće procese, ili da predvidi nova stanja i dešavanja.

U Industriji 4.0, podaci igraju dvostruku ulogu. Prikupljeni i generisani podaci se analiziraju, agregiraju, ukrštaju, u potrazi za paternima i novim uvidima koji potkrepljuju poslovne ideje i inicijative. S tim u vezi, prikupljeni i generisani podaci se pre svega mogu posmatrati kao sred-

1 World Economic Forum, The Fourth Industrial Revolution, by Klaus Schwab, dostupno na: weforum.org

stva uz pomoć kojih donosimo informisanije odluke pri radu. Drugu ulogu podaci igraju kao resursi koji nastaju dok se u svom svakodnevnom radu služimo različitim digitalnim rešenjima (eng. *Digital data footprint*).

Pretpostavku za razvoj Industrije 4.0 čini tehnička infrastruktura koja omogućava prikupljanje, strukturiranje, kategorizaciju, analizu i distribuciju raznovrsnih i veoma obimnih tokova podataka različitog kvaliteta (*Big data*). Sve to utiče na okolnost da savremene organizacije pretežno investiraju u digitalne komunikacije, kolaborativne alate, okvir za upravljanje podacima i digitalnu bezbednost.[2]

Upotrebna, a shodno tome i ekonomska vrednost podataka raste s njihovim obimom i kvalitetom. Što su specifičnije informacije čiju ekstrakciju omogućavaju podaci, to je veća šansa da će im se naći komercijalna primena. Kao resurs nove ekonomije, podaci su, poput informacija, po mnogo kriterijuma vrlo specifični.[3] Njihova proizvodnja često nije sama sebi svrha. Oni nastaju kao posledica čitavog niza operacija, a njihovo beleženje i čuvanje obično ne zahteva posebne dodatne resurse. Tako su podaci nusproizvod najrazličitijih procesa u digitalnom ekosistemu, vrlo često bez razumevanja da mogu biti naknadno iskorišćeni.

Zahvaljujući digitalnim tehnologijama, troškovi multiplikovanja, odnosno umnožavanja podataka i njihovog transfera trećim licima praktično su nepostojeći. U okviru informacionih sistema, umnožavanje podataka se odvija konstantno i nesvesno, a svako davanje ovlašćenja za pristup podacima potencijalno ih multiplikuje.

Dodatno, za razliku od ostalih dobara, podaci se ne mogu potrošiti. Njihovo korišćenje ni na koji način ne umanjuje njihov obim i kvalitet, već ih zapravo poboljšava. Korišćenje podataka omogućava da se prepoznaju i otklone svi eventualni nedostaci njihovog kvaliteta, kao i da se kontinuirano proizvode dodatni podaci koji osnovnim samo povećavaju kvalitet i upotrebljivost.

U okviru savremene ekonomije, koja se sve češće naziva ekonomijom podataka, podaci su postali svojevrsna valuta. Digitalni servisi na kojima građani provode najviše vremena, ne mogu se platiti novcem. Usluge društvenih mreža ili pretrage sadržaja plaćamo sopstvenim podacima na osnovu ugovora koje olako zaključujemo, prihvatajući uslove korišćenja usluga. U nedostatku svesti, često nismo u stanju da razaznamo da neke mobilne aplikacije koje praktično pružaju istovetne usluge, na primer usluge pretrage (*Google*, *Bing* i *DuckDuckGo*), zadržavaju pravo da sa naših mobilnih uređaja preuzmu prilično različite vrste i količine podataka i koriste ih za svoje dalje poslovanje.

Kao roba, podaci postaju predmet raznovrsnih poslovnih transakcija. Trgovci podacima se razvijaju u svim sektorima, nudeći zainteresovanim stranama sirove podatke ili njihove informacione derivate.

Tako su podaci postali ključni resurs digitalne ekonomije. Svaka od tehnologija koje pokreću Industriju 4.0, mora koristiti podatke u velikim količinama kao pogonsko gorivo. Konkurentska prednost koju pruža usavršavanje veštačke inteligencije, može biti zasnovana samo na pristupu velikim podacima, neophodnim za treniranje algoritama putem naprednih metoda mašinskog učenja.

Evropska unija prepoznaje značaj podataka kao ključnog resursa za ekonomski razvoj, konkurentnost, inovacije, stvaranje novih poslova i ukupan društveni napredak. Izgradnja ekonomije podataka jedan je od stubova razvoja jedinstvenog digitalnog tržišta Evrope. Procenjena vrednost evropske ekonomije podataka u 2016. godini iznosila je 300 milijardi EUR, što je činilo 1.99% evropskog društvenog dohotka. Očekuje se da će ubrzani rast u ovom segmentu dovesti do rasta obima ekonomije podataka do 2020. godine na iznos od 739 milijardi EUR, što će predstavljati 4% evropskog GDP.[4] Nastojeći da kreira stimulativno okruženje za razvoj novih proizvoda i usluga zasnovanih na podacima, EU teži da pospeši što širu upotrebu raspolo-

2 Schwab, K., 2016, The Fourth Industrial Revolution, World Economic Forum
3 Više o specifičnostima podataka: Lazović, V., Đuričković, T., 2018, Digitalna ekonomija, Miba Books
4 IDC 2017, European Data Market Study, Final Report, dostupno na: ec.europa.eu

živih podataka. To čini kroz mere koje olakšavaju pristup i uklanjaju prepreke za dalju upotrebu određenih kategorija podataka, poput podataka u posedu javnog ali i privatnog sektora, kao i kroz eliminaciju postojećih barijera za razmenu podataka u okviru evropskog ekonomskog prostora.

Bitan preduslov za održivi razvoj ekonomije podataka jeste i uspostavljanje poverenja u digitalnu ekonomiju i nove poslovne modele zasnovane na podacima. Naime, kada neki resurs ima takvu vrednost i donosi toliko moći, već i njegova zloupotreba ili neadekvatna upotreba može prouzrokovati nenadoknadive posledice (i nafta kad procuri nastaje višestruka šteta). Shodno tome, neophodno je da svakoj obradi podataka prethode ozbiljne procene rizika, a da je prati primena adekvatnih organizacionih i tehničkih mera. Posebno ukoliko je u pitanju obrada podataka o ličnosti, a naročito obrada osetljivih kategorija podataka o ličnosti, kao i sistemi masovnog nadzora, profilisanje i automatizacija procesa zasnovanih na takvim podacima.

Osnovni rizik koji sa sobom nose Industrija 4.0 i digitalna transformacija, tiče se privatnosti i bezbednosti građana. Lakoća s kojom prihvatamo nove tehnologije u svakodnevnom životu i prostorima koji su nekada predstavljali tvrđavu privatnog života, poput porodičnog doma, nameće nove izazove s kojima se kao društvo moramo suočiti. I pored svih poboljšanja životnog standarda koje donose proizvodi i usluge zasnovani na podacima, ni na koji način se ne može opravdati odbacivanje privatnosti kao osnovnog prava i odricanje građana od ovlašćenja da kontrolišu ko, za koje svrhe i na koji način obrađuje njihove podatke o ličnosti.

Neobično brz razvoj i implementacija tehnogija za prikupljanje, skladištenje i obradu podataka, uključujući razvoj poslovne inteligencije i mašinskog učenja, izazivaju bojazan da će se 'nedobronamernim licima' omogućiti sveobuhvatna slika o svakom pojedincu bez njihovog znanja. Rizik da ovako moćne alate poseduju određene kompanije i države svakako treba uzeti sa najvećim oprezom, ali to ne znači da ćemo olako napustiti prednosti koje obrada podataka o ličnosti može doneti, naročito ukoliko je transparentna i adekvatno uređena.

Vodič kroz novu pravnu regulativu, evropsku i domaću, koji je pripremila SHARE Fondacija na osnovu višegodišnjih istraživanja i praktičnog iskustva u usaglašavanju sa propisima u oblasti zaštite podataka o ličnosti, predstavlja dragocen alat i za privatni i za javni sektor - koji će u narednom periodu kreirati inovativne proizvode ili nastojati da, kroz digitalnu transformaciju, zadrže relevantnost sopstvenog poslovanja.

dr Đorđe Krivokapić
Beograd, marta 2019.

NOVO DOBA ZAŠTITE PODATAKA O LIČNOSTI

NOVO DOBA ZAŠTITE PODATAKA O LIČNOSTI

OPŠTA UREDBA O ZAŠTITI PODATAKA

U Evropskoj uniji je, u maju 2018. godine, na snagu stupila Opšta uredba o zaštiti podataka koja je podatke o ličnosti stavila pod zaštitu bez presedana.[5] Bilo je to finale dugogodišnjeg procesa: usaglašavanje konačne verzije teksta trajalo je četiri godine (2012-2016), na sam tekst podneto je rekordnih 4000 amandmana, dok su u javnoj raspravi učestvovali gotovo svi relevantni akteri iz javnog, privatnog i civilnog sektora. Nakon što je regulativa usvojena, maja 2016, državama članicama EU 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[6] i suštinski se nadovezuje na iste principe i norme. S druge strane, regulatori su iskoristili priliku da dodatno urede brojna sporna pitanja nastala tokom razvoja interneta i novih tehnologija, u pokušaju da obnove narušeni balans a građanima omoguće da povrate kontrolu nad svojim podacima. Kako je reč o vrlo kompleksnoj i sveobuhvatnoj regulativi, iz njene primene tek se očekuju preciznija tumačenja.

Značajna težnja GDPR-a jeste usaglašavanje pravila među članicama EU, s obzirom na to da je prethodna Direktiva 95/46 služila pre svega kao smernica za nacionalne zakone, uz preširok prostor za njeno prilagođavanje unutrašnjim prilikama, što je neminovno vodilo ka nejednakom stepenu zaštite ovog bitnog prava. Iako se GDPR direktno primenjuje u svih 28 članica, EU i dalje ostavlja prostor državama članicama da mnoge detalje samostalno regulišu u skladu sa svojim nacionalnim propisima. Takođe, GDPR štiti prava građana EU, što znači da se njegove odredbe odnose na svaku organizaciju u svetu koja obrađuje podatke stanovnika zemalja članica EU, bilo da im nudi robu i usluge ili prati njihovo ponašanje na internetu. Na ovaj način je pristup najvećem tržištu na svetu posredno uslovljen poslovanjem usklađenim sa novom regulativom, bez obzira da li je reč o javnim ili privatnim organizacijama, pristupu grantovima, stručnoj saradnji i slično.

NOVI ZAKON O ZAŠTITI PODATAKA O LIČNOSTI

U Srbiji je novi propis o zaštiti podataka o ličnosti usvojen u novembru 2018. sa odloženom primenom od devet meseci, počev od avgusta 2019. godine.[7] Tekst u najvećoj meri predstavlja adaptirani prevod GDPR-a kao i tzv. Policijske direktive[8] koja uređuje obradu podataka o ličnosti od strane nadležnih organa u vezi sa krivičnim postupcima i pretnjama nacional-

5 Iako se odnosi na engleski naziv, General Data Protection Regulation, GDPR je skraćenica koju ćemo koristiti u ovom tekstu, budući da je u tom obliku već u širokoj upotrebi kod nas. Integralni tekst evropskog propisa dostupan je u prevodu na hrvatski jezik, na adresi: eur-lex.europa.eu

6 Direktiva EU 95/46/EC o zaštiti podataka o ličnosti, tekst dostupan na: eur-lex.europa.eu

7 Zakon o zaštiti podataka o ličnosti ("Sl. glasnik RS", br. 87/2018), dostupan na: parlament.gov.rs

8 Direktiva EU 2016/680 o zaštiti pojedinaca u vezi s obradom podataka o ličnosti od strane nadležnih organa u svrhe sprečavanja, istrage, otkrivanja ili progona krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka, dostupna na hrvatskom jeziku na: eur-lex.europa.eu

noj bezbednosti. Stoga se može smatrati da su načela GDPR-a (i Policijske direktive) uvedena na domaći teren.

Nedostaci novog Zakona o zaštiti podataka o ličnosti (ZZPL) su brojni, a pre svega se odnose na nejasne odredbe i prepisane mehanizme koji ne postoje u domaćem pravnom sistemu, što dovodi u pitanje njegovu primenjivost. Ipak, značajno je napomenuti da ovakav Zakon, makar i samo normativno, predstavlja najviši standard zaštite podataka o ličnosti. Pre ili kasnije, manjkavosti i praznine će biti rešeni naknadnim intervencijama, dok će značajne pravne inovacije ostati ugrađene u naš sistem zaštite ljudskih prava. Po svoj prilici će se i tumačenje domaćeg Zakona ugledati na primenu evropskog propisa, čije su namere izražene u Preambuli, počev od potvrde da je zaštita ličnih podataka jedno od temeljnih ljudskih prava.

ŠTA JE NOVO U NOVOM PRAVNOM OKVIRU?

Većina osnovnih principa novog pravnog okvira nije novina, s obzirom na to da se oslanja na instrumente zaštite ličnih podataka iz doba papira i fascikli. Novost je u tome što su ovi principi dobili izričitu primenu na promet robe i usluga na internetu, a konačno je otvoreno i sporno pitanje regulisanja automatizovane obrade podataka i tzv. algoritamskog odlučivanja. Takođe, proširena je odgovornost ljudi i organizacija koji prikupljaju i obrađuju podatke, detaljno su razrađeni instrumenti i procedure sprovođenja propisa, dok su kazne drakonske i mogu iznositi i do 20 miliona evra ili 4% globalnog godišnjeg obrta, pri čemu se prednost daje višem iznosu. Mada domaći Zakon predviđa više kazne nego ranije, one ni približno nisu tako visoke kao prema GDPR. Tako će rukovaoci u prekršajnom postupku rizikovati kazne od najviše 2.000.000 dinara po pojedinačnom prekršaju, dok je najmanja zaprećena novčana kazna za prekršaje iz ove oblasti 50.000 dinara.

Osnovni cilj novih pravila jeste da se građanima omogući da povrate kontrolu nad svojim podacima. Propisani su novi uslovi za pristanak na obradu podataka, te više neće biti moguće davati blanko saglasnost, niti će se prihvatanje komplikovanih i prosečnom korisniku nerazumljivih politika privatnosti smatrati validnim pristankom. Iako se odnose na svaku vrstu obrade ličnih podataka, u analognom ili digitalnom okruženju, stroge norme Uredbe ciljaju pre svega na zauzdavanje ekonomije podataka, zbog čega im se već prognozira najradikalniji uticaj na internet u njegovoj istoriji. U senci panike u poslovnom sektoru, ostala je činjenica da je GDPR jedan od prvih propisa koji teži da reguliše kompleksne odnose na internetu, koji su do sada uspešno izmicali normiranju.

S obzirom na prilično nisku kulturu zaštite ličnih podataka u Srbiji i retku primenu propisa iz ove oblasti, svako pravilo nove regulative verovatno predstavlja novost za mnoge kompanije, ali i državne institucije. Usklađivanje njihovog poslovanja stoga praktično počinje ispočetka.

TUMAČENJE ZAKONA

Brojni koncepti novog Zakona, prepisani iz evropske regulative, nisu poznati domaćem pravnom sistemu, pa je novi propis zasad jedino moguće tumačiti na isti način na koji se tumače norme GDPR-a, za šta već postoji čitav niz instrumenata.

PREAMBULA GDPR

Integralni deo nove evropske regulative, Preambula se sastoji od čak 173 tačke koje dodatno razrađuju pravne norme i pojašnjavaju cilj svih odredbi GDPR-a, počev od tačke 1 koja definiše zaštitu podataka o ličnosti kao fundamentalno ljudsko pravo. Preambula je stoga ne samo korisna, već predstavlja neophodno polazište za tumačenje propisa. Domaći Zakon nije preuzeo Preambulu GDPR.

RADNA GRUPA 29 I EVROPSKI ODBOR ZA ZAŠTITU PODATAKA

Već je prilikom usvajanja stare Direktive 95/46 bilo jasno da je usaglašavanje tumačenja propisa presudno za njegovu primenu, pa je članom 29 bilo predviđeno osnivanje Radne grupe za zaštitu pojedinaca u vezi s obradom podataka o ličnosti, koja je postala poznata kao "Radna grupa 29". Grupu su činili predstavnici organa za zaštitu podataka o ličnosti iz država članica EU, a tokom godina je izradila i usvojila brojna mišljenja i smernice u kojima je detaljno obrađen čitav niz kompleksnih pitanja, počev od samog koncepta podatka o ličnosti, statusa rukovaoca i obrađivača, pravila za validan pristanak i tome slično.

Stupanjem na snagu GDPR-a, Radna grupa 29 je zamenjena Evropskim odborom za zaštitu podataka (EDPB) čiji je osnovni zadatak da doprinese ujednačenoj primeni pravila širom EU, te suštinski ima isti mandat kao i Radna grupa 29.[9] EDPB je već počeo sa izdavanjem mišljenja i smernica koje će biti ključne za razumevanje novih pravila o zaštiti podataka o ličnosti.

Takođe, sva mišljenja i smernice koje je izdala Radna grupa 29 i dalje su relevantna, ukoliko nisu u suprotnosti sa novim pravilima koje predviđa GDPR.

ODLUKE SUDA PRAVDE EVROPSKE UNIJE

Sud pravde Evropske unije tumači pravo Unije, čime se obezbeđuje ujednačena primena zakona u svim državama članicama. U skladu sa svojim mandatom, Sud je tokom godina doneo niz odluka koje su imale značajnu ulogu za tumačenje i primenu normi zaštite podataka. Jedna od najpoznatijih odluka Suda iz domena odnosa u onlajn sferi, svakako je ona u slučaju *Google Spain v. AEPD and Mario Costeja González* kojom je 2014. ustanovljeno tzv. pravo na zaborav. GDPR je potom ovo pravo uključio u regulatorni korpus zaštite.

PRAKSA NADLEŽNOG ORGANA ZA ZAŠTITU PODATAKA

Iako se GDPR direktno primenjuje u svih 28 članica EU, u svakoj od ovih zemalja postoji nezavisni nadzorni organ za zaštitu podataka o ličnosti koji samostalno prati primenu pravila o zaštiti podataka o ličnosti i ima ovlašćenja da izdaje mišljenja, sprovodi istrage, vodi postupke, izriče upozorenja i kazne, i drugo. Nadzorni organi su u načelu najoperativniji deo nacionalne administracije koja se bavi zaštitom podataka o ličnosti i do danas je već svaki od njih razvio obimnu praksu u tumačenju i primeni pravila. Neretko su ovi organi izuzetno proaktivni, dok je služba britanskog Povereništva za informacije (ICO) jedna od najproduktivnijih u izradi praktičnih mišljenja i smernica.[10]

U Srbiji, ulogu nadzornog organa ima Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti koji je razvio značajnu praksu kroz brojna mišljenja i odluke u postpucima nadzora, a koje se redovno objavljuju na sajtu Poverenika.

9 European Data Protection Board: edpb.europa.eu
10 Information Commissioner's Office: ico.org.uk

OBIM PRIMENE ZAKONA

OBIM PRIMENE ZAKONA

MATERIJALNA PRIMENA

Zakon se primenjuje na obradu podataka o ličnosti koja se, u celini ili delimično, vrši na automatizovan način, kao i na neautomatizovanu obradu podataka o ličnosti koji čine deo zbirke podataka ili su namenjeni zbirci podataka. Pod automatizovanom obradom se podrazumeva korišćenje tehnologije koja dozvoljava automatsku obradu podataka, poput kompjuterskih i drugih elektronskih uređaja koji mogu da prikupljaju, skladište, manipulišu i distribuiraju podatke, kako bi na brz i efikasan način obrađivali veće količine podataka uz minimalno učešće čoveka.

Izvan domena Zakona ostaje obrada podataka o ličnosti koju vrši fizičko lice za svoje lične potrebe, odnosno potrebe svog domaćinstva. Na primer, osoba koja u svom mobilnom telefonu ima telefonske brojeve i imena, a koje koristi za ličnu upotrebu, ne smatra se rukovaocem niti će morati da se pridržava obaveza koje ZZPL predviđa. Međutim, ukoliko fizičko lice obrađuje podatke na automatizovan način (koristeći, na primer, neki kompjuterski program), ili obrađuje podatke na neautomatizovan način tako što ih razvrstava u zbirke podataka da bi te podatke koristilo za neke poslovne, a ne lične potrebe, takvo će se lice smatrati rukovaocem ili obrađivačem pa će, samim tim, morati da ispuni niz zakonskih obaveza.

Zakon se ne primenjuje ni na neautomatizovanu obradu podataka o ličnosti koji ne čine zbirku ili deo zbirke podataka o ličnosti. Ukoliko u ormaru imamo kutiju raznih dokumenata od kojih neki sadrže podatke o ličnosti, radi se o neautomatizovanoj obradi podataka koji ne čine zbirku jer nisu sistematizovani i strukturno organizovani tako da im se može pristupiti ili da se mogu pretraživati po nekom kriterijumu, već su nasumično poslagani u kutiju. Međutim, kada bismo te papire strukturisali tako da oni čine pretraživu zbirku podataka o ličnosti, onda bi se ZZPL primenjivao na njihovu obradu.

Definicija materijalne primene Zakona je, dakle, prilično široka - ZZPL se ne primenjuje na onu obradu podataka o ličnosti koju vrši fizičko lice za svoje privatne potrebe ili potrebe svog domaćinstva, niti se primenjuje na neautomatizovanu obradu podataka o ličnosti koji ne čine zbirku podataka. U ostalim slučajevima, važi primena ZZPL.

TERITORIJALNA PRIMENA

Zakon se primenjuje na obradu podataka koju vrši rukovalac ili obrađivač sa sedištem, odnosno prebivalištem ili boravištem na teritoriji Republike Srbije, u okviru aktivnosti koje se vrše na teritoriji Republike Srbije, bez obzira da li se sama radnja obrade vrši na toj teritoriji. U slučaju rukovaoca sa sedištem u Srbiji, na primer, čiji se server sa podacima koje obrađuje za potrebe svog poslovanja nalazi izvan Srbije, nadležnost Zakona je nesumnjiva i rukovalac je u obavezi da se pridržava odredaba ZZPL i u odnosu na podatke koji se čuvaju na serveru van teritorije Srbije. Dakle, bez obzira na to gde se obrada dešava, ukoliko je obrada vezana za aktivnosti koje domaći rukovalac sprovodi u Srbiji, Zakon se primenjuje na takvu obradu.

Zakon predviđa i eksteritorijalnu primenu i to u slučaju kada rukovalac, odnosno obrađivač koji nema sedište, prebivalište ili boravište na teritoriji Srbije, obrađuje lične podatke lica sa prebivalištem ili boravištem u Srbiji, ako su radnje obrade vezane za:

- ponudu robe, odnosno usluge licu na koje se podaci odnose na teritoriji Republike Srbije, bez obzira da li se od

tog lica zahteva plaćanje naknade za ovu robu, odnosno uslugu; ili

- praćenje aktivnosti lica na koje se podaci odnose, ako se aktivnosti vrše na teritoriji Republike Srbije.

Dakle, ZZPL se primenjuje na inostrane rukovaoce i obrađivače, odnosno one koji u inostranstvu imaju sedište, prebivalište ili boravište, ukoliko oni targetiraju stanovnike Srbije, radi prodaje robe ili nuđenja usluga, odnosno praćenja njihovih aktivnosti na teritoriji Srbije. Slično predviđa i GDPR, s tim da se on odnosi na rukovaoce i obrađivače van teritorije EU koji nude robe i usluge stanovnicima EU, odnosno na rukovaoce i obrađivače koji vrše monitoring aktivnosti lica ukoliko se takve aktivnosti vrše na teritoriji EU.

Smernice

U svojim Smernicama 3/2018 o teritorijalnoj primeni regulative, EDPB navodi da činjenica obrade podataka fizičkog lica u EU od strane rukovaoca ili obrađivača van EU nije dovoljna za primenu GDPR-a.[11] Za to je potreban element *targetiranja* lica u EU tako što im se nude roba ili usluge, ili tako što se vrši monitoring njihovog ponašanja (na primer, koriste se *kolačići trekeri*). Ukoliko kineski sajt, na primer, prodaje robu tako što koristi neki od jezika koji se govore u EU, dozvoljava plaćanje u evropskoj valuti i omogućava dostavu na evropsku adresu naručioca, GDPR bi se eksteritorijalno primenjivao na rukovaoca podacima koje ovaj sajt prikuplja. Međutim, ukoliko neka kineska banka za klijenta ima danskog državljanina sa prebivalištem u Kini, pri čemu je banka aktivna isključivo u Kini bez poslovnih aktivnosti usmerenih na EU tržište, na obradu ličnih podataka danskog građanina neće se primenjivati GDPR.

Na ovakvo tumačenje bi se trebalo osloniti i u slučaju eksteritorijalne primene domaćeg Zakona.

Dileme

Da li se ZZPL primenjuje na kompaniju koja ima sedište van Srbije, ali obrađuje podatke građana Srbije?

Odgovor na ovo pitanje zavisi od nekoliko okolnosti. Ukoliko kao primer uzmemo hotel iz Mađarske u koji dođe naš građanin i ostavi svoje lične podatke, Zakon će se primenjivati na rukovaoca iz Mađarske samo ukoliko taj hotel na neki način targetira građane Srbije - na primer, ima verziju veb sajta na srpskom jeziku, ima marketinšku strategiju za ljude iz Srbije, itd. Ukoliko se, pak, radi o mađarskom hotelu koji nema sajt na srpskom jeziku, ne reklamira se na srpskom tržištu i ne targetira na taj način građane Srbije, odnosno građanin Srbije je slučajno odabrao taj hotel, Zakon se ne primenjuje na rukovaoca iz Mađarske. Za eksteritorijalnu primenu je, dakle, presudno da postoji element usmerenosti poslovanja na građane Srbije, odnosno praćenja njihovih aktivnosti.

Kako će nadležni organi Srbije prinuditi inostrane entitete da poštuju domaći Zakon?

ZZPL ne predviđa mehanizme za primenu u inostranstvu, odnosno ona zavisi od međunarodnih sporazuma. Delimičan oslonac za građane i organizacije iz Srbije predstavlja činjenica da novi režim zaštite podataka uspostavljen GDPR-om, po čijem je uzoru pisan i domaći Zakon, važi za rukovaoce sa teritorije EU, kao i one koji posluju sa podacima stanovnika EU.

11 EDPB, 2018, Smernice 3/2018 o teritorijalnoj primeni GDPR-a, dostupno na: edpb.europa.eu

OSNOVNI POJMOVI

OSNOVNI POJMOVI

PODATAK O LIČNOSTI

Podatak o ličnosti je svaki podatak koji se odnosi na neko fizičko lice, uz pomoć kojeg je identitet tog fizičkog lica određen ili odrediv, posredno ili neposredno. Podatak o ličnosti je, dakle, svaka informacija koja nas, kao fizička lica, bliže određuje i koja se može dovesti u vezu sa konkretnom osobom. To mogu biti ime i prezime, adresa, JMBG, broj telefona, broj računa u banci i slično, ali i svaki drugi podatak koji nešto govori o nama.

Veliki broj naših ličnih podataka se nalazi na internetu, poput IP adrese, IMEI broja uređaja kojim pristupamo mreži, lozinki, naših naloga za elektronsku poštu i društvene mreže, istorije aktivnosti sa takvih naloga (šerovi, lajkovi, klikovi), istorije pretrage interneta i slično. Iako mnogi digitalno generisani podaci na prvi pogled ne deluju kao podaci o ličnosti, uz pomoć njih se neko lice može posredno identifikovati, u nekim slučajevima čak i samo na osnovu takvih podataka, ili u kombinaciji sa još nekim podacima. Upravo mogućnost identifikacije fizičkog lica i te podatke čini ličnim podacima. Zbog toga kategorizacija određenog podatka kao podatka o ličnosti ponekad zahteva da se u obzir uzme celokupan kontekst konkretnog slučaja, pa je i pravna definicija podatka o ličnosti dovoljno široka da bi se u primeni testirala u odnosu na različite situacije i neke još nepredvidljive događaje koji mogu uticati na osnovna prava i slobode.

Dileme

Da li je svojeručni potpis lični podatak?

Jeste, ukoliko se može dovesti u vezu sa određenim ili odredivim fizičkim licem.[12] Načelno govoreći, za kategorizaciju jednog podatka kao podatka o ličnosti bitno je utvrditi da li se uz pomoć njega neko lice može posredno ili neposredno identifikovati. Ukoliko je odgovor potvrdan, onda se radi o podatku o ličnosti.

Da li je podatak o mom zdravstvenom stanju koji me bliže ne određuje i koristi se u statističke svrhe - podatak o ličnosti?

Ukoliko se uz pomoć takvog podatka osoba ne može identifikovati, on ne predstavlja podatak o ličnosti. U statističke svrhe se koriste anonimizovani podaci, oni koji se više ne mogu dovesti u vezu sa konkretnim osobama. Na primer, informacija da je od gripa u 2019. godini na određenoj teritoriji oboleo određeni broj ljudi, predstavlja skup anonimizovanih podataka iz kojih se ne može saznati o kojim se ljudima radi.

Praksa

U prilog stavu da je IP adresa podatak o ličnosti govori i presuda Suda pravde Evropske unije C-582/14.[13] Po njoj, dinamička IP adresa se može smatrati podatkom o ličnosti ukoliko postoji razumno očekivanje da rukovalac ima mogućnost da odredi kojem licu ta adresa pripada, odnosno ima mogućnost da identifikuje vlasnika IP adrese.

12 Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije, 2017, Zaštita podataka o ličnosti: stavovi i mišljenja Poverenika - Publikacija br. 2, str. 13, dostupno na: poverenik.rs

13 Sud pravde EU, 2016, Slučaj C-582/14, Patrick Breyer v Bundesrepublik Deutschland, dostupno na: eur-lex.europa.eu

LICE NA KOJE SE PODACI ODNOSE

Fizičko lice čiji se podaci o ličnosti obrađuju i koje se uz pomoć takvih podataka može posredno ili neposredno identifikovati, jeste lice na koje se podaci odnose. Kao što i sam naziv govori, podaci o ličnosti su uvek samo oni podaci koji se odnose na fizičko lice, prema tome, podaci o ličnosti nisu podaci koji se odnose na entitete poput pravnih lica, životinja ili slično. Međutim, ukoliko podatak o nekom pravnom licu može da dovede do indentifikacije nekog fizičkog lica, takav podatak se smatra podatkom o ličnosti.

Iako ZZPL eksplicitno ne predviđa da lice na koje se podaci odnose mora biti živo lice, naše je shvatanje da ovaj uslov mora biti ispunjen, te da se Zakon ne primenjuje u odnosu na podatke o ličnosti lica koja su preminula. Tačka 27 Preambule propisuje da se GDPR ne primenjuje na preminula lica, s tim što se ostavlja mogućnost nacionalnim zakonodavstvima država članica EU da propišu pravila u vezi sa obradom podataka o ličnosti umrlih lica. Pored toga, određena zaštita podataka o ličnosti umrlog lica može da bude ostvarena kroz zakonodavstvo koje ne reguliše materiju zaštite podataka o ličnosti. Primera radi, Zakon o javnom informisanju i medijima propisuje mogućnost članova porodice umrlog lica da daju pristanak za objavljivanje informacija o privatnom životu umrlog, kao i pravo članova porodice umrlog lica da umesto umrlog lica podnesu tužbu za objavljivanje odgovora ili ispravke u slučaju objavljivanja nepotpunih ili netačnih informacija o umrlom licu, odnosno informacija koje su podobne da povrede pravo ili interes umrlog.[14]

POSEBNE VRSTE PODATAKA O LIČNOSTI

Podatke koji se odnose na rasno ili etničko poreklo, političko mišljenje, versko, filozofsko uverenje, članstvo u sindikatu, genetske i biometrijske podatke, kao i podatke o zdravstvenom stanju, seksualnom životu ili seksualnoj orijentaciji fizičkog lica, Zakon tretira kao posebne vrste podataka o ličnosti.

Radi se, dakle, o naročito osetljivim podacima čija obrada zahteva viši stepen pažnje u odnosu na ostale podatke o ličnosti. ZZPL propisuje da je obrada posebnih vrsta podataka o ličnosti zabranjena, osim u određenim izuzecima, koji su taksativno navedeni u Zakonu.

Intencija zakonodavca je da kao osnovno pravilo uspostavi zabranu obrade posebnih vrsta podataka o ličnosti, ali da istovremeno predvidi izuzetke u kojima je njihova obrada dozvoljena. Prilikom obrade posebnih vrsta podataka o ličnosti kao naročito osetljivih podataka, svakako treba primeniti načelo minimizacije podataka, odnosno obradu svesti na minimum koji je neophodan da bi se ostvarila svrha obrade. Izuzetak od poštovanja pravila obrade posebnih vrsta podataka o ličnosti koji se primenjuje na obradu koju nadležni organi vrše u posebne svrhe, ukazuje da postoje prilike kada je svrha obrade pretežnija od zaštite posebnih podataka o ličnosti, u ovom slučaju radi otkrivanja, sprečavanja i kažnjavanja za krivična dela, odnosno pretnji po javnu i nacionalnu bezbednost.

14 Zakon o javnom informisanju i medijima ("Sl. glasnik RS", br. 83/2014, 58/2015 i 12/2016 - autentično tumačenje)

Dileme

Da li je fotografija biometrijski podatak, samim tim i posebna vrsta podataka o ličnosti?

Po zakonskoj definiciji, biometrijski podatak je podatak o ličnosti dobijen posebnom tehničkom obradom u vezi sa fizičkim obeležjima, fiziološkim obeležjima ili obeležjima ponašanja fizičkog lica, koja omogućava ili potvrđuje jedinstvenu identifikaciju tog lica, kao što je slika njegovog lica ili njegovi daktiloskopski podaci. Prema tome, ZZPL svrstava fotografiju u biometrijske podatke samo ukoliko je ona izrađena posebnom tehničkom obradom u vezi sa fizičkim obeležjima konkretnog lica. Dalje se fotografija kao podatak o ličnosti u Zakonu ne pominje.

Međutim, GDPR u tački 51 Preambule precizira da obrada fotografije u načelu ne predstavlja obradu posebnih vrsta podataka o ličnosti, jer se fotografija smatra biometrijskim podatkom samo ukoliko je obrađena posebnim tehničkim sredstvima koja omogućavaju jedinstvenu identifikaciju ili identifikaciju lica. Ovo znači da neće baš svaka fotografija neke osobe biti biometrijski podatak. Međutim, fotografije na ličnoj karti, pasošu, fotografija snimljena kamerom koja koristi tehniku za prepoznavanje lica, smatraju se biometrijskim podacima.

Praksa

Mišljenje nezavisnog advokata Suda pravde Evropske unije je da, ukoliko je od onlajn servisa za pretraživanje zatraženo da iz pretrage ukloni rezultate koji se odnose na određeno lice i posebne vrste podataka o ličnosti, servis mora da u konkretnom slučaju odredi da li pravo na privatnost i zaštitu podataka o ličnosti ima prevagu nad pravom javnosti da pristupi tim podacima i pravom na slobodu izražavanja lica koje je takve podatke objavilo.[15]

OBRADA PODATAKA

Obrada podataka o ličnosti je svaka (automatizovana ili neautomatizovana) radnja koja se preduzima u vezi sa podacima o ličnosti, kao što su prikupljanje, beleženje, čuvanje, razvrstavanje, uvid, brisanje, uništavanje, pohranjivanje podataka i mnoge druge. Iako reč 'obrada' asocira na aktivno ponašanje, pod obradom podataka se mogu smatrati i pasivne radnje, poput čuvanja i skladištenja podataka.

Namera zakonodavca je, dakle, da ne zatvara spisak radnji koje se mogu smatrati radnjama obrade podataka o ličnosti, dok nabraja samo najčešće i tipične radnje obrade. Stoga je potrebno imati na umu da svako aktivno ili pasivno ponašanje u vezi sa podacima o ličnosti predstavlja njihovu obradu, pa je teško zamisliti situaciju da je neko došao u dodir sa podacima o ličnosti a da se to ne smatra obradom. Dakle, svaka upotreba ili svaki dodir sa podacima o ličnosti, bez obzira na to koliko je takva obrada trajala i kakve je vrste bila (aktivna ili pasivna), smatraće se obradom u smislu Zakona.

Dileme

Da li se samo čuvanje podataka na serveru, bez uvida u podatke, smatra obradom podataka o ličnosti?

Iako je čuvanje podataka pasivan odnos, čak i kada onaj ko ih čuva nema uvid u te podatke, Zakon to smatra obradom podataka o ličnosti.

Ukoliko moja kompanija primi dokumentaciju koja sadrži podatke o ličnosti i odmah ih prosledi drugom primaocu, bez kopiranja takve dokumentacije, da li se sam prijem i kratko zadržavanje dokumentacije smatra obradom?

Prijem i prosleđivanje podataka, čak i bez uvida ili kopiranja, takođe se smatraju obradom u smislu Zakona. U zavisnosti od same radnje obrade,

15 Sud pravde EU, 2019, Saopštenje povodom mišljenja nezavisnog advokata u slučaju C-136/17, G.C. and Others v CNIL, dostupno na: curia.europa.eu

rukovalac će odlučiti koji su to koraci koje je optimalno da preduzme u skladu sa ZZPL-om. Što je obrada manje invanzivna i kraće traje, to će i mere zaštite podataka koje se preduzimaju biti jednostavnije.

ZBIRKA PODATAKA

Zbirka podataka je svaki strukturisani skup podataka o ličnosti kojem se može pristupiti, ili se može pretraživati po nekom kriterijumu, bez obzira da li je zbirka centralizovana, decentralizovana ili razvrstana po funkcionalnim ili geografskim osnovama. Prema tome, da bi se radilo o zbirci podataka u smislu Zakona, potrebno je da su podaci sistematizovani i strukturno grupisani na jednom mestu, bilo da su to fascikle u ormaru, fleš memorija, disk, kompjuter ili nešto drugo.

Primera radi, pod zbirkom podataka možemo smatrati listu korisnika nekog servisa poređanih po abecednom redu, dok razbacane hartije oko kopir mašine ne predstavljaju strukturisani skup podataka. Međutim, ukoliko ove hartije poređamo po nekom kriterijumu, tako da se lični podaci mogu pretraživati po tom kriterijumu, takav skup postaje zbirka podataka o ličnosti.

Imajući u vidu da se ZZPL ne primenjuje na obradu podataka o ličnosti koju vrši fizičko lice za lične potrebe, odnosno potrebe svog domaćinstva, zbirkom podataka u smislu Zakona ne smatraju se lični adresari, foto albumi i slično, u slučaju da ih vlasnik koristi isključivo u lične, neposlovne svrhe. Međutim, ukoliko se fizičko lice registruje kao preduzetnik za pružanje određenih usluga, pa svoj lični adresar iskoristi za slanje poslovnih ponuda licima čije brojeve telefona ima, ono postaje rukovalac u smislu Zakona dok adresar postaje zbirka podataka, jer se više ne koristi isključivo u lične, privatne svrhe.

Stari Zakon o zaštiti podataka o ličnosti ustanovio je Centralni registar zbirki podataka koji vodi Poverenik, a koji se sastoji iz registra i kataloga zbirki podataka. Po starom propisu takođe su rukovaoci bili u obavezi da pre započinjanja obrade, odnosno uspostavljanja zbirke podataka dostave Povereniku obaveštenje o nameri uspostavljanja zbirke, zajedno sa propisanim podacima koji identifikuju tu zbirku podataka. Drugim rečima, rukovaoci su morali da registruju svaku zbirku koju vode u Centralnom registru Poverenika. Međutim, u praksi je malo rukovalaca poštovalo ove obaveze. Najčešće registrovane zbirke podataka su bile one koje su kompanije vodile o svojim zaposlenima.

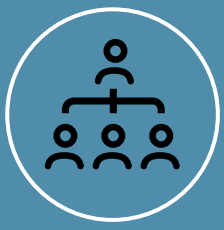
Novi Zakon predviđa da Centralni registar zbirki podataka prestaje da se vodi danom stupanja na snagu. Budući da je primena ZZPL odložena za avgust 2019. godine, u međuvremenu su na snazi stare odredbe.

Dileme

Da li je neophodno obavestiti Poverenika o nameri uspostavljanja zbirke podataka, ako će se ona uspostaviti tek nakon što novi Zakon stupi na snagu i ukine ovu obavezu?

Na osnovu člana 49 starog Zakona o zaštiti podataka o ličnosti, rukovalac je dužan da pre uspostavljanja zbirke dostavi Povereniku obaveštenje o nameri uspostavljanja takve zbirke. Međutim, novi Zakon članom 98 ukida obavezu vođenja Centralnog registra, pa samim tim i obavezu obaveštenja o nameri. U ovom slučaju treba imati u vidu mišljenje Poverenika u kom se ističe da obaveza prijavljivanja zbirki podataka postoji sve do početka primene novog Zakona, odnosno do 21. avgusta 2019. godine,[16] što se svakako odnosi na ostale obaveze iz starog Zakona, uključujući i obaveštenje o nameri.

16 Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije, 2018, Mišljenje u vezi sa vođenjem evidencija o obradi podataka o ličnosti, dostupno na: poverenik.rs



OSNOVNE ULOGE U OBRADI PODATAKA O LIČNOSTI

OSNOVNE ULOGE U OBRADI PODATAKA O LIČNOSTI

Strožije nego do sada, novi pravni režim zaštite podataka definiše odgovornost lica koja u različitim ulogama dolaze u dodir sa podacima o ličnosti. To mogu biti rukovaoci, zajednički rukovaoci, obrađivači, primaoci i treća strana. Glavni akteri u obradi podataka o ličnosti su svakako rukovalac i obrađivač, čija se prava i obaveze razlikuju - rukovalac određuje način i svrhu obrade podataka, pa je logično da ima širi spektar zakonskih obaveza u odnosu na obrađivača. Međutim, i obrađivač mora ispuniti niz propisanih obaveza.

Svako ko obrađuje podatke o ličnosti, mora najpre da utvrdi da li se u odnosu na konkretnu obradu javlja u ulozi rukovaoca, zajedničkog rukovaoca ili obrađivača. U praksi se često dešava da se isti entitet u odnosu na jednu grupu podataka javlja kao rukovalac, a u odnosu na drugu kao obrađivač. Zbog toga je potrebno ispitati uloge u odnosu na svaku konkretnu obradu i kategoriju podataka o ličnosti koji se obrađuju.

Tokom utvrđivanja uloga, u obzir se uzimaju sve okolnosti konkretnog slučaja, ali se najpre utvrđuje ko određuje svrhu obrade podataka - odgovor na pitanje "zašto se podaci obrađuju?" - i način obrade podataka.

RUKOVALAC

Rukovalac je fizičko ili pravno lice, odnosno organ vlasti koji samostalno ili zajedno sa drugima određuje svrhu i način obrade podataka o ličnosti.

U praksi to znači da, u odnosu na podatke o ličnosti koje obrađuje, rukovalac ima sveobuhvatnu kontrolu - on najpre odlučuje da počne prikupljanje i obradu podataka, te utvrđuje pravni osnov za takvu obradu, odnosno zašto i kako se takvi podaci o ličnosti obrađuju.

Rukovalac takođe određuje:

- koji podaci o ličnosti se obrađuju,
- u koju svrhu se oni obrađuju,
- o kojim pojedincima se prikupljaju podaci,
- da li će se podaci dalje distribuirati i, ako da, kome,
- koliko dugo će se čuvati podaci.

ZAJEDNIČKI RUKOVAOCI

U nekim slučajevima moguće je da više od jednog entiteta vrši ulogu rukovaoca, odnosno više od jednog entiteta donosi odluke o svrsi i načinu na koji se ti podaci obrađuju - tada će se oni smatrati zajedničkim rukovaocima, pa će imati obavezu da na transparentan način odrede odgovornost svakog od njih za poštovanje prava i obaveza predviđenih Zakonom, a posebno u pogledu ostvarivanja prava lica na koje se podaci odnose.

Međusobnu odgovornost u vezi obrade podataka o ličnosti zajednički rukovaoci uređuju u skladu sa principima autonomije volje, zajedničkim sporazumom, koji mora da sadrži informaciju o licu za kontakt sa licem na koje se podaci odnose i uređuju odnos svakog od zajedničkih rukovalaca sa licem na koje se podaci odnose. Najbitniji element u odnosu zajedničkih ruko-

valaca jeste jasan i transparentan način raspodele njihove odgovornosti u vezi sa ostvarivanjem prava lica na koje se podaci odnose. U suprotnom se može desiti da lice na koje se podaci odnose želi da ostvari prava prema oba zajednička rukovaoca (na šta ima pravo, jer su oba zajednička rukovaoca odgovorna licu na koje se podaci odnose za ostvarivanje njegovih prava), umesto u odnosu na jednog zajedničkog rukovaoca koji je za to nadležan, u skladu sa internim sporazumom sa drugim zajedničkim rukovaocem.[17]

Primera radi, kompanija koja koristi usluge agencije za zapošljavanje biće u položaju zajedničkog rukovaoca sa agencijom, budući da i jedna i druga određuju svrhu i način obrade. U slučaju kompanije, ona kao faktički poslodavac omogućava da radnici vrše posao, dok agencija kao formalni poslodavac treba da zaključuje ugovore o radu i ispunjava svoje obaveze iz drugih relevantnih zakona. U odnosu zajedničkih rukovalaca mogu biti turistička agencija i hotelski lanac, recimo, koji odluče da uspostave zajedničku internet stranicu za onlajn rezervacije smeštaja. Oni se dogovaraju koje će podatke prikupljati i na koji način, za koje svrhe, kako će ih i koliko dugo čuvati, ko im može pristupiti i slično. Svako od zajedničkih rukovalaca mora izvršiti sve obaveze propisane Zakonom, odnosno svako od njih je u potpunosti odgovoran licu čiji se podaci obrađuju.

Praksa

Status zajedničkog rukovaoca ponekad nije moguće jasno razaznati u onlajn sferi. Međutim, u jednoj svojoj odluci, Sud pravde Evropske unije pojašnjava da, pored Fejsbuka, odgovornost mora da snosi i kompanija koja je kreirala, odnosno koja je administrator fejsbuk stranice, jer je samim činom kreiranja stranice dozvolila Fejsbuku da prikuplja i obrađuje lične podatke posetilaca te stranice, te se ima smatrati zajedničkim rukovaocem.[18]

Štaviše, prema mišljenju nezavisnog advokata Suda pravde Evropske unije, vlasnik vebsajta koji je embedovao fejsbukovo 'lajk' dugme na svoj sajt mora se smatrati zajedničkim rukovaocem sa Fejsbukom, jer samim tim što je embedovao 'lajk' dugme on omogućava prikupljanje podataka o ličnosti.[19]

OBRAĐIVAČ

Obrađivač je fizičko ili pravno lice, odnosno organ vlasti, koji obrađuje podatke o ličnosti u ime rukovaoca. To znači da obrađivač ne određuje svrhu i sredstva za obradu ličnih podataka i predstavlja odvojeno pravno lice od rukovaoca. Obično je to organizacija sa posebnim veštinama i znanjima koju rukovalac angažuje kako bi izvršila obradu podataka o ličnosti. Odnos obrađivača sa rukovaocem je takav da obrađivač u principu mora da postupa u skladu sa pisanim uputstvima rukovaoca, što znači da rukovalac ima kontrolu nad obradom, ali sledstveno i odgovornost ukoliko obrada nije zakonita.

Ukoliko neka kompanija koja traži novog radnika, ne želi da troši svoje resurse na proces selekcije kandidata, ona u tu svrhu može da unajmi kadrovsku agenciju. U ovom slučaju, agencija će obrađivati podatke o ličnosti mnogih kandidata za koje kompanija nikada neće saznati jer nisu prošli selekciju, ali će to agencija raditi u ime kompanije i u svrhu koju je odredila kompanija. Sve dok agencija postupa u skladu sa pisanim instrukcijama kompanije koja u krajnjoj liniji kontroliše i svrhu i način obrade podataka (tako što kompanija daje uputstva koje podatke da obrađu-

17 Rücker, D., Kugler, T. (eds.), 2018, New European General Data Protection Regulation: A Practicioner's Guide, C.H. Beck, Hart, Nomos

18 Sud pravde EU, 2018, Slučaj C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, dostupno na: curia.europa.eu

19 Sud pravde EU, 2018, Saopštenje povodom mišljenja nezavisnog advokata u slučaju C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, dostupno na: curia.europa.eu

je i kako), agencija će se smatrati obrađivačem, a kompanija rukovaocem podataka o ličnosti kandidata za zaposlenje. Međutim, ukoliko je kompanija agenciji dala samo uopšten nalog da joj agencija uputi potencijalnog kandidata, dok sama agencija određuje koje će podatke obrađivati u kojoj fazi selekcije, na koji način i kojim sve sredstvima - tada sama agencija ima status rukovaoca u odnosu na obradu podataka koju vrši, ili eventualno status zajedničkog rukovaoca sa kompanijom.

Iako radi u okvirima koje je definisao rukovalac, obrađivač može samostalno odlučivati o pojedinim segmentima procesa obrade, a u dogovoru sa rukovaocem. Obrađivač može odlučiti:

- koje metode koristiti za prikupljanje podataka o ličnosti,
- kako skladištiti podatke o ličnosti,
- o detaljima koji se tiču bezbednosti podataka o ličnosti,
- o sredstvima koja se koriste za prenos podataka o ličnosti,
- o sredstvima koja se koriste za brisanje ili odlaganje podataka.

PODELA ODGOVORNOSTI

Po ugledu na GDPR, novi Zakon uvodi čitav niz obaveza za obrađivača. Ranije se većina obaveza i odgovornosti u vezi sa zaštitom podataka o ličnosti odnosila na rukovaoca, dok je obrađivač ostajao u drugom planu. Sada to više nije slučaj.

ZAKONITOST OBRADE

ZZPL predviđa obavezu zakonite obrade podataka o ličnosti, odnosno obavezu da se obrada vrši na osnovu jednog od Zakonom propisanih pravnih osnova. Utvrđivanje relevantnog pravnog osnova je prevashodno obaveza rukovaoca, budući da on određuje svrhu obrade.

NAČELA OBRADE

I rukovalac i obrađivač su u obavezi da obrađuju podatke o ličnosti u skladu sa načelima obrade, ali će samo rukovalac imati obavezu da demonstrira usklađenost sa načelima obrade, što ne znači da obrađivač ne mora da se pridržava ovih načela.

ODGOVARAJUĆE TEHNIČKE I ORGANIZACIONE MERE

Nezavisno od toga da li se entitet nalazi u ulozi obrađivača ili rukovaoca, moraće da implementira određene tehničke i organizacione mere u svoje poslovanje u cilju potpunog usklađivanja sa odredbama Zakona. Najvažnije je utvrditi koje kategorije podataka o ličnosti se obrađuju i koja je svrha obrade. Što su osetljiviji podaci koji se obrađuju, to iziskuje sofisticiranije tehničke i organizacione mere.

LICE ZA ZAŠTITU PODATAKA O LIČNOSTI

Kada je ispunjen jedan od zakonskih uslova, i rukovalac i obrađivač imaju obavezu da odrede lice za zaštitu podataka o ličnosti.

EVIDENCIJA RADNJI OBRADE

Zakon predviđa obavezu i za rukovaoca i za obrađivača da vode evidenciju obrade i da je dostave na zahtev nadležnog organa, međutim, evidencija koju vodi rukovalac sadrži više podataka od evidencije koju vodi obrađivač. S druge strane, obrađivač mora evidentirati sve rukovaoce u čije ime obrađuje podatke.

OBAVEŠTENJE O POVREDI PODATKA O LIČNOSTI

U slučaju povrede podataka o ličnosti, rukovalac je dužan da bez odlaganja, a najkasnije u roku od 72 sata o tome obavesti Poverenika, dok je obrađivač dužan da obavesti rukovaoca čim sazna za povredu. Rukovalac je takođe obavezan da o povredi obavesti i lice na koje se podaci odnose, dok obrađivač nema ovu obavezu.

PROCENE UTICAJA NA ZAŠTITU PODATAKA O LIČNOSTI

Rukovalac će biti odgovoran za izradu procene uticaja obrade na zaštitu podataka o ličnosti u slučaju da za to ima zakonsku obavezu, dok obrađivač ne snosi takvu odgovornost.

PRENOS PODATAKA VAN SRBIJE

U slučaju iznošenja podataka o ličnosti iz Srbije, i rukovalac i obrađivač imaju obavezu da ispune brojne uslove koje ZZPL pred njih postavlja. Takođe, i rukovalac i obrađivač sarađuju sa Poverenikom na ispunjavanju svojih zakonskih obaveza, te su dužni da se povinuju zahtevima Poverenika u ovom smislu.

PRAVA LICA NA KOJE SE PODACI ODNOSE

Po Zakonu, lica na koje se podaci odnose imaju pravo na pristup, izmenu, brisanje ili prenos svojih podataka, dok rukovalac nosi primarnu obavezu da omogući ispunjenje ovih prava i da u vezi s njima komunicira sa licima na koje se podaci odnose. Obrađivač u tom smislu ima obavezu samo da asistira rukovaocu, tako što će primeniti odgovarajuće tehničke i organizacione mere.

ODNOS RUKOVAOCA I OBRAĐIVAČA

Za obrađivača koji u njegovo ime vrši obradu, rukovalac može da odredi samo ono lice ili organ vlasti koji u potpunosti garantuje primenu tehničkih, organizacionih i kadrovskih mera na način koji obezbeđuje da obrada bude zakonita. Namera zakonodavca je da osigura isti nivo bezbednosti podataka koji se obrađuju u situaciji kada, pored rukovaoca, podatke obrađuje jedan ili više obrađivača. Imajući u vidu da rukovalac određuje da li će i koje obrađivače imati, lice na koje se odnose podaci ne treba da se nađe u nepovoljnijem položaju u slučaju da su njegovi podaci povereni obrađivaču koji ne ispunjava odgovarajuće tehničke i organizacione mere.

ZZPL propisuje obavezu zaključenja ugovora o obradi, odnosno drugog pravno obavezujućeg akta u pisanom obliku između rukovaoca i obrađivača, a u cilju regulisanja predmeta i trajanja obrade, prirode i svrhe obrade, vrste podataka o ličnosti i kategorije lica o kojima se podaci obrađuju, kao i prava i obaveze rukovaoca. Obavezna sadržina ugovora o obradi je propisana Zakonom, te ne ostavlja puno prostora za autonomiju volje rukovaoca i obrađivača. Uz druge odredbe, ugovorom o obradi je potrebno da se propiše da je obrađivač dužan da:

- obrađuje podatke samo na osnovu pisanih uputstava rukovaoca;
- preduzme odgovarajuće tehničke i organizacione mere potrebne za obezbeđivanje integriteta podataka o ličnosti koji se obrađuju;
- posle okončanja ugovorenih radnji obrade, a na osnovu odluke rukovaoca, izbriše ili vrati rukovaocu sve podatke o ličnosti i izbriše sve kopije ovih podataka, osim ako je zakonom propisana obaveza čuvanja podataka;
- učini dostupnim rukovaocu sve informacije potrebne za predočavanje ispunjenosti obaveza obrađivača.

PRIMALAC

Primalac je fizičko ili pravno lice, odnosno organ vlasti, kome su podaci o ličnosti otkriveni, bez obzira da li se radi o trećoj strani ili ne, osim ako se radi o organima vlasti koji u skladu sa zakonom primaju podatke o ličnosti u okviru istraživanja određenog slučaja i obrađuju ove podatke u skladu sa pravilima o zaštiti podataka o ličnosti koja se odnose na svrhu obrade. To je, dakle, onaj kome su podaci učinjeni dostupnim, a taj neko može biti i drugi rukovalac i obrađivač i tzv. treća strana.

Lice na koje se podaci odnose ima pravo da od rukovaoca zahteva informaciju o primaocu ili primaocima kojima su njegovi podaci o ličnosti otkriveni ili će im biti otkriveni.

TREĆA STRANA

Treća strana je fizičko ili pravno lice, odnosno organ vlasti, koji nije lice na koje se podaci odnose, rukovalac ili obrađivač, kao ni lice koje je ovlašćeno da obrađuje podatke o ličnosti pod neposrednim nadzorom rukovaoca ili obrađivača.

NAČELA OBRADE PODATAKA

NAČELA OBRADE PODATAKA

ZNAČAJ PRINCIPA I DOMEN PRIMENE

Načela obrade podataka uspostavljena novom evropskom regulativom, a koja su ugrađena i u novi domaći Zakon, imaju višestruki značaj. Najpre, ovim načelima se praktično usmerava tumačenje konkretnih odredbi koje mogu biti nejasne. Dakle, ukoliko je rukovalac ili obrađivač u dilemi na koji način da primeni neku konkretnu odredbu, uvek treba da se osloni na ono tumačenje koje je u duhu ovih načela.

Međutim, postavljena načela imaju još jednu značajnu dimenziju, budući da za samo nepoštovanje bilo kog od načela rukovaoci i obrađivači mogu odgovarati prekršajno. Dakle, bez obzira na to što formalno poštuju ostale obaveze iz Zakona, moguće je da se utvrdi odgovornost ukoliko način na koji su te obaveze sprovedene nije u skladu sa nekim od načela. Kršenje načela obrade ličnih podataka ujedno povlači i najteže kazne - prema domaćem Zakonu, kazna za pojedinačni prekršaj kojim se krši neko od načela iznosi 2.000.000 dinara, dok u sticaju kazna može biti i duplo veća. Prema GDPR, za kršenje načela može se izreći kazna u visini od 20 miliona evra ili 4% ukupnog godišnjeg prihoda, šta god je veće.

ZAKONITOST, POŠTENJE I TRANSPARENTNOST

Podaci o ličnosti moraju se obrađivati zakonito, pošteno i transparentno u odnosu na lice na koje se podaci odnose ("zakonitost, poštenje i transparentnost"). Zakonita obrada je obrada koja se vrši u skladu sa ovim zakonom, odnosno drugim zakonom kojim se uređuje obrada.[20]

Iz formulacije ovog načela jasno je da se ono sastoji iz više međusobno povezanih, ali zasebnih delova. Naime, ovo načelo sadrži pravila da lični podaci moraju da budu obrađeni zakonito, pravično i transparentno u odnosu na lice na koje se odnose. Ovo konkretno znači sledeće:

- podaci mogu da budu obrađivani samo ukoliko postoji odgovarajući pravni osnov za konkretnu obradu i uz poštovanje svih propisa koji se na tu obradu primenjuju;
- rukovaoci moraju uvek imati u vidu i interese lica čije podatke obrađuju i ponašati se pošteno u konkretnim okolnostima, u zavisnosti od toga čije podatke prikupljaju;
- od momenta kada započne prikupljanje, lice čiji se podaci obrađuju u svakom trenutku ima pravo da zna kako se sa njima postupa - što uključuje pravo da bude upoznato sa činjenicom da se podaci obrađuju, u kojoj meri, za koje svrhe, ko je rukovalac i ko su obrađivači, i slično - a te informacije treba da budu saopštene na jasan i razumljiv način.

Drugim rečima, ovo načelo zahteva od rukovalaca da ne zloupotrebljavaju svoju nesrazmerno jaču poziciju naspram vlasnika podataka, u odnosu na koje postoji asimetrija informacija, već da prema njima imaju pošten i iskren stav. Taj stav podrazumeva da se rukovaoci obrade podataka ponašaju na način koji bi njihovi klijenti, korisnici ili partneri čije podatke obrađuju smatrali prihvatljivim i očekivanim.

20 Član 5, stav 1, tačka 1 ZZPL

Smernice

Prema stavovima Radne grupe 29, transparentnost je načelo koje je relevantno u svim aspektima primene pravila o zaštiti ličnih podataka, i na snazi je u tri centralne oblasti: (1) informisanje lica čiji se podaci obrađuju u vezi sa poštenom obradom; (2) način na koji rukovaoci komuniciraju sa nosiocima podataka povodom njihovih prava; i (3) načini na koje rukovaoci mogu nosiocima podataka pomoći da svoja prava efikasno iskoriste. Takođe, načelo transparentnosti je jednako značajno kroz sve cikluse obrade podataka: pre početka obrade tj. u fazi prikupljanja podataka, tokom same obrade - što uključuje i komunikaciju po osnovu prava na informisanost i ostalih prava, i ukoliko se tokom obrade dese nepredviđene okolnosti koje ugrožavaju bezbednost i poverljivost podataka.[21]

Kao primer, možemo zamisliti situaciju u kojoj rukovalac na svom vebsajtu objavi politike privatnosti gde klijentima čije podatke prikuplja preko svog onlajn servisa, obelodani koje sve podatke o njima poseduje, po kom osnovu ih koristi i koliko dugo ih čuva, pa čak i da podatke deli sa nekim svojim partnerima (često se u ovim slučajevima samo navede da su partneri "pouzdani"). Međutim, ovaj princip zaštite biće prekršen ako u tekstu politika privatnosti ne navede činjenicu da zapravo nema nikakvu kontrolu nad tim za šta tačno partneri koriste podatke, koje podatke preuzimaju, koliko ih dugo čuvaju i da li ih dalje dele sa neodređenom grupom lica - tako da se na kraju ispostavlja da je obrada koja se odvija na onlajn platformi samog rukovaoca beznačajno mala u poređenju sa obradom kod raznih partnera o kojoj lica na koja se podaci odnose nisu obaveštena.

SVRHA OBRADE

Podaci o ličnosti moraju se prikupljati u svrhe koje su konkretno određene, izričite, opravdane i zakonite i dalje se ne mogu obrađivati na način koji nije u skladu sa tim svrhama ("ograničenje u odnosu na svrhu obrade").[22]

Princip ograničenosti svrhe obrade u suštini se sastoji od dva osnovna zahteva: (1) da se pre započinjanja obrade precizno definiše i izričito objasni zbog čega se podaci prikupljaju, kao i da se (2) podaci prikupljeni za inicijalnu svrhu ne mogu dalje obrađivati za bilo koju drugu, nekompatibilnu svrhu.

Smernice

Da li je svrha dovoljno jasno određena može biti diskutabilno pitanje, međutim, prema mišljenju Radne grupe 29 to svakako znači da svrha ne može biti definisana uopštenim terminima kao što su "poboljšanje iskustva korisnika" ili "marketinške svrhe". Izričitost svrhe podrazumeva zahtev da je svrha izražena u jasnim i nedvosmislenim terminima, koji omogućavaju razumevanje o kakvoj tačno se svrsi radi.[23]

Što se tiče drugog zahteva, takođe će ponekad biti jasno da su svrhe nekompatibilne. Na primer, kontakti prikupljeni za potrebe ispunjenja ugovora, ne mogu se koristiti za marketing. Za ne tako jasne situacije, Radna grupa 29 je dala određene smernice rukovaocima, sugerišući okolnosti o kojima se mora voditi računa prilikom sprovođenja "testa kompatibilnosti". Te okolnosti su: (1) da li postoje i kakve su veze između inicijalne svrhe i svrhe dalje obrade, (2) u kakvom su kontekstu podaci bili inicijalno prikupljeni i kakva je u tom trenutku bila veza rukovaoca i lica čiji se poda-

21 Radna grupa 29, 2018, Smernice za transparentnost prema Uredbi 2016/679, dostupno na: ec.europa.eu
22 Član 5, stav 1, tačka 2 ZZPL
23 Radna grupa 29, 2013, Mišljenje 03/2013 o ograničenosti svrhe, dostupno na: ec.europa.eu

> ci obrađuju, odnosno kakva su razumna očekivanja tih lica u datoj situaciji, (3) kakva je priroda ličnih podataka, a pogotovo da li se radi o posebno osetljivim podacima, (4) koje su moguće posledice dalje obrade (pri čemu se mogu uzeti u obzir i pozitivne i negativne posledice) i (5) kakve mere sigurnosti, predostrožnosti i opreza su preduzete (npr. enkripcija, pseudonimizacija).[24]

Najzad, prema Zakonu se, pod određenim uslovima, izuzetno može dozvoliti dalja obrada u svrhe arhiviranja u javnom interesu, u svrhe naučnog i istorijskog istraživanja i u statističke svrhe.

Uzmimo za primer rukovaoca koji vodi sportski centar, gde drži i veliku zbirku podataka o svojim korisnicima, njihovim navikama i interesovanjima, prikupljenim kako bi oni u sportskom centru mogli da treniraju i kako bi mogao da se izvrši njihov korisnički ugovor. U međuvremenu, rukovalac ostvari poslovnu saradnju sa novim sportskim brendom na tržištu pa, u cilju promocije novog brenda, sportski centar svom partneru stavi na raspolaganje određene lične podatke svojih korisnika, kako bi im bile dostavljene ponude za sportsku opremu u skladu sa njihovim interesovanjima. Iako je ideja rukovaoca da bi korisnici bili srećni da dobiju ovakve ponude, jer one uključuju i određene popuste, u pitanju je korišćenje podataka u potpuno druge svrhe od one za koju su inicijalno bili prikupljeni.

MINIMIZACIJA

Podaci o ličnosti moraju biti primereni, bitni i ograničeni na ono što je neophodno u odnosu na svrhu obrade ("minimizacija podataka").[25]

Prema ovom načelu, lični podaci koji se prikupljaju moraju biti ograničeni samo na ono što je neophodno za konkretnu svrhu obrade, odnosno moraju biti primereni i relevantni baš za tu svrhu. Na primer, ukoliko rukovalac klijentima želi da šalje obaveštenja elektronskom poštom, za to su mu potrebne samo njihove mejl adrese, dok je obrada svih ostalih podataka za ovu svrhu nepotrebna. Drugim rečima, svaki podatak bez kog bi se svrha obrade mogla ispuniti, predstavlja višak i podrazumeva kršenje ovog načela.

Načelo minimizacije podataka je u uskoj vezi sa GDPR institutima ugrađene i podrazumevane privatnosti (*privacy by design & by default*), koji su u ZZPL implementirani članom 42 i nazivaju se "mere zaštite". Naime, pravila ovog člana nalažu rukovaocima i obrađivačima da se još u fazi razvoja i oblikovanja načina obrade i planiranja toka podataka, sistemi koji obrađuju podatke podese tako da se u njima ne nalaze podaci čija obrada nije neophodna.

Zamislimo onlajn knjižaru koja sa svojim korisnicima zaključuje ugovor o prodaji knjiga, za šta su joj zapravo potrebni podaci za plaćanje i podaci za isporuku kupljene knjige. Princip minimizacije biće prekršen ukoliko se u onlajn formularu za kupovinu kao obavezna polja navode i podaci koji nisu neophodni za izvršenje ovog ugovora, kao što su datum rođenja, broj telefona, pol i slično, pri čemu onlajn kupovina ne može da se izvrši dok se ovi podaci ne unesu.

Ilustrativan primer može biti i kompanija čija delatnost podrazumeva i neke opasne poslove, ili poslove sa povećanim rizikom. Dok bi obrada podataka o krvnoj grupi zaposlenih koji rade ovakve poslove mogla biti opravdana u slučaju incidenta, nije neophodno tražiti takav podatak od onih radnika koji obavljaju administrativne poslove u svojim kancelarijama.

TAČNOST

Podaci o ličnosti moraju biti tačni i, ako je to neophodno, ažurirani. Uzimajući u obzir svrhu obrade, moraju se preduzeti

24 Ibid.
25 Član 5, stav 1, tačka 3 ZZPL

sve razumne mere kojima se obezbeđuje da se netačni podaci o ličnosti bez odlaganja izbrišu ili isprave ("tačnost").[26]

Ovo načelo praktično zahteva od rukovalaca pedantnost u obradi ličnih podataka. Podaci koji se koriste u obradi moraju biti tačni i, kada za tim postoji potreba, usklađeni sa eventualnim promenama. Imajući u vidu svrhe za koje se podaci obrađuju, rukovalac mora da obezbedi da netačni podaci budu bez odlaganja obrisani ili ispravljeni. Podaci se mogu smatrati netačnim i u situacijama kada su nepotpuni ili kada su izvučeni iz konteksta.[27]

U određenim situacijama, primena ovog načela može imati značajne i dalekosežne posledice po nosioce podataka. To će uvek biti slučaj kada se na osnovu ličnih podataka donosi odluka o nekim pravima ili mogućnostima, na primer, prilikom odobravanja kredita. Svakodnevni primer takođe može biti prodavnica koja obrađuje adresu korisnika kom na nedeljnom nivou šalje kupljene proizvode i koja efikasno mora da izmeni ovaj podatak kada korisnik promeni boravište. Primena ovog načela je u direktnoj vezi sa pravom na ispravku i dopunu podataka.

U zavisnosti od prirode posla i zakonskih obaveza, ponekad može biti jako važno da rukovalac čuva i celu istoriju izmena određenog podatka, odnosno da čuva i prethodne netačne podatke i informaciju o tome kada su i zašto izmenjeni.

Uzmimo za primer bolničkog pacijenta koji je tokom lečenja dobio pogrešnu dijagnozu, na osnovu koje je nedeljama primao određenu terapiju. Nakon dodatnih analiza, dijagnoza je promenjena i pacijent je dobio novu terapiju. Međutim, inicijalna pogrešna terapija je na njegov organizam ostavila posledice koje se takođe moraju pratiti. Da bi lečenje bilo uspešno, jednako je važno da se čuvaju i pogrešni i tačni podaci.

Ili, na primer, imamo korisnika koji se pretplatio na nedeljno izdanje nekog časopisa. Međutim, podatak o njegovoj adresi je pogrešan, te mu svake nedelje časopis stiže kod komšije iz susednog ulaza koji sticajem okolnosti ima isto prezime. Od početka pretplate prošlo je dva meseca tokom kojih je korisnik uredno plaćao svoju pretplatu, ali časopis nije dobijao zbog pogrešnog podatka.

OGRANIČENJE ČUVANJA

Podaci o ličnosti moraju se čuvati u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade ("ograničenje čuvanja").[28]

Lični podaci smeju da se čuvaju u obliku koji omogućava identifikaciju fizičkih lica samo onoliko dugo koliko je neophodno za ispunjenje svrhe za koju se podaci obrađuju. Dakle, kada odredi konkretnu svrhu obrade i vrste podataka koje je potrebno da prikupi da bi ta svrha mogla da bude ostvarena, rukovalac bi u tom trenutku trebalo da odredi i koliko dugo je neophodno da se predmetni podaci nalaze u njegovom posedu. Načelo ograničenja čuvanja tako u sebi sadrži dve komponente: (1) obavezu da se unapred odredi period čuvanja podataka, u zavisnosti od svrhe obrade, pri čemu taj period mora biti neophodan za ispunjenje svrhe, tj. mora postojati racionalno i ubedljivo obrazloženje zašto svrha ne može biti ostvarena u kraćem roku, i (2) brisanje ili anonimizaciju podataka (tako da više nije moguća identifikacija) posle isteka tog perioda. U teoriji se ovo načelo još označava i kao "vremenski aspekt načela minimizacije".[29]

Rok čuvanja svakako je u direktnoj vezi i sa pravnim osnovom za obradu podataka. Ukoliko se lični podaci obrađuju u kontekstu ispunjavanja ugovora, kada se ugovor izvrši obrada po tom pravnom osnovu prestaje. Međutim, u tom slučaju će rukovalac po pravilu imati interes da određe-

26 Član 5, stav 1, tačka 4 ZZPL
27 Rücker, D., Kugler, T. (eds.), 2018, New European General Data Protection Regulation: A Practicioner's Guide, C.H. Beck, Hart, Nomos, str. 68
28 Član 5, stav 1, tačka 5 ZZPL
29 Ibid.

ne lične podatke nastavi da čuva po osnovu legitimnog interesa, recimo, sve dok ne isteknu rokovi zastarelosti, kako bi mogao da u tom periodu ostvari eventualne pravne zahteve protiv tog lica, bivšeg saugovarača.

Kao i kod ograničenosti svrhe, izuzetak su svrhe arhiviranja u javnom interesu, svrhe naučnog ili istorijskog istraživanja i statističke svrhe, pod određenim uslovima.

Recimo, rukovalac koji ima postavljen video nadzor radi obezbeđivanja poslovnih prostorija od krađe ili neovlašćenog ulaska, treba da odredi koliko dugo je potrebno da se ti snimci čuvaju kako bi se ostvarila ova svrha, te da snimke posle tog vremena obriše. Kada neka prodavnica postavi sigurnosne kamere između rafova u cilju sprečavanja krađa, a svakog meseca radi popis čiji je cilj da se utvrdi da li postoji manjak, u takvim okolnostima nije opravdano da se snimci sigurnosnih kamera čuvaju u dužem vremenskom periodu.

Dileme

U Srbiji je na snazi Zakon o evidencijama u oblasti rada koji propisuje da se svi lični podaci iz ovih evidencija čuvaju trajno.[30] Iako se može postaviti pitanje da li su takve odredbe same po sebi u skladu sa načelima obrade ličnih podataka, dok god je Zakon na snazi poslodavci moraju da obezbede čuvanje velikog broja ličnih podataka po ovom osnovu bez vremenskog ograničenja. Zbog toga je jako važno da se u cilju ove obrade poštuju sva druga načela obrade, a pre svega primena odgovarajućih organizacionih i tehničkih mera.

INTEGRITET I POVERLJIVOST

Podaci o ličnosti moraju se obrađivati na način koji obezbeđuje odgovarajuću zaštitu podataka o ličnosti, uključujući zaštitu od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera ("integritet i poverljivost").[31]

Zbog značaja zaštite ličnih podataka građana od raznih vidova narušavanja njihove bezbednosti, integritet i poverljivost se takođe nalaze među šest osnovnih principa. Po uzoru na GDPR, Zakon među najčešće situacije narušavanja bezbednosti navodi neovlašćenu ili nezakonitu obradu, slučajni gubitak, uništenje ili oštećenje podataka. Međutim, ovo načelo se odnosi i na sve druge situacije u kojima lični podaci na bilo koji način mogu biti kompromitovani.

Obaveza rukovaoca i obrađivača je da zaštite bezbednost podataka primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera. Kao ni GDPR, ni domaći Zakon ne propisuje koje se to mere moraju primeniti,[32] jer one uvek zavise od konkretne situacije i od čitavog niza faktora, kao što su: koja vrsta i količina podataka je u pitanju, koja je svrha obrade, koliko dugo i na koji način se podaci čuvaju, u kojim sistemima, i slično. Opasnosti mogu vrebati od spoljnih napada, ali i iz same organizacije (na primer, ako zaposleni koji obrađuju lične podatke nisu dovoljno obučeni).

Dakle, odluka o odgovarajućim tehničkim i organizacionom merama je još jedna u nizu odluka koju bi rukovalac trebalo da donese pre početka obrade. Međutim, zbog brzog razvoja tehnologije i promena u internoj organizaciji, potrebno je stalno proveravati adekvatnost postojećih mera i uvoditi primerena unapređenja i adaptacije, kako bi se očuvao optimal-

30 Zakon o evidencijama u oblasti rada ("Sl. list SRJ", br. 46/96 i "Sl. glasnik RS", br. 101/2005 - dr. zakon i 36/2009 - dr. zakon)
31 Član 5, stav 1, tačka 1 ZZPL
32 ZZPL navodi primere ovih mera u članu 50

ni nivo sigurnosti i bezbednosti obrade. Konkretizacija ovog načela sadržana je u članovima ZZPL koji regulišu bezbednost podataka.

Za primer možemo uzeti rukovaoca koji u svom poslovanju koristi softversku aplikaciju u kojoj se obrađuju i podaci klijenata i podaci samih zaposlenih. Sa stanovišta odgovarajućih organizacionih i tehničkih mera, nije prihvatljivo da se sa svih korisničkih naloga može pristupati svim podacima, već rukovalac treba da uvede sistem rola i autorizacija koje će da obezbede da samo kadrovska služba može da ima uvid u podatke zaposlenih, dok zaposleni kojima je to potrebno za obavljanje radnih zadataka mogu da imaju uvid u odgovarajuće podatke klijenata.

Ili, na primer, fizikalna ambulanta u ulozi rukovaoca koja o svojim klijentima čuva informacije o programu vežbi koje fizioterapeut treba da sprovede sa svakim klijentom, što uključuje i osetljive zdravstvene podatke. Recimo da se iz praktičnih razloga predmetne informacije, pored elektronske forme, čuvaju i na papiru koji se koristi svaki put kada klijent dođe na terapiju. Odgovarajuće mere zaštite podrazumevaju da se papirna forma čuva pod ključem i da joj pristupaju samo ovlašćena lica, kao i to da se papirna forma uništava čim ispuni svoju svrhu.

ODGOVORNOST RUKOVAOCA

Rukovalac je odgovoran za primenu odredaba stava 1 ovog člana i mora biti u mogućnosti da predoči njihovu primenu ("odgovornost za postupanje").[33]

Princip odgovornosti praktično znači da je teret na rukovaocu da obezbedi primenu svih šest načela u svojoj organizaciji, odnosno da mora biti u mogućnosti da dokaže svoju usklađenost. Ovo je značajna promena za rukovaoce u Srbiji, pošto uvodi drastično drugačiju logiku od one na kojoj se temelji stari Zakon o zaštiti podataka o ličnosti. Naime, prema starom Zakonu, rukovalac je bio obavezan da zbirke podataka prijavi Povereniku kao nadležnom organu, pa je taj mehanizam trebalo da obezbedi rukovaocima svojevrsnu potvrdu da su njihove zbirke zakonite, odnosno da su njihove prakse obrade ličnih podataka u skladu sa zakonskim pravilima. Pošto se prema novom Zakonu zbirke ne prijavljuju, rukovaoci sada sami moraju obezbediti primenu svih potrebnih pravila u svojim sistemima obrade ličnih podataka, dok se eventualna provera njihove usklađenosti sa propisima vrši samo ukoliko je rukovalac u situaciji da mora svoju usklađenost da dokazuje u nekom postupku (na primer, u postupku nadzora koji pokreće Poverenik).

Praktičan aspekt ovog načela se ogleda u tome da bi rukovaoci trebalo da dokumentuju sve svoje odluke u vezi sa primenom ZZPL načela. Takva dokumenta mogu da uključuju odgovarajuće politike privatnosti ili politike zaštite ličnih podataka, koje su se u praksi pokazale vrlo korisnim iako Zakon ne nameće obavezu njihovog donošenja. U zavisnosti od svrhe i sadržine takvih dokumenata, oni mogu mogu biti javno dostupni (na primer, politike privatnosti objavljene na vebsajtu), ali mogu biti izrađeni i u formi internih akata, sa ciljem da se regulišu interni postupci i procedure (na primer, pravilnik o postupanju sa podacima o ličnosti). Takođe, rukovaoci mogu imati koristi od primene mehanizama dobrovoljne sertifikacije.[34]

Praksa

Prema odluci Suda pravde EU, načelo transparentnosti nalaže rukovaocu koji ima svojstvo javnog organa, da je neophodno da obavesti nosioce podataka ukoliko njihove lične podatke prenosi drugom javnom organu, i to pre nego što se prenos izvrši.[35]

33 Član 5, stav 2 ZZPL
34 Član 61 ZZPL
35 Sud pravde EU, 2015, Slučaj C-201/14, Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others, paras. 28-46, dostupno na: eur-lex.europa.eu

Poverenik je 2015. godine izdao saopštenje koje se ticalo zadržavanja ličnih karata građana u različitim institucijama, u cilju njihove identifikacije i sigurnosnih provera prilikom ulaska u poslovne prostorije. Naime, u praksi je bilo uobičajeno da se od lica pre ulaska u određenu zgradu, pogotovo u državne institucije, zahteva da preda ličnu kartu koja je bila zadržavana i/ili kopirana sve dok lice ne napusti zgradu. Poverenik je ovu praksu ocenio kao neopravdanu i nepotrebnu, jer se isti cilj mogao postići i na manje intruzivan način. U saopštenju Poverenika se navodi: "Ako u nekim situacijama može biti opravdano da službeno lice u javnom ili privatnom sektoru u svrhu preventivne ili eventualno aposteriorne zaštite imovine i lica, vrši identifikaciju lica uvidom u ličnu kartu i eventualno prepiše određene podatke lica (ime, prezime, broj i vrstu lične isprave, vreme i razlog ulaska i izlaska...), to izvesno ne znači da je opravdano da zadržava ili kopira ličnu kartu, jer je to očito nepotrebno za ostvarivanje svrhe obrade."[36]

U slučaju koji se nije direktno ticao primene regulative u vezi sa zaštitom ličnih podataka, ali se jeste ticao načela minimizacije i načela roka čuvanja, CJEU je doneo čuvenu odluku kojom je poništena evropska Direktiva o zadržavanju podataka.[37] Naime, Direktiva o zadržavanju podataka je imala za cilj da harmonizuje pravila država članica o zadržavanju ličnih podataka koji se prikupljaju u vezi sa pružanjem javno dostupnih elektronskih komunikacijskih usluga. CJEU je smatrao neprihvatljivim odredbe ove Direktive o obradi svih vrsta podataka i to svih građana, putem svih sredstava elektronskih komunikacija, bez ikakve selekcije, ograničenja ili izuzetaka. Takođe, nije bilo prihvatljivo pravilo Direktive da se svi prikupljeni podaci čuvaju u periodu od šest do 24 meseca, i to zbog toga što ovi periodi nisu dovedeni u vezu sa tačnom vrstom podataka koji su potrebni radi ostvarenja proklamovanih svrha, niti su ustanovljeni kriterijumi za određivanje jasnog perioda čuvanja u okviru datog raspona od 18 meseci, a koji bi bio zaista neophodan za ostvarivanje tih svrha.

Pregled relevantne sudske prakse evropskih sudova na temu povrede glavnih načela obrade ličnih podataka može se naći u Priručniku o evropskom pravu zaštite ličnih podataka koji je izdala Agencija Evropske unije za osnovna prava (FRA).[38]

Dileme

U praksi se često postavlja pitanje da li pristanak lica čiji se podaci obrađuju, koji je u svemu dat validno, može da pokrije, odnosno "ozakoni" kršenje nekog od načela obrade. Jasan odgovor da ne može dala je Radna grupa 29, koja je o ovom pitanju savetovala sledeće: "Pribavljanje pristanka takođe ne negira niti na bilo koji način umanjuje obaveze rukovaoca da poštuje načela obrade koja su sadržana u GDPR, pogotovo u članu 5 u vezi sa poštenjem, neophodnošću i proporcionalnošću, kao i kvalitetom podataka. I ukoliko je obrada ličnih podataka zasnovana na pristanku lica na koje se podaci odnose, ta okolnost ne bi mogla obezbediti zakonitost prakse prikupljanja podataka koji nisu neophodni u vezi sa specifičnom svrhom obrade i koja bi bila fundamentalno nepoštena".[39]

36 Saopštenje je dostupno na zvaničnom sajtu Poverenika: poverenik.rs

37 Sud pravde EU, 2014, Slučajevi C-293/12 i C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, dostupno na: curia.europa.eu

38 Dostupno na zvaničnom sajtu Agencije Evropske unije za osnovna prava, na adresi: fra.europa.eu

39 Radna grupa 29, 2018, Smernice za pristanak prema Uredbi 2016/679, dostupno na: ec.europa.eu

ZAKONITOST OBRADE PODATAKA

ZAKONITOST OBRADE PODATAKA

KADA JE OBRADA ZAKONITA?

Kada govorimo o zakonitosti obrade ličnih podataka, u suštini govorimo o tome da rukovalac ima pravo da vrši obradu samo ukoliko je ona utemeljena, zasnovana na jednom od šest raspoloživih pravnih osnova. Drugim rečima, kada odredi za koju su mu svrhu podaci potrebni, rukovalac mora da se odluči na osnovu kog pravnog osnova će se obrada vršiti - jer pravila obrade u velikoj meri od toga zavise. Ako obrada za željenu svrhu ne može da se zasnuje ni na jednom od raspoloživih pravnih osnova, onda je takva obrada nedozvoljena, odnosno nezakonita. Takođe treba naglasiti da nijedan od pravnih osnova nije "jači" ili "bolji" od drugih, već se za osnov bira onaj koji najviše odgovara konkretnoj svrsi pre početka obrade.

Prema našem Zakonu, a u skladu sa GDPR, raspoloživi pravni osnovi su: pristanak lica na koje se podaci odnose, zaključenje i izvršenje ugovora, poštovanje pravnih obaveza, zaštita životno važnih interesa, obavljanje poslova u javnom interesu i legitimni interes rukovaoca.

PRISTANAK

Pristanak je verovatno najpoznatiji pravni osnov u GDPR eri. U prvi plan je izbio zbog toga što GDPR uspostavlja čitav niz zahteva koji moraju da se ispune da bi ovaj osnov bio valjan, čime podiže lestvicu za rukovaoca u odnosu na sve ranije propise. Ista pravila usvaja i ZZPL, prema kome legalan pristanak mora da ispuni sledeće zahteve i usvojene evropske standarde:[40]

- dat je **slobodno**, nije dat pod ucenom, pritiskom ili prinudom, što između ostalog podrazumeva da ne postoji velika neravnoteža u odnosu sa rukovaocem (u suprotnom, rukovalac teško može da dokaže da ta neravnoteža nije praktično izvršila pritisak na lice koja pristanak treba da slobodno da);
- **bezuslovan** je, što znači da nije uslovljen prihvatanjem drugih usluga ili uslova (na primer, nije spojen sa prihvatanjem celokupnih uslova poslovanja);
- **specifičan** je, odnosno dat je za konkretnu a ne neodređenu i preširoko definisanu svrhu (ako je svrha određena preširoko, to bi praktično vodilo blanko pristanku za svrhe koje licu uopšte nisu bile poznate u trenutku pristajanja, te zapravo ni ne zna za šta je sve dalo svoju saglasnost);
- ukoliko postoji više svrha na koje je potrebno da lice pristane, pristanak mora biti **granuliran**, što znači da jasan pristanak treba da se da za svaku pojedinačnu svrhu;
- **informisan** je, lice razume na šta pristaje, ima sve potrebne informacije od rukovaoca da bi moglo da donese informisanu odluku;
- **nedvosmislen** je, što podrazumeva da radnja davanja pristanka mora biti jasna afirmativna radnja, a ne pasivno držanje (aktivan *opt-in*, a ne *opt-out*);
- da bi, u slučaju potrebe, rukovalac mogao da dokaže da je dobio validan pristanak, on treba da bude **dokumentovan**;

40 Ibid.

- može da se **povuče** u bilo koje vreme, i to jednostavno i lako, odnosno rukovalac mora da obezbedi da na isti način na koji je pristanak bio dat, on može biti i povučen (nije opravdano otežavati povlačenje pristanka dodatnim formalnostima, na primer popunjavanjem formulara ili pozivanjem određenih službi, ako je pristanak dat mejlom).

Posebna pravila o davanju pristanka važe ako su davaoci deca, tj. maloletna lica. Određena posebna pravila iz ZZPL odnose se samo na obradu podataka o deci u vezi sa uslugama informacionog društva. Ako rukovalac obrađuje podatke lica mlađih od 15 godina u tom kontekstu, onda će obrada njihovih podataka biti zakonita samo ako je pristanak dalo lice koje je nosilac roditeljske odgovornosti nad detetom (obično roditelji). Ako je lice starije od 15 godina, pristanak može dati samostalno. Stoga bi rukovaoci koji pružaju usluge koje su u vezi sa uslugama informacionog društva, trebalo da uspostave mehanizme koji omogućavaju da se utvrdi da je svako lice koje daje svoj pristanak dovoljno staro da ima pravo to da učini (bez potrebe da se utvrdi tačna starosna dob). U zavisnosti od rizika koji se odnose na obradu podataka, ova verifikacija se može uraditi jednostavno, traženjem izjave da je korisnik dovoljno star da obezbedi sopstveni pristanak ili, u nekim slučajevima, korišćenjem usluge verifikacije treće strane.

U svakom slučaju, ukoliko pristanak daju maloletna lica, tekst pristanka treba da bude posebno prilagođen njihovom uzrastu.

ZAKLJUČENJE I IZVRŠENJE UGOVORA

Ugovor je čest osnov u poslovnim odnosima rukovaoca sa partnerima i korisnicima, kada je obrada neophodna za izvršenje ugovora ili kada nosilac podataka zahteva konkretne radnje pre zaključenja ugovora. Dakle, ovaj pravni osnov se zapravo sastoji iz dva pod-osnova, koja ne moraju biti korišćena istovremeno, a to su zaključenje i izvršenje ugovora.

Kod zaključenja ugovora, ovaj osnov može da se koristi ako se prikupljaju lični podaci da bi do zaključenja ugovora došlo, i to baš po zahtevu tog lica. Ovo će, na primer, biti slučaj kada lice pošalje zahtev prodavcu da dobije ponudu za kupovinu nekog proizvoda, a prodavac zadrži podatke o imenu i (mejl) adresi određeni period vremena da bi mu poslao odgovarajuću ponudu.

Kod izvršenja ugovora mora se voditi računa da su podaci zaista neophodni za izvršenje, tj. sama činjenica da su podaci dati u ugovornom kontekstu ne znači da rukovalac po ovom osnovu može da koristi sve podatke do kojih je došao. Zbog toga ovo nije odgovarajući pravni osnov za, recimo, prodavca koji hoće da profiliše svoje kupce na osnovu postojećih kupovina i da im šalje nove promotivne ponude, iako je do podataka došao u kontekstu ugovora. Takođe, ZZPL eksplicitno navodi da se radi o ugovoru baš sa licem čiji se podaci obrađuju. Dakle, ovaj pravni osnov se ne može koristiti ako se radi o izvršavanju ugovora sa nekim trećim licem. Međutim, pošto ZZPL ne navodi da ugovorna strana mora biti sam rukovalac, možemo zaključiti da se ovaj pravni osnov može koristiti i ako rukovalac obrađuje lične podatke u cilju izvršavanja ugovora između lica na koje se podaci odnose i nekog trećeg lica.[41]

POŠTOVANJE PRAVNIH OBAVEZA

Pored poštovanja ugovora, Zakon kao poseban osnov predviđa poštovanje pravnih obaveza koje ima rukovalac. Iako je termin "pravne obaveze" poprilično neodređen, uz oslanjanje na tumačenje pravila iz GDPR možemo zaključiti da se ovde

41 Rücker, D., Kugler, T. (eds.), 2018, New European General Data Protection Regulation: A Practicioner's Guide, C.H. Beck, Nomos, Hart, str. 77

u stvari radi o obavezama rukovaoca da poštuje pozitivne propise koji se na njega primenjuju.

Ako rukovalac mora da obrađuje neke podatke zato što se to od njega zahteva prema nekom drugom propisu, onda je ovaj osnov valjan ukoliko se lični podaci obrađuju samo u meri u kojoj propis to nalaže.

ZAŠTITA ŽIVOTNO VAŽNIH INTERESA

Ako je obrada nečijih ličnih podataka neophodna radi zaštite vitalnih interesa nosioca podataka ili nekog drugog fizičkog lica, onda je to dozvoljeno po ovom pravnom osnovu. Generalno govoreći, u pitanju su zapravo situacije života i smrti - na primer, obrada je neophodna za nadgledanje epidemija i njihovo širenje, ili u slučajevima humanitarnih kriznih situacija, u situacijama prirodnih katastrofa i katastrofa uzrokovanih ljudskim delovanjem. Stoga će na ovaj osnov po pravilu moći da se oslone državni organi koji imaju određene specifične nadležnosti u ovakvim situacijama ili organizacije sa javnim ovlašćenjima. Krug ostalih potencijalnih rukovalaca će biti mnogo manji.

IZVRŠENJE JAVNIH OVLAŠĆENJA

Pravni osnov koji se sastoji u obavljanju poslova u javnom interesu ili izvršenja zakonom propisanih ovlašćenja rukovaoca, po pravilu će moći da koriste samo organi vlasti, ili institucije kojima su poverena javna ovlašćenja. Da bi ovaj osnov bio validan, obrada treba da ima svoju konkretnu osnovu u zakonu.

Naime, ZZPL ne daje definicije koje bi precizirale šta sve podrazumeva javni interes ili zakonom propisano ovlašćenje. Međutim, u skladu sa odredbama člana 42 Ustava Republike Srbije koji kaže da se prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuju zakonom, važno je pojasniti šta je potrebno da bude regulisano zakonom kako bi organ vlasti mogao zakonito da obrađuje podatke koji su mu neophodni za obavljanje svojih nadležnosti i delatnosti. U tom smislu, zakon treba da reguliše: (1) koji organ vlasti je ovlašćen da obrađuje podatke o ličnosti, pri čemu organ vlasti može biti konkretno određen ili barem odrediv; (2) šta je svrha zbog koje se podaci obrađuju, što može biti regulisano direktno ili indirektno; (3) koje su vrste odnosno skup podataka koji se obrađuju, što uključuje konkretno navođenje samih identifikatora, ali i preciziranje lica na koje se podaci odnose, i (4) ko ima ovlašćenje za pristup podacima.

LEGITIMNI INTERES

Legitimni interes je pravni osnov koji rukovalac može koristiti tek pošto obavi tzv. test balansiranja, gde su na jednom tasu i pretežu njegovi legitimni interesi, dok su na drugom tasu i nisu ugroženi interesi i slobode lica na koje se podaci odnose. Naime, postoje situacije kada neki praktični interesi rukovaoca (ili trećih lica) nisu zaštićeni ili regulisani merodavnim propisima, već rukovalac mora da ih zaštiti i obezbedi sam - a da bi to mogao da postigne, neophodno je da obrađuje određene lične podatke. Međutim, s druge strane postoje interesi i osnovna prava i slobode fizičkog lica koji nalažu zaštitu podataka o ličnosti. Ukoliko interesi iz druge grupe ne preovlađuju, rukovalac može da se osloni na svoj legitimni interes kao pravni osnov za obradu ličnih podataka za konkretnu svrhu.

U tom smislu je važno napomenuti da sam rukovalac, u skladu sa načelom odgovornosti, ima obavezu da sprovede test balansiranja. U tome se može osloniti na zvanične preporuke nadležnih i relevantnih organa ili na prethodnu praksu. Takođe, ZZPL jasno reguliše da ne mora biti u pitanju legitimni interes samog rukovaoca, već to može biti i interes trećih lica.

Česti primeri legitimnog interesa jesu obrada podataka koja je neophodna radi direktnog marketinga pod odgovarajućim uslovima, ostvarivanje prava slobode izražavanja ili informacija, otkrivanje prevare ili prijavljivanje kriminalnih aktivnosti, ukazivanje na eventualne pretnje javnoj sigurnosti od strane rukovaoca, zaštita mreže i sigurnosti informacija kod rukovaoca, obezbeđenje poslovnih prostorija putem identifikacije posetilaca ili postavljanja sigurnosnih kamera, i slično.

Primena testa balansiranja u svim ovim situacijama podrazumeva da rukovalac uzme u obzir više okolnosti. Što se tiče ličnih interesa, oni su posebno važni ako je lice na koje se podaci odnose dete. Mogućnost oslanjanja na legitimni interes zavisi i od odnosa koji rukovalac ima sa konkretnim fizičkim licem, kao i od toga kakva su očekivanja tog lica. Tako će individualna prava biti ugrožena ako obrada može dovesti do isključivanja ili diskriminacije pojedinaca, do klevete ili povrede reputacije, ali i ako postoje širi emotivni uticaji kao što su iritacija, strah ili stres koji nastaju usled gubitka kontrole nad ličnim podacima, ili zbog shvatanja da oni jesu ili mogu biti zloupotrebljeni ili kompromitovani. Takođe, važno je uzeti u obzir i prirodu i osetljivost podataka koji se obrađuju. Test balansiranja interesa će teže proći podaci koji spadaju u kategoriju posebno osetljivih podataka, nego podaci koje je lice već na neki način učinilo dostupnim (mada, prema GDPR, i javno dostupni lični podaci uživaju pravnu zaštitu).

Dakle, iako legitimni interes može biti primamljiv za rukovaoce, pošto praktično može da obuhvati neograničeni broj situacija za svrhe koje ne mogu da budu opravdane drugim pravnim osnovima, savetuje se oprez. Jasno je da rukovaoci ne mogu jednostavno i jednostrano da proglase zaštitu nekih svojih interesa (kao što su razni čisto komercijalni interesi), pogotovo kad se uzme u obzir da sama lica čiji se podaci obrađuju imaju neka posebna prava koja mogu da iskoriste baš u tim situacijama, kao što je pravo na prigovor.

Na kraju valja napomenuti da prema pravilima ZZPL organi vlasti ne smeju da koriste ovaj osnov prilikom obavljanja poslova iz svoje nadležnosti.

ZAKONITOST OBRADE POSEBNIH VRSTA PODATAKA

Zakon propisuje da je obrada posebnih vrsta podataka o ličnosti u principu zabranjena, osim u izuzetnim slučajevima.[42] Drugim rečima, za obradu podataka iz ove kategorije nije dovoljno samo da postoji jedan od opisanih pravnih osnova, već mora da bude ispunjen bar još jedan dodatni uslov.[43] Dodatni uslovi u kojima je obrada posebnih vrsta podataka dozvoljena uključuju sledeće situacije:

- kada lice na koje se podaci odnose da izričit pristanak na obradu za jednu ili više svrha obrade, osim ako je zakonom propisano da se obrada ne vrši na osnovu pristanka;
- kada je obrada neophodna u cilju izvršenja obaveza ili primene zakonom propisanih ovlašćenja rukovaoca ili lica na koje se podaci odnose u oblasti rada, socijalnog osiguranja i socijalne zaštite, ako je takva obrada propisana zakonom ili kolektivnim ugovorom;
- kada je obrada neophodna u cilju zaštite životno važnih interesa lica na koje se podaci odnose ili drugog fizičkog lica, ako lice na koje se podaci odnose nije u mogućnosti da da pristanak za obradu;
- kada se obrada vrši u okviru registrovane delatnosti i uz primenu odgovarajućih mera zaštite od strane zadužbine, fondacije, udruženja ili druge neprofitne organizacije, pod uslovom da se takva obrada vrši samo u odnosu na članove, bivše članove ili lica koja imaju redovne kontakte

42 Član 17 ZZPL

43 Ovakav stav je zauzela Radna grupa 29, videti na primer Smernice za automatizovano donošenje odluka o pojedincima i profilisanje za potrebe Uredbe 2016/679 iz februara 2018. godine, dostupno na: ec.europa.eu

sa organizacijom u vezi sa ciljem organizacije;

- kada se obrađuju podaci o ličnosti koje je lice na koje se oni odnose učinilo javno dostupnim;
- kada je obrada neophodna u cilju podnošenja, ostvarivanja ili odbrane nekog pravnog zahteva ili kada sud postupa u okviru svojih nadležnosti;
- kada je obrada neophodna u cilju ostvarivanja značajnog javnog interesa određenog zakonom, pod uslovom da je takva obrada srazmerna ostvarivanju cilja, uz poštovanje suštine prava na zaštitu podataka o ličnosti i primenu odgovarajućih mera zaštite osnovnih prava lica čiji se podaci obrađuju;
- kada je obrada neophodna u svrhu preventivne medicine ili medicine rada, radi procene radne sposobnosti zaposlenih, medicinske dijagnostike, pružanja usluga zdravstvene ili socijalne zaštite odnosno upravljanja zdravstvenim ili socijalnim sistemima, na osnovu zakona ili na osnovu ugovora sa zdravstvenim radnikom, ako se obrada vrši od strane ili pod nadzorom zdravstvenog radnika ili drugog lica koje ima obavezu čuvanja profesionalne tajne;
- kada je obrada neophodna u cilju ostvarivanja javnog interesa u oblasti javnog zdravlja, kao što je zaštita od ozbiljnih prekograničnih pretnji zdravlju stanovništva ili obezbeđivanje visokih standarda kvaliteta i sigurnosti zdravstvene zaštite i lekova ili medicinskih sredstava, na osnovu zakona koji obezbeđuje odgovarajuće i posebne mere zaštite prava i sloboda lica na koje se podaci odnose, posebno u pogledu čuvanja profesionalne tajne;
- kada je obrada neophodna u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, ako je takva obrada srazmerna ostvarivanju ciljeva koji se nameravaju postići, uz poštovanje suštine prava na zaštitu podataka o ličnosti i ako je obezbeđena primena odgovarajućih i posebnih mera zaštite osnovnih prava i interesa lica na koje se ovi podaci odnose.

Prilikom obrade posebno osetljivih podataka, zbog toga što je njihova obrada u principu zabranjena, u prvi plan izbija načelo minimizacije podataka, odnosno njihova obrada treba da bude svedena na krajnji minimum koji je neophodan da bi se ostvarila svrha obrade.

Smernice

Radna grupa 29 izdala je više mišljenja i smernica na temu odgovarajuće primene pravnih osnova, pre svega u vezi sa pristankom i legitimnim interesom. U ovim dokumentima se mogu naći ilustrativni primeri situacija kada su ovi pravni osnovi primereni, a kada nisu.[44]

Što se tiče legitimnog interesa, nadležni organ Ujedinjenog kraljevstva takođe je izdao smernice koje, iako nisu obavezujuće, daju dosta korisnih primera i upućuju rukovaoce šta sve treba da se zapitaju kako bi bili sigurni da je njihova samoprocena legitimnog interesa prihvatljiva. Preporučuje se sledeći tripartitni test: (1) "test svrhe" - koji služi identifikovanju legitimnog interesa, pomoću pitanja kao što su: zbog čega želimo da obrađujemo podatke, ko sve ima koristi od te obrade, kakva je ta korist i koliko je važna za sva zainteresovana lica, da li su umešana neka etička pitanja, da li je obrada u skladu sa svim merodavnim propisima i slično; (2) "test neophodnosti" - koji treba da razreši da li se identifikovana svrha zaista može postići jedino ako se obrađuju odabrani lični podaci, uz pitanja:

44 Radna grupa 29 izdala je više smernica na ovu temu tokom godina primene Direktive 95/46/EC, a poslednja verzija smernica u skladu sa GDPR je izdata u aprilu 2018. godine, videti: Smernice za pristanak prema Uredbi 2016/679, dostupno na: ec.europa.eu. Mišljenje Radne grupe 29 o legitimnom interesu je doneto 2014. godine na osnovu teksta Direktive 95/46/EC, ali je i dalje validno, videti: Mišljenje 06/2014 o legitimnom interesu rukovaoca podacima prema članu 7 Direktive 95/46/EC, dostupno na: ec.europa.eu

da li se svrha može postići na drugi način koji ne uključuje obradu ličnih podataka, da li se može koristiti manje podataka, da li obrada može da bude manje intruzivna; (3) "test balansiranja" - koji stavlja na drugi tas interese, prava i slobode lica čiji se podaci obrađuju, uz pitanja: kakva su razumna očekivanja tih lica, da li su oni sami dali podatke, da li sa njima postoji već prethodno uspostavljena veza i kakva, kakva je vrsta podataka u pitanju, itd.[45]

Praksa

Pitanje legitimnog interesa kao pravnog osnova bila je tema jedne odluke CJEU, koji je zauzeo stav da je validan legitimni interes rukovaoca da zahteva lične podatke od treće strane kako bi mogao da pokrene sudski postupak protiv lica koje mu je prouzrokovalo štetu. U ovom slučaju je lice - nosilac podataka bilo maloletno. Međutim, stav CJEU je da sama ova činjenica nije dovoljan dokaz da prava i interesi tog lica svakako pretežu, već da je to jedna od činjenica koja mora biti uzeta u obzir prilikom sprovođenja "testa balansiranja".[46]

U vezi sa pravnim osnovom koji se tiče izvršenja javnih ovlašćenja, Poverenik je oktobra 2014. izdao upozorenje u kom se, između ostalog, navodi: "Kako je prema članu 42 Ustava Republike Srbije prikupljanje, čuvanje, obradu i korišćenje podataka o ličnosti moguće urediti isključivo zakonom, a članom 8, tačka 2 ZZPL je propisano da obrada podataka o ličnosti nije dozvoljena ako fizičko lice nije dalo pristanak za obradu, odnosno ako se obrada vrši bez zakonskog ovlašćenja, tako i skup podataka o ličnosti koje se obrađuje i svrha obrade moraju biti definisani samim zakonom. Podzakonskim propisima moguće je urediti način pribavljanja (od koga se podaci prikupljaju), kao i druge tehničke detalje prikupljanja zakonski definisanih podataka od trećih lica, ali se ne može određivati rukovalac podataka koji je ovlašćen da prikuplja podatke, kao ni svrha, odnosno skup podataka koji se mogu obrađivati" (Upozorenje broj 164-00-00300/2012-07 od 03.10.2014. godine).

Dileme

Jedna od glavnih tema tokom priprema evropskih kompanija za GDPR, bio je strah od mogućnosti da će nova regulativa zahtevati od rukovalaca da za veliki broj svojih procesa obrade ličnih podataka imaju validan pristanak. Pristanak je tih meseci postao toliko popularan, da se u određenim krugovima raširila ideja kako je on glavni i superiorni pravni osnov, dok su svi ostali pravni osnovi manje bitni. Ta ideja nije tačna, a svakako može biti veoma opasna. Pristanak nije glavni ni najbolji osnov, a često nije ni odgovarajući. Svi pravni osnovi su ravnopravni i svi funkcionišu u određenim okolnostima, dok u nekim drugim uopšte nisu primereni ili su čak nezakoniti.

Primer hotela kao rukovaoca podacima o ličnosti može da ilustruje kako ponekad i isti podaci mogu da se obrađuju po više pravnih osnova, uvek u zavisnosti od konkretne svrhe obrade. Kada gost dođe u hotel da iznajmi sobu ili zatraži druge usluge hotela, svakako treba da da određene podatke koji su neophodni da bi se zaključio i izvršio ugovor o smeštaju. Hotel takođe ima obavezu da određene podatke koje tom prilikom prikupi, dostavi policiji u skladu sa merodavnim propisima koji ga na to obavezuju. Tokom boravka u hotelu, gostu može biti ponuđeno da koristi određene neobavezne pogodnosti, na primer da učestvuje u tzv. lojaliti programu - u tom slučaju on daje pristanak za obradu podataka u te svrhe, a svoj pristanak može

45 Detaljne smernice Kancelarije britanskog Poverenika su dostupne na: ico.org.uk

46 Sud pravde EU, 2017, Slučaj C-13/16, Valsts policijas R gas re iona p rvaldes K rt bas policijas p rvalde v R gas pašvald bas SIA 'R gas satiksme', paras. 29, 33, dostupno na: curia.europa.eu

u bilo kom trenutku povući bez posledica na pružanje usluga po osnovu glavnog ugovora o smeštaju. Dodatne pogodnosti mogu, na primer, uključivati i spremanje određene vrste hrane u skladu sa njegovim verskim ubeđenjima ili zdravstvenim stanjem, u kom slučaju za ovu svrhu gost mora da da eksplicitan pristanak, dok se takvi podaci moraju tretirati kao posebno osetljivi. Ako se prilikom boravka u hotelu dogodi neka nesreća, na primer požar, može doći u obzir i obrada podataka gostiju po osnovu zaštite njihovih vitalnih interesa. Najzad, po odlasku iz hotela, svojim bivšim gostima hotel može odlučiti da šalje određene promotivne poruke po osnovu svog legitimnog interesa.

Što se tiče pristanka, nema govora o tome da se on traži od nosilaca podataka onda kada je zakonska obaveza rukovaoca da prikuplja neke podatke, ili kada su podaci neophodni radi izvršenja ugovora sa tim licem. U praksi srpskih kompanija često se, na primer, dešavalo da zaposleni potpisuju izjave da su saglasni da se koriste njihovi lični podaci, dok prema pozitivnim domaćim propisima poslodavci imaju obavezu da od zaposlenih prikupljaju na desetine raznih podataka kako bi mogli da izvrše sve obaveze iz oblasti rada, poreza, doprinosa, bezbednosti i zaštite na radu, evidencija iz oblasti rada i slično. Pored toga, postoji i obaveza izvršavanja ugovora o radu. Ovo naravno ne znači da od zaposlenih ne treba tražiti pristanak onda kada je taj pravni osnov jedino moguć - na primer, kada zaposleni pristaju da poslodavac za njih ostvaruje neke pogodnosti, kao što su razne vrste dobrovoljnih osiguranja, za šta je potrebno da poslodavac uđe u dodatne procese obrade ličnih podataka pored onih koji su obavezni.

Takođe, često postoji konfuzija oko toga da li se za određene procese obrade rukovalac može osloniti na svoj legitimni interes, ili treba da traži pristanak. Koji je od ovih osnova više primeren zavisi pre svega od svrhe obrade, ali i drugih okolnosti. Međutim, rukovalac uvek može da se zapita šta su posledice za ostvarivanje konkretne svrhe ako lice povuče pristanak i zahteva brisanje podataka. Pošto su pravila u vezi sa pristankom takva da se u tom scenariju mora smesta prekinuti sa obradom podataka, ukoliko rukovalac bez obrade ne može da ostvari željenu svrhu, pristanak kao pravni osnov svakako nije rešenje. Takođe, ako je rukovalac za ispunjenje određene svrhe inicijalno odlučio da obrađuje lične podatke na osnovu pristanka - ukoliko lice odluči da pristanak povuče i traži brisanje podataka, rukovalac nema pravo da se predomisli u vezi sa ustanovljenim pravnim osnovom, pa da podatke u istom procesu nastavi da obrađuje po osnovu legitimnog interesa.

S druge strane, ako je test balansiranja pokazao da interesi nosilaca podataka nisu u konkretnoj situaciji ugroženi u značajnoj meri, nema mesta traženju bilo kakve saglasnosti za obradu od tih lica. Ako je osnov za obradu legitimni interes rukovaoca, koji su eventualno već potvrdili sud ili Poverenik, nosilac podataka nema neograničeno pravo da zahteva da se obrada zaustavi i da se podaci brišu. Ostvarivanje tih prava moguće je samo pod određenim uslovima, dok su mu na raspolaganju i neka druga prava, kao što je pravo na prigovor.

TEHNIČKE MERE ZAŠTITE PODATAKA O LIČNOSTI

TEHNIČKE MERE ZAŠTITE PODATAKA O LIČNOSTI

Svet dnevno proizvodi 2.5 kvintiliona bajtova[47] podataka dnevno.[48] Kako se tehnologija sve više integriše u naše privatne i profesionalne živote, udeo podataka koji se mogu smatrati ličnim podacima postaje sve veći. Samim tim, rastu i rizici po lične podatke u digitalnom okruženju. Česte zloupotrebe kreću se od kompanija koje profilišu korisnike kako bi njihove profile, zasnovane na ličnim podacima, koristili ili preprodavali za oglašavanje; preko državnih organa koji nadziru sve građane bez razlike, kako bi uštedeli resurse ili se obračunavali sa političkim neistomišljenicima - sve do različitih vrsta sajber predatora i pljačkaša koji kupovinu preko interneta vrše tuđim kreditnim karticama.

Podaci su postali valuta za onlajn plaćanje raznih vrsta dobara, pa je i radikalan predlog da prestanemo sa korišćenjem svih tih "besplatnih" servisa postao besmislen i neefikasan. U najvećem broju slučajeva, privatnost u onlajn sferi može se u dobroj meri zaštititi održavanjem "higijene" ličnih podataka i razvojem svesti o postojećim rizicima.

PRIVATNOST I BEZBEDNOST

Koncepti privatnosti i bezbednosti blisko su povezani. Sistem ne može biti smatran privatnim ako nije bezbedan i obrnuto. Bezbednost informacionog sistema je kompleksna materija sačinjena od više komponenata i faktora koji utiču na nju, a jedan od njih svakako je privatnost.

Nedekvatna zaštita ličnih podataka u okviru informacionog sistema može dovesti do različitih problema, počev od finansijskih kazni propisanih domaćom i evropskom regulativom; može uticati na kontinuitet rada, odnosno funkcionisanje sistema, ili ugroziti bezbednost lica na koja se podaci odnose. Posledice po kredibilnost i reputaciju organizacije koja je pretrpela bezbednosni incident su dugoročne i mogu dovesti do teških gubitaka.

TEHNIČKE MERE PO NOVOJ REGULATIVI

GDPR se ne bavi specifičnim detaljima u vezi sa tehničkim merama koje treba da osiguraju adekvatan nivo zaštite podataka. Takav pristup ima u vidu brzinu kojom se tehnologija razvija i relativan odnos trenutno odgovarajućih mera sa tehnološkim razvojem u određenom periodu. Takođe, tehničke mere svrstane su zajedno sa organizacionim, budući da su u uzajamnoj vezi te da i na najsloženije informacione sisteme, pored tehničkih aspekata, presudno utiče ljudski faktor.

Proces uspostavljanja principa podrazumevane privatnosti (*privacy by default*) u sistemu polazi od privatnosti kao temeljnog uslova, dok ne sme da zanemari upotrebljivost i funkcionalnu komponentu; sistem koji je previše komplikovan za korišćenje će biti napušten, bez obzira koliko su dobri tehnički standardi zaštite privatnosti i bezbednosti.

Sistem ne mora da čini jedan softver koji je implementirala treća strana. On može biti sačinjen od seta različitih programa i procedura koje sama organizacija definiše, što je upravo i slučaj kod

47 2,500,000,000,000,000,000 B = 2,500,000,000 GB = 2.5 Exabytes

48 Marr, B., 2018, How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read, Forbes, dostupno na: forbes.com

mnogih malih preduzeća. Na primer, organizacija može koristiti *Microsoft Office* za kancelarijske poslove i *Dropbox* za onlajn čuvanje podataka.

BEZBEDNOST OBRADE

Domaći Zakon se uzgred dotiče tehničkih, kadrovskih i organizacionih mera zaštite podataka o ličnosti u članovima 41 i 42, a detaljnije se bezbednošću podataka bavi u članu 50.

Konkretno, ZZPL koncept tehničkih mera uvodi zajedno sa kadrovskim i organizacionim merama. Zakon propisuje primenu *odgovarajućih* mera u skladu sa prirodom, obimom, okolnostima i svrhom obrade, te sa verovatnoćom nastupanja i stepenom rizika po prava i slobode fizičkih lica. Takođe, uređuje se i dokazivanje primene mera.

Član 50 ZZPL, kao i 32 GDPR, predviđa nivo neophodne bezbednosti koji treba da se primeni prilikom obrade podataka o ličnosti. Prema ovoj odredbi, utvrđivanje odgovarajućeg nivoa i mera treba da bude zasnovano na dostupnoj tehnologiji, prirodi, obimu i svrsi obrade, kao i na proceni rizika, tj. implikacija koje bi incident mogao da ima po ljudska prava.

Postoje mnogi faktori koji se smatraju relevantnim u procesu definisanja bezbednosnih mera i protokola, uključujući veličinu organizacije, grupe podataka koja se prikuplja i dalje obrađuje, vrstu zaposlenih koji dolaze u kontakt sa podacima, itd. Međutim, najvažniji faktor jeste procena rizika koja se sprovodi od slučaja do slučaja; ne postoji opšti rizik koji se može pripisati određenoj vrsti podataka, pošto kontekst može široko da varira.

Četiri principa proističu iz stava 1, člana 50 ZZPL, odnosno člana 32 GDPR, i koliko god se činili široko postavljenim, oni pokrivaju sve aspekte bezbednosti i pouzdanosti sistema. To su:

1. Pseudonimizacija i enkripcija podataka o ličnosti.
2. Mogućnost da se kontinuirano obezbede poverljivost, integritet, dostupnost i otpornost sistema i usluga za obradu podataka.
3. Mogućnost da se ponovo uspostave dostupnost i pristup podacima o ličnosti na blagovremen način u slučaju fizičkog ili tehničkog incidenta.
4. Proces redovnog testiranja, procene i evaluacije efektnosti tehničkih i organizacionih mera za očuvanje bezbednosti obrade.

UGRAĐENA I PODRAZUMEVANA PRIVATNOST

Koncepti ugrađene, odnosno privatnosti po dizajnu i podrazumevane privatnosti (*privacy by design* & *privacy by default*) predstavljaju međunarodni standard i, mada se u novom Zakonu ne pominju izričito, smisao ovih principa je razrađen u članu 42:

- Minimizacija količine podataka kroz pseudonimizaciju (stav 1, tačka 1).
- Primena neophodnih mehanizama zaštite u toku obrade kako bi se ispunili uslovi za obradu propisani ZZPL i zaštita prava i sloboda lica čiji se podaci obrađuju (stav 1, tačka 2) - što je primena principa *privacy by design*.
- Obrađuju se samo oni podaci o ličnosti koji su neophodni za ostvarivanje svake pojedinačne svrhe obrade (stav 2) - što je primena principa *privacy by default*.

Ovim principima treba da se vodi rukovalac prilikom određivanja načina obrade, odnosno pre nego što je obrada uopšte započela, tako da njihova primena adekvatno prati tehnološka dostignuća, imajući u vidu troškove, prirodu, obim, okolnosti i svrhu obrade, kao i nivo i verovatnoću nastupanja rizika po prava i slobode fizičkih lica, a koji proizlaze iz obrade.

S druge strane, GDPR eksplicitno uvodi koncepte zaštite podataka *by design* i *by default*, čime nedvosmileno nameće obaveze da se privatnost podataka razmatra u početnim stadijumima dizajna projekta,

ali i tokom čitavog životnog ciklusa obrade podataka. Ova obaveza je izričito propisana samo za rukovaoce.

Smernice

Još sredinom 1990-tih, tadašnja kanadska Poverenica za informacije i privatnost objavila je sedam osnovnih principa poštene prakse pri obradi podataka, na kojima je utemeljen koncept privatnosti po dizajnu:

1. **Proaktivnost umesto reaktivnosti** - podrazumeva da se što veći broj rizika prepozna i smanji, kako bi se najveći deo pretnji sprečio pre nego što se ostvare.
2. **Privatnost kao standardna postavka** - u sistemu su predefinisane konzervativne vrednosti u odnosu na podatke, odnosno implementiraju minimizovanu obradu podataka bez dodatnih, "opcionih" obrada. Ukoliko se korisnik odluči da hoće da koristi dodatne mogućnosti, onda svesno bira uključenje dodatnih obrada.
3. **Privatnost ugrađena u dizajn** - podrazumeva da se sistem projektuje i da se njime upravlja na način koji uzima u obzir privatnost subjekata čiji se podaci u okviru tog sistema obrađuju. Ovaj princip prati ceo životni ciklus obrade, od planiranja do uništenja podataka.
4. **Puna funkcionalnost** - "pozitivna suma" umesto "nulte sume", podrazumeva da implementacija mera koje se odnose na privatnost ne predstavlja opterećenje za poslovanje, odnosno da se ove mere implementiraju tako da stimulišu razvoj poslovanja, umesto da ga ometaju obavezama.
5. ***End-to-End* bezbednost** - mere zaštite ličnih podataka se primenjuju od početka do kraja obrade, odnosno od unošenja podataka, preko procesuiranja i transfera, do skladištenja i brisanja.
6. **Vidljivost i transparentnost** - proces obrade i implementirane mere zaštite su transparentno objašnjeni licima čiji se podaci obrađuju.
7. **Poštovanje individualne privatnosti** - podrazumeva da je *suština* zaštite podataka o ličnosti, zapravo zaštita lične privatnosti pojedinca, ta da se ceo sistem postavlja oko prava pojedinca na privatnost.[49]

PROCENA RIZIKA

Prvi korak u izboru odgovarajućih mera koje štite integritet i bezbednost podataka, a da pri tom ne ometaju poslovanje, jeste procena rizika. To praktično znači da treba utvrditi šta sve može ugroziti bezbednost i kolika je verovatnoća da se to i desi. Ako se server sa podacima nalazi u podrumu, na primer, podaci su izloženi riziku od poplave - što ne znači da će do poplave ikada doći, ali bi bilo razumno postaviti servere na nosače iznad poda.

Preduslov dobre procene rizika jeste dobro poznavanje sistema, odnosno opreme koja se koristi, hardvera i softvera, kao i klasifikacija podataka koji se obrađuju. Drugim rečima, potrebno je *mapirati resurse*. U slučaju opreme, to obično znači popisivanje pojedinačnih uređaja i redovno ažuriranje popisa, prema tipu i modelu uređaja, datumu nabavke, eventualnom isteku licence, podrške ili osiguranja, zaposlenom koji koristi uređaj ili je odgovoran za njegovo korišćenje, i slično.

Podaci se klasifikuju prema stepenu osetljivosti ili tajnosti u odnosu na koji se primenjuju konkretne mere zaštite, odnosno procedure pristupa. Stepen tajnosti podataka zavisi od poslovanja i internih odluka u okviru organizacije, dok je osetljivost kriterijum propisan Zakonom (odredbe o posebnim vrstama podataka) i mora se poštovati bez obzira na interese organizacije.

49 Cavoukian, A., 2010, Privacy by Design - The 7 Foundational Principles, dostupno na: iab.org

Primer klasifikacije podataka

Vrsta podataka	Mere zaštite
Javni podaci	Procedure za zaštitu integriteta podataka (tehničke mere koje obezbeđuju dostupnost usluge; npr. antivirus program, fizičko obezbeđenje opreme)
Podaci dostupni zaposlenima	Procedure za zaštitu internih podataka
Podaci dostupni menadžmentu	
Poverljivi podaci	Procedure za zaštitu poverljivih i osetljivih/ posebnih podataka
Strogo poverljivi podaci Osetljivi/posebni podaci	

Primer mapiranja podataka

Set podataka	Gde se čuva?	Ko može da pristupi?	Koliko su podaci osetljivi?	Mere zaštite
Baza poverljivih informacija	Zaštićena datoteka na klaud serveru	Samo vlasnik baze	Strogo poverljivi/ Posebni	Procedura za zaštitu poverljivih i posebnih podataka
Baza podataka o istoriji poslovanja	Veb server	Svako	Javni podaci	Procedura za zaštitu integriteta podataka
Informacije o platama u organizaciji	Registratori kod knjigovođe	Finansijski menadžer i direktor	Poverljivi podaci	Procedura za zaštitu internih podataka

Pošto se ustanovi čime se raspolaže, gde se šta nalazi i kako mu se može pristupiti, potrebno je *identifikovati pretnje,* odnosno utvrditi šta sve može da ugrozi informacioni sistem. Metodološki pristup je stvar interne odluke organizacije, prema vlastitim potrebama i prilikama u kojima posluje, ali je značajno obuhvatiti sve delove organizacije jer svaka od njih može biti izložena drugačijim pretnjama. Važno je popisati i što širi opseg pretnji, bez obzira na to koliko su verovatne, da li dolaze spolja ili unutar organizacije, da li su tehnički napredne ili su posledica prirodnih nepogoda.

Primer identifikacije pretnji

Pretnja	Šta je pretnja?
Cilj	Ko je meta pretnje (pojedinac, organizaciona jedinica, cela organizacija)?
Izvor pretnje	Ko stoji iza pretnje?
Kapacitet izvora pretnje	Opisati koje su jače strane, prednosti i mogućnosti izvora pretnje, koje bi doprinele da se pretnja ostvari
Preduslovi	Koji su preduslovi da se pretnja ostvari?
Gde	Koja su fizička i/ili logička mesta gde se pretnja može ostvariti?
Naš kapacitet	Koje procedure i kapacitete imamo, koji bi mogli da spreče realizaciju pretnje?
Naše ranjivosti	Koji naši nedostaci mogu doprineti realizaciji pretnji?

Kada se utvrde moguće pretnje, potrebno je proceniti njihov uticaj na poslovanje kao što su ometanje ili obustavljanje rada, dodatni troškovi, materijalna šteta, zakonska odgovornost i slično.

Konačno, dobra procena rizika zavisi i od razumnog utvrđivanja verovatnoće da se neka pretnja ostvari. Mada je korisno imati u vidu sve moguće pretnje, besmisleno je trošiti sredstva na zaštitu opreme od, recimo, peščane oluje - ako se serveri nalaze u području umereno-kontinentalne klime.

Ukrštanje uticaja pretnje i verovatnoće da se ona ostvari, za rezultat daje konačnu procenu rizika. Na jednom kraju zamišljene skale procene rizika biće mala verovatnoća da će se realizovati pretnja koja neće naročito uticati na poslovanje, dok će na suprotnom kraju biti neposredna pretnja koja može da ugrozi čitavo poslovanje organizacije.

Procena rizika tako postaje lista prioriteta kojima organizacija treba da se što pre pozabavi.

MERE ZAŠTITE

Standardne mere koje se danas primenjuju obuhvataju sistem privilegija, enkripciju, pseudonimizaciju i slično.

PRIVILEGIJE I ROLE

Važan segment bezbednosti podataka u informacionom sistemu rešava se kontrolom pristupa različitim setovima podataka i to kroz sistem privilegija i rola, odnosno definisanjem različitih uloga u obradi podataka za različite grupe zaposlenih, poslovnih partnera i korisnika. Neke setove podataka mogu da vide svi bez razlike, u druge uvid mogu da imaju samo stručni saradnici, treće mogu da menjaju samo zaposleni sa posebnim ovlašćenjima, itd. Role se definišu u skladu sa potrebama i obavezama u organizaciji, dok informacioni sistem automatski registruje vreme i mesto svakog pristupa.

Ovaj sistem podrazumeva dodelu korisničkih naloga i neki oblik potvrde vlasništva - lozinkom, kvalifikovanim ser-

tifikatom, biometrijskim informacijama. Lozinke ili šifre su najčešći metod autentifikacije i zato je važno da budu što kompleksnije, da ne sadrže podatke o korisniku ni reči prirodnog jezika.

KRIPTOVANJE DISKOVA

Enkripcija ili automatsko šifriranje sadržaja postaje opšti standard u zaštiti bezbednosti informacionih sistema, odnosno podataka koji se u sistemu obrađuju. Lokalna enkripcija diskova odnosi se na fizičke uređaje na kojima se čuvaju važni podaci kao dodatni metod zaštite, odnosno novi nivo kontrolisanog pristupa. U slučaju krađe kompjutera ili diskova, enkripcija je solidna prepreka neovlašćenom pristupu podacima.

Praksa

Regionalni sud u Vircburgu je 13. septembra 2018. godine izdao privremenu zabranu advokatu koji je na svojoj internet stranici imao politike privatnosti neusklađene sa GDPR-om, dok kontakt forma za komunikaciju nije bila zaštićena enkripcijom. Sud je prilikom obrazloženja odluke istakao da oba nedostatka predstavljaju povredu odredbi GDPR-a, te je advokatu zapretio kaznom od 250.000 evra ukoliko ne ispuni obavezu usklađivanja.[50]

PSEUDONIMIZACIJA I ANONIMIZACIJA

Tokom čitavog procesa obrade ličnih podataka, ukoliko se oni ne moraju čuvati u izvornom obliku, preporučuje se anonimizacija ili pseudonimizacija. Anonimizacija podrazumeva nepovratan prekid veza između podataka i identiteta osobe na koju se ti podaci odnose. Pseudonimizacija je privremeno maskiranje podataka koji se po potrebi mogu vratiti u izvorni oblik, obično uz pomoć šifrarnika ili orginalnog dokumenta.

Primer

Podatak	Pseudonimizacija	Anonimizacija
Pera Perić	OSOBA 1	XXX XXX
Žika Mikić	OSOBA 2	XXX XXX
Milica Milić	OSOBA 3	XXX XXX
Pera Perić	OSOBA 1	XXX XXX

OBAVEŠTAVANJE POVERENIKA

Rukovalac je u obavezi da obavesti Poverenika o svakoj povredi podataka o ličnosti. Zakon izričito navodi da je rukovalac dužan da, ukoliko povreda podataka o ličnosti može da proizvede rizik po prava i slobode fizičkih lica, obavesti Poverenika bez nepotrebnog odlaganja ili ukoliko je moguće u roku od 72 časa od saznanja za povredu. Dodatno, rukovaocu je ostavljena mogućnost da, ukoliko ne obavesti Poverenika u propisanom roku, obrazloži razloge zbog kojih nije postupio u roku. Obrađivač je dužan da, posle saznanja o povredi, bez nepotrebnog odlaganja obavesti rukovaoca o incidentu.

Zakon takođe taksativno navodi koje sve informacije mora da sadrži takvo obaveštenje: opis prirode povrede podataka o ličnosti, približan broj lica na koja se podaci odnose, opis mogućih posledica povrede, opis mera koje je rukovalac preduzeo, i slično. Bitno je istaći da Zakon ostavlja mogućnost postupnog dostavljanja informacija, ukoliko se sve ne mogu dostaviti istovremeno.

Na kraju, Zakon propisuje još jednu obavezu za rukovaoca koji je dužan da dokumentuje svaku povredu podataka o ličnosti, uključujući i činjenice o povredi, njenim posledicama i preduzetim merama za njihovo otklanjanje.

50 Regionalni sud u Vircburgu, 2018, Odluka 11 O 1741/18 UWG, dostupno na: gesetze-bayern.de

OBAVEŠTAVANJE LICA NA KOJE SE PODACI ODNOSE

Pored obaveštavanja Poverenika, ZZPL propisuje obavezu obaveštavanja bez odlaganja lica na koje se podaci odnose. Ovakva obaveza se odnosi na rukovaoca u slučajevima kada povreda podataka o ličnosti može da proizvede visok rizik po prava i slobode fizičkih lica, s tim da je rukovalac dužan da u obaveštenju, na jasan i razumljiv način, opiše prirodu povrede podataka i licu pruži informacije o kontaktu lica za zaštitu podataka o ličnosti, opisu mogućih posledica povrede, te da navede mere koje je predložio, odnosno preduzeo u vezi sa povredom što uključuje i mere preduzete u cilju umanjenja štetnih posledica povrede.

Takođe, Zakon predviđa nekoliko izuzetaka od ove obaveze, u slučajevima kada je:

- rukovalac preduzeo odgovarajuće tehničke, organizacione i kadrovske mere zaštite u odnosu na podatke o ličnosti čija je bezbednost povređena, a posebno ako je kriptozaštitom ili drugim merama onemogućio razumljivost podataka svim licima koja nisu ovlašćena za pristup ovim podacima;
- rukovalac naknadno preduzeo mere kojima je obezbedio da povreda podataka o ličnosti sa visokim rizikom za prava i slobode lica na koje se podaci odnose više ne može da proizvede posledice za to lice;
- obaveštavanje lica na koje se podaci odnose predstavljalo nesrazmeran utrošak vremena i sredstava. U tom slučaju, rukovalac je dužan da putem javnog obaveštavanja ili na drugi delotvoran način obezbedi pružanje obaveštenja licu na koje se podaci odnose. Ako rukovalac nije obavestio lice na koje se podaci odnose o povredi podataka o ličnosti, Poverenik može, uzimajući u obzir mogućnost da povreda podataka proizvede visok rizik, da naloži rukovaocu da to učini ili može da utvrdi da su ispunjeni uslovi o nesrazmernom utrošku.

OSTALE OBAVEZE

OSTALE OBAVEZE

LICE ZA ZAŠTITU PODATAKA O LIČNOSTI

Lice za zaštitu podataka o ličnosti je osoba stručnih kvalifikacija, a naročito stručnog znanja i iskustva u oblasti zaštite podataka o ličnosti u pogledu nacionalnog i međunarodnog zakonodavstva. Ova pozicija treba da predstavlja glavnu sponu između organizacije koja obrađuje podatke o ličnosti i svih lica na koja se podaci odnose, u pogledu informisanja kao i ostvarivanja zakonom zagarantovanih prava. Njen glavni zadatak je da se stara da organizacija primenjuje sva pravila u vezi sa zaštitom podataka o ličnosti, odnosno da nadzire usklađenost sa Zakonom. Između ostalog, lice za zaštitu podataka o ličnosti dužno je da osigura da organizacija obrađuje podatke o ličnosti svojih zaposlenih, klijenata ili bilo koje druge osobe u skladu sa zakonskim normama.

KADA POSTOJI OBAVEZA?

ZZPL utvrđuje da obaveza postavljanja lica za zaštitu podataka o ličnosti postoji u slučajevima kada se:

- obrada vrši od strane organa vlasti, osim ako se radi o obradi koju vrši sud u svrhu obavljanja sudskih ovlašćenja;
- osnovne aktivnosti rukovaoca ili obrađivača sastoje u radnjama obrade koje po svojoj prirodi, obimu, odnosno svrhama zahtevaju redovan i sistematski nadzor velikog broja lica na koje se podaci odnose;
- osnovne aktivnosti rukovaoca ili obrađivača sastoje u obradi posebnih vrsta podataka o ličnosti ili podataka o ličnosti u vezi sa krivičnim presudama i kažnjivim delima, u velikom obimu.

Ovakva zakonska definicija, preuzeta iz GDPR-a, ipak ostavlja prostora za nedoumice, jer određeni pojmovi nisu dovoljno jasno definisani.

Smernice

Radna grupa 29 daje pojašnjenje formulacije "redovan i sistematski nadzor", pa ukazuje da redovan nadzor može biti nadzor koji je u toku ili u određenim intervalima za određen period; da se ponavlja u određenom definisanom periodu; da se dešava konstantno ili periodično. Sistematski nadzor može imati više značenja: događa se prema sistemu; unapred je dogovoren; organizovan je ili metodičan; određuje se kao deo opšteg plana za prikupljanje podataka; sprovodi se kao deo strategije.[51]

Dodatno, domaći Zakon predviđa mogućnost postavljanja zajedničkog lica za zaštitu podataka o ličnosti, te navodi da grupa privrednih subjekata može odrediti zajedničko lice za zaštitu podataka o ličnosti, pod uslovom da je ovo lice jednako dostupno svakom članu grupe. U slučaju da su rukovaoci ili obrađivači organi vlasti ili nadležni organi, može se odrediti zajedničko lice za zaštitu podataka o ličnosti, uzimajući u obzir organizacionu strukturu i veličinu tih organa vlasti.

Smernice

Evropski supervizor za zaštitu podataka o ličnosti ističe da bi postavljanje zajedničkog lica za zaštitu podataka o ličnosti bilo praktično rešenje za manje organe vlasti kod kojih imenovanje stalnog lica za zaštitu podataka ne bi bilo praktično. Bitno je istaći da se u ovakvoj situaciji mora voditi računa o tome da organi vlasti budu povezani funkcionalno i organi-

51 Radna grupa 29, 2017, Smernice za lica za zaštitu podataka o ličnosti, str. 8-9, dostupno na: ec.europa.eu

zaciono, dok imenovanje zajedničkog lica za zaštitu podataka o ličnosti ne umanjuje zakonske obaveze rukovalaca, odnosno obrađivača.[52]

ZZPL takođe propisuje uslove na osnovu kojih se određuje lice za zaštitu podataka o ličnosti, a to su stručne kvalifikacije, stručno znanje i iskustvo u oblasti zaštite podataka o ličnosti, kao i sposobnost za izvršavanje zakonskih obaveza. Međutim, Zakon propušta da bliže definiše koje su to kvalifikacije, stručna znanja i iskustva, odnosno da odredi način na koji se ovi kriterijumi utvrđuju.

Smernice

Radna grupa 29 u objavljenim smernicama o licu za zaštitu podataka o ličnosti navodi da stručno znanje nije strogo definisano, ali da mora biti srazmerno osetljivosti, kompleksnosti i količini podataka koje se obrađuju, odnosno ukoliko se obrađuje velika količina osetljivih podataka o ličnosti onda se podrazumeva da lice za zaštitu podataka o ličnosti mora imati veći nivo stručnog znanja. Takođe, s obzirom na zadatke koje obavlja, neophodno je da lice za zaštitu podataka o ličnosti poseduje znanje u oblasti nacionalnih i evropskih zakona kao i praksi koje se odnose na zaštitu podataka o ličnosti.[53]

S obzirom da je evropska regulativa temelj i domaćeg Zakona, u Srbiji bi se ovim uslovima moglo dodati i stručno poznavanje GDPR-a.

POLOŽAJ LICA ZA ZAŠTITU PODATAKA O LIČNOSTI

Pored imenovanja lica za zaštitu podataka o ličnosti, neophodno je utvrditi njegov položaj, stoga Zakon propisuje obavezu kojom su:

- rukovalac i obrađivač dužni da blagovremeno i na odgovarajući način uključe lice za zaštitu podataka o ličnosti u sve poslove koji se odnose na zaštitu podataka o ličnosti;
- rukovalac i obrađivač dužni da omoguće licu za zaštitu podataka o ličnosti izvršavanje zakonskih obaveza na taj način što mu obezbeđuju neophodna sredstva za izvršavanje ovih obaveza, pristup podacima o ličnosti i radnjama obrade, kao i njegovo stručno usavršavanje;
- rukovalac i obrađivač dužni da obezbede nezavisnost lica za zaštitu podataka o ličnosti u izvršavanju njegovih obaveza.

Zakon uređuje i odnos između lica na koja se podaci odnose i lica za zaštitu podataka o ličnosti, tako što lice za zaštitu podataka o ličnosti čini ključnom tačkom za sva pitanja u vezi sa zaštitom podataka - lica na koje se podaci odnose mogu se obratiti licu za zaštitu podataka o ličnosti u vezi sa svim pitanjima koja se odnose na obradu njihovih podatka, kao i u vezi sa ostvarivanjem svojih prava propisanih Zakonom. Dodatno, lice za zaštitu podataka o ličnosti dužno je da čuva tajnost, odnosno poverljivost podataka do kojih je došlo u izvršavanju svojih obaveza.

Smernice

Preporuke Radne grupe 29 u pogledu položaja lica za zaštitu podataka o ličnosti govore da je od presudnog značaja da lice za zaštitu podataka o ličnosti bude što ranije uključeno u sve procese koji se odnose na zaštitu podataka. Takođe, ovo lice bi trebalo da:

- učestvuje na sastancima višeg i srednjeg menadžmenta,
- bude prisutno prilikom donošenja odluka koje se odnose na zaštitu podataka,
- bude odmah konsultovano u slučaju povrede podataka o ličnosti.[54]

52 EDPS, 2018, Mišljenje o ulozi lica za zaštitu podataka o ličnosti u institucijama i telima EU, str. 5, dostupno na: edps.europa.eu
53 Radna grupa 29, 2017, Smernice za lica za zaštitu podataka o ličnosti, str. 11, dostupno na: ec.europa.eu
54 Ibid., str. 13-14

OBAVEZE LICA ZA ZAŠTITU PODATAKA O LIČNOSTI

Zakon taksativno navodi obaveze lica za zaštitu podataka o ličnosti:

- informiše i daje mišljenje rukovaocu ili obrađivaču, kao i zaposlenima koji vrše radnje obrade o njihovim zakonskim obavezama u vezi sa zaštitom podataka o ličnosti;
- prati primenu odredbi ZZPL, drugih zakona i internih propisa rukovaoca ili obrađivača koji se odnose na zaštitu podataka o ličnosti, uključujući i pitanja podele odgovornosti, podizanja svesti i obuke zaposlenih koji učestvuju u radnjama obrade, kao i kontrole;
- daje mišljenje, kada se to zatraži, o proceni uticaja obrade na zaštitu podataka o ličnosti i prati postupanje po toj proceni;
- sarađuje sa Poverenikom, predstavlja kontakt tačku za saradnju sa Poverenikom i savetuje se sa njim u vezi sa pitanjima koja se odnose na obradu, uključujući i obaveštavanje i pribavljanje mišljenja.

EVIDENCIJE RADNJI OBRADE

Zakon propisuje obavezu vođenja evidencije obrade koja se odnosi na rukovaoce i obrađivače. Ova evidencija mora da sadrži podatke koji su kumulativno nabrojani u članu 47 Zakona, kao što su podaci o rukovaocu i obrađivaču, svrsi i vrsti obrade, vrsti lica na koja se podaci odnose, vrsti podataka, prenosu podataka, itd. Evidencije se vode u pisanom i/ili u elektronskom obliku i čuvaju se trajno.

Dodatno, obaveza vođenja evidencija se ne odnosi na privredne subjekte i organizacije u kojima je zaposleno manje od 250 lica, osim u slučajevima kada:

- obrada može da prouzrokuje visok rizik po prava i slobode lica na koje se podaci odnose;
- obrada nije povremena;
- obrada obuhvata posebne vrste podataka o ličnosti ili podatke koji se odnose na krivične presude, kažnjiva dela i mere bezbednosti.

Bez obzira što je izuzetak od ove obaveze široko postavljen, rukovaoci i obrađivači bi trebalo da vode evidencije obrade podataka, jer će na taj način razumeti koje sve podatke imaju u svom posedu i moći će lakše da se prilagode novim pravilima. Takođe, evidencije radnji obrade su vrlo pogodne za rukovaoce kao sredstvo pomoću kog mogu da predoče, odnosno dokazuju svoju usaglašenost sa Zakonom, a u skladu sa principom odgovornosti.

Zakon o zaštiti podataka o ličnosti ne predviđa obavezu formalnog prijavljivanja evidencija kod Poverenika ili nekog drugog organa, već samo obavezu organizacija da ih vode interno i daju ih na uvid nadležnom organu kada se to od njih zatraži.

EVIDENCIJA RUKOVAOCA

Zakon iscrpno popisuje informacije koje mora da sadrži evidencija obrade za koju je odgovoran rukovalac, odnosno njegov predstavnik. Takva evidencija, između ostalog, mora da sadrži informacije o imenu i kontakt podacima rukovaoca, zajedničkih rukovaoca, predstavnika rukovaoca, svrsi obrade, vrsti podataka o ličnosti i slično.

EVIDENCIJA OBRAĐIVAČA

Zakonska obaveza u pogledu vođenja evidencija obrade koja se odnosi na obrađivača i njegovog predstavnika vrlo je slična obavezi rukovaoca, te Zakon navodi da evidencija mora sadržati informacije o imenu i kontakt podacima svakog obrađivača i svakog rukovaoca u čije ime se obrada vrši, odnosno predstavnika rukovaoca ili obrađivača i lica za zaštitu podataka o ličnosti, vrsti obrada koje se vrše u ime svakog rukovaoca, prenosu podataka o ličnosti u druge države ili međunarodne organizacije, itd.

PROCENA UTICAJA NA ZAŠTITU PODATAKA

Poučen evropskom regulativom, ZZPL u nacionalno zakonodavstvo uvodi obavezu procene uticaja na zaštitu podataka o ličnosti. To je proces koji za cilj ima da pomogne rukovaocima da lakše identifikuju i umanje rizike koje obrada podataka o ličnosti nosi sa sobom, a u pogledu prava i sloboda lica na koje se ti podaci odnose.

Pošto uvede obavezu procene uticaja na zaštitu podataka o ličnosti, Zakon nalaže rukovaocu da pre započinjanja obrade izvrši procenu uticaja radnji obrade na zaštitu podataka o ličnosti, ukoliko je verovatno da će neka vrsta obrade, posebno upotrebom novih tehnologija i uzimajući u obzir prirodu, obim, okolnosti i svrhu obrade, prouzrokovati visok rizik za prava i slobode fizičkih lica. Zakon takođe predviđa mogućnost zajedničke procene uticaja, ali samo ukoliko više sličnih radnji obradi može prouzrokovati slične visoke rizike za zaštitu podataka o ličnosti, te propisuje obavezu konsultovanja lica za zaštitu podataka o ličnosti prilikom procene, ukoliko je takvo lice određeno.

Zakonom su takođe definisane prilike kada je neophodno izvršiti procenu uticaja, a to su:

- sistematske i sveobuhvatne procene stanja i osobina fizičkog lica koja se vrši pomoću automatizovane obrade podataka o ličnosti, uključujući i profilisanje, na osnovu koje se donose odluke od značaja za pravni položaj pojedinca ili na sličan način značajno utiču na njega;
- obrade posebnih vrsta podataka o ličnosti ili podataka o ličnosti u vezi sa krivičnim presudama i kažnjivim delima, u velikom obimu;
- sistematskog nadzora nad javno dostupnim površinama u velikoj meri.

Dodatno, Zakon navodi i da procena uticaja, između ostalog, mora da sadrži sveobuhvatan opis predviđenih radnji obrade, svrhu obrade, opis legitimnog interesa rukovaoca ako postoji, procenu rizika za prava i slobode lica na koje se podaci odnose i slično.

Smernice

Radna grupa 29 navodi više kriterijuma koji se moraju uzeti u obzir prilikom odlučivanja da li je neophodno izvršiti procenu uticaja:

1. Evaluacija ili bodovanje, uključujući profilisanje i predviđanje, posebno iz ugla koji se tiče učinka lica na koje se podaci odnose na poslu, ekonomsku situaciju, zdravlje, lične preferencije ili interesovanja, ponašanja, lokacije ili kretanja (npr. provera lica u kreditnom birou, institucijama koje se bave sprečavanjem pranja novca).
2. Automatizovano donošenje odluke sa pravnim ili sličnim značajnim uticajem na fizička lica (npr. obrada može dovesti do diskriminacije pojedinaca).
3. Sistematsko nadgledanje, obrada koja se koristi za posmatranje, nadgledanje ili kontrolu lica. Ovaj kriterijum se mora uzeti u obzir jer lični podaci lica mogu biti prikupljeni bez njihovog znanja, a posebno kada lica na koja se podaci odnose ne mogu da izbegnu da budu predmet takve obrade.
4. Obrada u velikom obimu mora uzeti u obzir sledeće kriterijume: broj lica na koje se obrada odnosi, obim i/ili opseg različitih podataka koji se obrađuju.
5. Usklađivanje ili kombinovanje skupova podataka koji potiču od dva ili više procesa obrade podataka koje se obavljaju u različite svrhe i/ili od strane različitih rukovalaca i to na način koji bi premašio razumna očekivanja lica na koja se podaci odnose.
6. Obrada podataka ranjivih lica kod kojih postoji značajan disbalans moći između njih i rukovaoca podataka, odnosno lica čiji su podaci predmet

obrade neće moći lako da prihvate ili se suprostave obradi (npr. deca, zaposleni, lica sa posebnim potrebama, starija lica).

7. Upotreba inovativnih tehnologija ili organizacionih rešenja, kao što je kombinovanje otisaka prstiju sa prepoznavanjem lica za naprednu kontrolu fizičkog pristupa.[55]

Dileme

Da li je neophodno izvršiti ponovnu procenu uticaja kada novi Zakon stupi na snagu?

Radna grupa 29 smatra da nije neophodno izvršiti novu procenu uticaja u situacijama kada je operacije obrade proverio, odnosno odobrio nadležni organ za zaštitu podataka o ličnosti pre stupanja na snagu novog propisa, pri čemu je imperativ da se specifični uslovi obrade nisu promenili. Na osnovu ovakvog mišljenja, može se zaključiti da je procenu uticaja neophodno ponovo izvršiti za svaku obradu čiji su se uslovi implementacije promenili od prethodne provere.[56]

55 Radna grupa 29, 2017, Smernice za procenu uticaja na zaštitu podataka, str. 9-11, dostupno na: ec.europa.eu

56 Ibid., str. 13

PRENOS PODATAKA

PRENOS PODATAKA

Izvoz podataka van određene teritorije odnosi se na svaki oblik prenosa, bez obzira da li su podaci zabeleženi na papiru ili u elektronskom obliku i da li se šalju običnom ili e-poštom. ZZPL reguliše pravila koja rukovaoci i obrađivači moraju da poštuju kada se podaci izvoze iz Srbije, dok GDPR reguliše pravila izvoza van granica Evropske unije. S obzirom na to da je u savremenom digitalnom okruženju više izuzetak nego pravilo da se podaci obrađuju na teritoriji samo jedne zemlje, značaj ovih pravila je jasan, iako na prvi pogled možda nije očigledan. Mnoge kompanije koje, na primer, pružaju *hosting* i *cloud* usluge imaju svoje servere van Evrope. Štaviše, podaci u okviru jednog procesa obrade često "putuju" kroz više jurisdikcija, zbog čega su za srpske rukovaoce bitna pravila i ZZPL-a i GDPR-a.

OPŠTE PRAVILO ZA PRENOS PODATAKA

Prema pravilima domaćeg Zakona, svaki prenos podataka o ličnosti čija je obrada u toku ili su namenjeni daljoj obradi posle njihovog prenošenja iz Srbije u drugu državu ili međunarodnu organizaciju, može se izvršiti samo ako rukovalac i obrađivač postupaju u skladu sa propisanim uslovima. Ovi uslovi treba da obezbede da se i nakon prenosa podataka sačuva primereni nivo zaštite podataka fizičkih lica koji je jednak nivou garantovanom Zakonom. Takođe, rukovaoci i obrađivači koji žele da izvoze lične podatke to mogu učiniti samo ako za taj izvoz imaju obezbeđen odgovarajući pravni osnov. ZZPL predviđa više mogućnosti, odnosno više situacija u kojima postoji pravni osnov za zakoniti prenos podataka.

PRENOS NA OSNOVU PRIMERENOG NIVOA ZAŠTITE

Univerzalni pravni osnov primenjiv na sve rukovaoce i obrađivače jeste izvoz u sve zemlje (ili manje teritorije u okviru zemlje) u kojima postoji primereni nivo zaštite. Sa stanovišta ZZPL, smatra se da primereni nivo zaštite postoji u državama i međunarodnim organizacijama koje su članice Konvencije Saveta Evrope o zaštiti lica u odnosu na automatsku obradu ličnih podataka, u državama ili međunarodnim organizacijama za koje je Evropska unija utvrdila da obezbeđuju primereni nivo zaštite, odnosno sa kojima je Srbija zaključila međunarodni sporazum o prenosu podataka o ličnosti. Praktično, ovog trenutka je izvoz podataka iz Srbije dozvoljen u sve zemlje Evropske unije, kao i u ostale zemlje koje su potpisnice Konvencije Saveta Evrope, ali i sve zemlje u koje je izvoz iz Evropske unije dozvoljen u skladu sa "odlukama o adekvatnosti" Evropske komisije. To su za sada Andora, Argentina, Džerzi, Farska ostrva, Gernzi, Izrael, Japan, Kanada (komercijalne organizacije), Novi Zeland, Ostrvo Man, Sjedinjene Američke Države (ograničeno na sporazum o "štitu privatnosti" između EU i SAD), Švajcarska i Urugvaj.[57]

Što se tiče izvoza ličnih podataka u Sjedinjene Američke Države, prenos u tu zemlju nije potpuno slobodan. Naime, prema uslovima "štita privatnosti" nisu sve američke kompanije automatski podobne da budu uvoznici - već kompanije koje žele da budu uključene na listu bezbednih primalaca podataka iz EU moraju da ispune posebne uslove i da se u tu svrhu prijave nadležnom organu u svojoj zemlji (na dobrovoljnoj bazi). Ideja je da se kroz ovaj mehanizam proveri i obezbedi da će ti primaoci podataka zasta osigurati ade-

57 Prema navodima Evropske komisije, trenutno su u toku pregovori sa Južnom Korejom, videti na: ec.europa.eu

kvatan nivo zaštite za podatke koje uvezu. Stoga je odgovor na pitanje koje su kompanije prošle ovu proveru i smatraju se adekvatnim prema uslovima "štita privatnosti" donekle dinamičan, te se preporučuje da se pre prenosa podataka na odgovarajućem vebsajtu proveri status potencijalnog uvoznika.[58]

ZZPL predviđa pravilo da se lista teritorija za koje se smatra da obezbeđuju primereni nivo zaštite, odnosno za koje je Vlada Srbije utvrdila da ne obezbeđuju primereni nivo zaštite, objavljuje u Službenom glasniku.

Dakle, ako podatke izvoze na teritorije sa primerenim nivoom zaštite, rukovaoci i obrađivači ne moraju da preduzimaju nikakve dodatne korake - smatra se da je primeren nivo zaštite već ustanovljen u odnosu na celu teritoriju gde se uvoze podaci.

PRENOS UZ PRIMENU ODGOVARAJUĆIH MERA ZAŠTITE

U ovom slučaju, sami rukovaoci ili obrađivači obezbeđuju da su primalac, odnosno uvoznik podataka primenili odgovarajuće mere zaštite.

Rukovalac ili obrađivač obezbeđuju ostvarivost prava i pravnu zaštitu licu na koje se odnose podaci, bez posebnog odobrenja Poverenika, na jedan od sledećih načina koje predviđa ZZPL:

- pravno obavezujućim aktom sačinjenim između organa vlasti;
- standardnim ugovornim klauzulama koje izrađuje Poverenik (a koje se ne smeju menjati da bi mogle da služe kao pravni osnov za prenos);
- obavezujućim poslovnim pravilima;
- odobrenim kodeksom postupanja;
- izdatim sertifikatima koje reguliše ZZPL.

Takođe, ukoliko nijedan od ovih mehanizama nije primenjiv u konkretnoj situaciji, rukovaoci i obrađivači mogu obezbediti odgovarajuće mere zaštite i na osnovu posebnog odobrenja Poverenika za konkretan slučaj, i to: (1) ugovornim odredbama koje je odobrio Poverenik; ili (2) odredbama koje se unose u sporazum između organa vlasti, a kojima se obezbeđuje delotvorna i sprovodiva zaštita prava lica na koje se podaci odnose.

PRENOS PODATAKA U POSEBNIM SITUACIJAMA

Zakon izričito popisuje specifične situacije u kojima je prenos dozvoljen ako nije moguće primeniti nijedan od mehanizama za primenu odgovarajućih mera zaštite. To su prilike u kojima je: (1) lice na koje se podaci odnose izričito pristalo na izvoz, nakon što je informisano o mogućim rizicima vezanim za izvoz podataka zbog nepostojanja primerenog nivoa zaštite, odnosno odgovarajućih mera zaštite; (2) prenos neophodan za izvršenje ugovora između lica na koje se podaci odnose i rukovaoca, ili za primenu predugovornih mera preduzetih na zahtev lica na koje se podaci odnose; (3) izvoz neophodan za zaključenje ili izvršenje ugovora zaključenog u interesu lica na koje se podaci odnose; (4) izvoz neophodan za podnošenje, ostvarivanje ili odbranu pravnog zahteva.

Praksa

Odgovornost za neovlašćeni izvoz može biti višestruka, a može se utvrđivati u prekršajnom, parničnom i krivičnom postupku. Prema raspoloživoj sudskoj praksi, izvoz podataka van Srbije bez odgovarajućeg pravnog osnova sudovi su kvalifikovali kao radnju neovlašćenog prikupljanja ličnih podataka, iz člana 146 Krivičnog zakonika.

58 Proveru je moguće uraditi na: privacyshield.gov

Dileme

Koji je optimalan pravni osnov za izvoz podataka?

Sa stanovišta prava, ovo pitanje se rešava od slučaja do slučaja. Valja naglasiti da su odredbe Zakona kojima je regulisan prenos podataka, kao i većina ostalih odredbi, preuzete iz GDPR-a koji reguliše izvoz iz Evropske unije. Evropski rukovaoci koji izvoze podatke se u najvećoj meri oslanjaju na standardne ugovorne klauzule koje je izradila Evropska komisija. Standardne klauzule Evropske komisije postoje u više varijanti, a ugovorne strane biraju onaj tip koji najviše odgovara njihovoj situaciji. Kada odaberu tip klauzula, ugovorne strane mogu samo da popune nedostajuće podatke, a pritom ne smeju da promene nijednu od sadržanih odredbi. Pretpostavka je da je sama Evropska komisija tim klauzulama predvidela odgovarajuće mere zaštite, te ugovorne strane nemaju mogućnost da te mere menjaju ako hoće da se koriste ovim mehanizmom za prenos.

U Srbiji nadležnost za izradu standardnih ugovornih klauzula ima Poverenik. Sve dok ih Poverenik ne izradi, rukovaoci i obrađivači su uskraćeni za korišćenje ovog najpopularnijeg pravnog osnova za izvoz podataka. To je posebna prepreka za organizacije koje podatke izvoze u Sjedinjene Američke Države jer, za razliku od država članica EU, SAD ne spadaju u teritorije gde je izvoz unapred dozvoljen.

NOVI INSTITUTI

NOVI INSTITUTI

Za razliku od starog Zakona o zaštiti podataka o ličnosti, novi Zakon uvodi nekoliko novih instituta samoregulacije po ugledu na GDPR i to: mogućnost izrade kodeksa postupanja, mogućnost sertifikacije (izdavanje sertifikata o zaštiti podataka o ličnosti), kao i primenu tzv. obavezujućih poslovnih pravila. Imajući u vidu da su ovo potpuno novi pravni instituti, praksa Poverenika i ostalih aktera u vezi sa njima će se tek razvijati u budućnosti, a naša je pretpostavka da će na tu praksu uticati i smernice i stavovi EDPB-a i uporedna praksa EU zemalja.

KODEKS POSTUPANJA

ZZPL uvodi mogućnost izrade *kodeksa postupanja* kako bi udruženja i drugi subjekti koji predstavljaju grupe rukovalaca ili obrađivača, efikasnije primenjivali propis. Institut kodeksa uzima u obzir specifičnosti obrade podataka u odgovarajućim sektorima industrije i konkretne potrebe malih i srednjih kompanija. Kodeksi bi trebalo da bliže regulišu principe poštene i transparentne obrade, da podrobnije objasne legitimni interes rukovaoca kao pravni osnov obrade u konkretnom slučaju, dodatno regulišu prikupljanje i pseudonimizaciju podataka o ličnosti, način na koji se ostvaruju prava lica na koje se podaci odnose, prenos podataka u druge države i međunarodne organizacije, način rešavanja sporova između rukovaoca i lica na koje se podaci odnose mirnim putem, bliže opišu međusobne obaveze rukovaoca i obrađivača, itd.

Budući da je izrada kodeksa postupanja samo mogućnost, a ne obaveza, ZZPL utvrđuje obavezu Poverenika da podstiče i promoviše izradu ovakvih kodeksa. Usvajanje kodeksa je korisno ne samo da bliže odgovori potrebama konkretnih rukovalaca i obrađivača, već i da se lakše demonstrira usklađenost tih rukovalaca i obrađivača sa Zakonom.

Potencijalni problem može nastati prilikom određivanja subjekata koji mogu da izrade kodeks postupanja. Prema Zakonu, to su udruženja i drugi subjekti koji predstavljaju grupe rukovalaca ili obrađivača, što navodi na pomisao da kodeks može izraditi i jedno udruženje kao zasebno pravno lice osnovano u skladu sa Zakonom o udruženjima. Budući da je ovaj deo ZZPL-a donet po ugledu na GDPR, potrebno je imati u vidu da se u GDPR-u koristi engleska reč "associations", koja ipak ima drugačije značenje od reči "udruženje" u našem pravnom sistemu.

Smatramo da je intencija GDPR-a da se pod *udruženja* podvede *više različitih entiteta* koji su udruženi po nekom zajedničkom osnovu. Stoga bi se moglo zaključiti i da je namera domaćeg zakonodavca ista - da se kodeks odnosi na samoregulisanje ponašanja više entiteta koje povezuju određene zajedničke okolnosti, a ne samo jednog udruženja. Ostaje da se vidi da li će udruženja, kao nezavisna i zasebna pravna lica, samostalno u praksi donositi ovakve kodekse postupanja da regulišu sama sebe.

Kodeks postupanja mora sadržati odredbe koje omogućavaju akreditovanom pravnom licu vršenje nadzora nad primenom kodeksa rukovalaca i obrađivača koji su se obavezali da ga primenjuju.

Da bi se izradio ili izmenio kodeks postupanja, predlog kodeksa ili njegovih izmena se dostavlja Povereniku na mišljenje i saglasnost. Poverenik je ovlašćen i da podstiče izradu ovakvog kodeksa, a ukoliko smatra da je kodeks u skladu sa Zakonom i sadrži dovoljne garancije za zaštitu podataka o ličnosti, kodeks postupanja odnosno njegove izmene će biti registrovane i javno objavljene na internet stranici Poverenika.

ZZPL predviđa da kontrolu primene kodeksa vrši "pravno lice koje je akreditovano za vršenje kontrole u skladu sa za-

konom koji uređuje akreditaciju". Pritom, kontrola takvog akreditovanog lica ne utiče na mogućnost kontrole i inspekcijskih ovlašćenja koje ima Poverenik u vezi sa kodeksom postupanja (podsticanje izrade kodeksa i davanje mišljenja i saglasnosti na kodeks).

Zakon predviđa koje uslove pravno lice mora da ispunjava da bi bilo akreditovano, ali ostaje nejasno ko su pravna lica koja će se baviti kontrolom primene kodeksa ukoliko mogućnost izrade kodeksa zaživi u praksi (budući da je izrada kodeksa samo mogućnost, a ne i obaveza). Jedan od uslova da pravno lice bude akreditovano jeste i da "dokaže Povereniku svoju nezavisnost i stručnost u odnosu na sadržinu kodeksa", a pritom se ne određuje bliže na koji način se takva nezavisnost i stručnost dokazuju.

U slučaju da rukovalac ili obrađivač povrede kodeks postupanja, akreditovano pravno lice može, između ostalih mera, privremeno ili trajno isključiti rukovaoca odnosno obrađivača iz primene kodeksa, a dužno je da o preduzetim merama obavesti Poverenika. Mere koje je akreditovano pravno lice preduzelo ne utiču na ovlašćenja Poverenika, niti na pravo lica na koje se podaci odnose da podnese pritužbu Povereniku ili zatraži sudsku zaštitu.

SERTIFIKACIJA

ZZPL uvodi mogućnost ustanovljavanja postupka za izdavanje sertifikata o zaštiti podataka o ličnosti, u cilju dokazivanja da rukovalac i obrađivač poštuju odredbe Zakona, posebno uzimajući u obzir potrebe malih i srednjih kompanija. Smisao izdavanja sertifikata je, dakle, lakše dokazivanje da je rukovalac, odnosno obrađivač, implementirao ZZPL u svoje poslovanje i da ga se pridržava, ali samo izdavanje sertifikata ne utiče na prava i obaveze koje rukovaoci i obrađivači imaju u skladu sa Zakonom, niti utiče na inspekcijska i druga ovlašćenja Poverenika. Međutim, posedovanje sertifikata olakšava rukovaocu da demonstrira usklađenost sa Zakonom i, na kraju krajeva, može da dovede do konkurentske prednosti na tržištu jer povoljno utiče na reputaciju rukovaoca kao tržišnog učesnika.

Slično kao i sa kodeksom postupanja, Poverenik ima nadležnost da podstiče izdavanje sertifikata za zaštitu podataka o ličnosti, budući da se radi o procesu koji je dobrovoljan. Poverenik propisuje kriterijume za sertifikaciju, proverava ispunjenost uslova za sertifikaciju i sprovodi periodično preispitivanje izdatih sertifikata. Kriterijumi Poverenika za sertifikaciju, dakle, tek treba da budu razvijeni u praksi.

Smernice

Prema Smernicama 1/2018 o sertifikaciji i sertifikacionim kriterijumima EDPB-a od 23.01.2019. godine, kriterijumi moraju biti takvi da odražavaju zahteve i principe zaštite lica u odnosu na obradu njihovih ličnih podataka, kao i da doprinesu konzistentnoj primeni GDPR-a.[59] Prilikom izrade kriterijuma sertifikacije, na snazi su neki opšti principi: kriterijumi treba da budu uniformni i podložni verifikaciji i kontroli, treba da uzmu u obzir okolnosti slučaja i na koga se oni odnose (da li se, na primer, odnose na dve kompanije koje sarađuju ili na kompaniju i njenog klijenta), treba da budu fleksibilni tako da se mogu primeniti na različite tipove organizacija uključujući mikro, mala i srednja preduzeća, itd.

Sertifikate izdaje ili Poverenik, ili tzv. sertifikaciono telo, na osnovu kriterijuma koje propisuje Poverenik. Kako takvi kriterijumi još uvek nisu usvojeni, ostaje da se vidi koje sve uslove jedan rukovalac, odnosno obrađivač mora da ispuni da bi mu se sertifikat izdao, kao i koja je njegova motivacija da se upusti u postupak sertifikacije. Naime, sertifikacija

59 EDPB, 2019, Smernice 1/2018 za sertifikaciju i sertifikacione kriterijume u skladu sa članovima 42 i 43 Uredbe 2016/679, dostupno na: edpb.europa.eu

može pomoći rukovaocu, odnosno obrađivaču, da u postupku kontrole lakše dokaže usklađenost sa Zakonom i pozitivno uticati na njegovu reputaciju. S druge strane, posedovanje sertifikata ne utiče na propisana prava i obaveze rukovalaca u vezi sa obradom podataka o ličnosti. Drugim rečima, posedovanje sertifikata ne znači automatsku usklađenost sa Zakonom, ali može da se iskoristi za dokazivanje usklađenosti. Jednom izdati sertifikat može isteći ili biti oduzet, tako da entitet koji je pribavio sertifikat i dalje mora da vodi računa da, prilikom obrade podataka, postupa u skladu sa ZZPL-om.

Sertifikat se izdaje na period od najviše tri godine, a može se i obnoviti pod uslovom da imalac sertifikata i dalje ispunjava kriterijume za njegovo izdavanje. Poverenik ili sertifikaciono telo mogu ukinuti sertifikat ukoliko se utvrdi da imalac sertifikata više ne ispunjava potrebne kriterijume. Poverenik vodi i objavljuje spisak sertifikacionih tela i izdatih sertifikata na svojoj internet stranici.

Slično kao i kod akreditovanog pravnog lica za kodeks postupanja, ZZPL predviđa postojanje sertifikacionog tela koje, pored Poverenika, ima pravo da izdaje sertifikate. Poverenik propisuje i objavljuje kriterijume za akreditaciju sertifikacionog tela, ali ostaje da se vidi na koji način će ova tela funkcionisati u praksi, te da li će se rukovaoci i obrađivači odlučivati da izdavanje sertifikata zatraže od sertifikacionih tela ili od Poverenika.

OBAVEZUJUĆA POSLOVNA PRAVILA

Interna pravila o zaštiti podataka o ličnosti Zakon smatra obavezujućim poslovnim pravilima. Njih usvaja i primenjuje rukovalac, odnosno obrađivač sa prebivalištem ili boravištem, odnosno sedištem na teritoriji Republike Srbije, u svrhu regulisanja prenošenja podataka o ličnosti rukovaocu ili obrađivaču u jednoj ili više država unutar multinacionalne kompanije ili grupe privrednih subjekata.

Dakle, obavezujuća poslovna pravila odnose se na prenos podataka unutar multinacionalnih kompanija. Ovo praktično znači da više kompanija koje pripadaju jednoj grupi i imaju jednog krajnjeg vlasnika u više različitih država (korporativne grupe) mogu da ustanove svoja interna pravila o zaštiti podataka o ličnosti u cilju regulisanja transfera podataka rukovaocu ili obrađivaču van teritorije Srbije, ali unutar iste korporativne grupe i na taj način regulišu transfer podataka o ličnosti bez primene komplikovanih pravila za transfer podataka koje propisuje ZZPL.

Obavezujuća poslovna pravila odobrava Poverenik, ukoliko takva pravila ispunjavaju sledeće uslove:

- pravno su obavezujuća, primenjuje ih i sprovodi svaki član multinacionalne kompanije ili grupe privrednih subjekata, uključujući i njihove zaposlene;
- izričito obezbeđuju ostvarivanje prava lica na koje se podaci odnose u vezi sa obradom njihovih podataka;
- definišu strukturu, kontakt podatke multinacionalne kompanije ili grupe privrednih subjekata; prenos podataka o ličnosti, vrste podataka o ličnosti, radnje obrade, svrhu, lica na koja se podaci odnose i naziv države u koju se prenose; propisuju obaveznost sopstvene primene; određuju primenu opštih načela zaštite podataka o ličnosti i prava lica na koje se podaci odnose, kao i načine ostvarivanja takvih prava; definišu prihvatanje odgovornosti rukovaoca, odnosno obrađivača na teritoriji Republike Srbije za povredu pravila koju je učinio drugi član korporativne grupe sa sedištem, prebivalištem, odnosno boravištem van Srbije, osim ukoliko rukovalac ili obrađivač dokaže da taj drugi član grupe nije odgvoran za događaj koji je prouzrokovao štetu; ovlašćenja lica za zaštitu podataka o ličnosti; postupak po pritužbama; način saradnje sa Poverenikom, itd.

Ukoliko obavezujuća poslovna pravila ispunjavaju zakonske uslove, Poverenik ih odobrava u roku od 60 dana od dana podnošenja zahteva za njihovo odobrenje. Međutim, budući da se po prirodi stvari ovde radi o multinacionalnoj grupi kompanija, ostaje da se vidi na koji način će obavezujuća poslovna pravila koje je odobrio srpski Poverenik primeniti (a možda i dalje verifikovati) organi nadležni za zaštitu podataka o ličnosti u zemljama u kojima druge povezane kompanije iste korporativne grupe imaju sedište. Takođe se postavlja pitanje šta se dešava u situaciji da srpska kompanija, koja je deo multinacionalne korporativne grupe, nije usvojila obavezujuća poslovna pravila, već je to učinjeno u državi neke druge kompanije-članice korporativne grupe. Po slovu Zakona, Poverenik bi morao da odobri i takva obavezujuća poslovna pravila, iako je njih možda već odobrio nadležni organ druge države.

PRAVA LICA NA KOJE SE PODACI ODNOSE

PRAVA LICA NA KOJE SE PODACI ODNOSE

Po uzoru na GDPR, Zakon određuje čitav niz prava koja imaju lica čiji se podaci obrađuju, pri čemu je obaveza rukovaoca da obezbedi njihovu primenu. Ukoliko rukovalac ne postupa u skladu sa ovim pravima, ili ne ogovara na zakonit način na zahteve za njihovo ostvarivanje, tim licima je na raspolaganju niz pravnih sredstava i lekova. U prvom redu, to su pravo na žalbu Povereniku i pravo na tužbu sudu.

Ostvarivanje prava u praksi može da dovede do promene čitavih biznis modela pojedinih rukovalaca, posebno onih koji su poslovanje razvili u složenoj industriji podataka. U cilju ostvarivanja prava, fizička lica koja koriste pravna sredstva koja su im na raspolaganju direktno učestvuju u formiranju određenih pravnih standarda. Na primer, od osećanja i stavova fizičkih lica u vezi sa njihovim interesima i slobodama, direktno može zavisiti mogućnost rukovaoca da se u obradi podataka osloni na svoj legitimni interes.

Što se tiče obrađivača, oni su u obavezi da asistiraju rukovaocu u ostvarivanju prava putem implementacije odgovarajućih tehničkih i organizacionih mera, resursa i sredstava, u meri u kojoj su te aktivnosti u njihovoj kontroli.

OSTVARIVANJE PRAVA I TRANSPARENTNOST

Postupak i rokovi ostvarivanja svih prava regulisani su odredbama Zakona i oni su u principu isti bez obzira na vrstu zahteva za ostvarivanje prava. Kako bi ovaj postupak išao glatko i bio završen u predviđenim rokovima, preporuka za rukovaoce je da unapred imaju spremna interna pravila i procedure po kojima postupaju njihovi zaposleni kada pristigne zahtev za ostvarivanje nekog od prava.

Rukovalac je dužan da licu na koje se podaci odnose pruži sve propisane informacije na sažet, transparentan, razumljiv i lako dostupan način, korišćenjem jasnih i jednostavnih reči, a posebno ako se radi o informaciji koja je namenjena detetu. Oblik i način u kom će informacije biti pružene zavise od konkretnih okolnosti. ZZPL u tom smislu nije isključiv, već pominje pisani i elektronski oblik, ali i mogućnost da se informacije pruže usmeno (pod uslovom da je identitet lica nesumnjivo utvrđen). Međutim, pravilo je da se informacija mora pružiti elektronskim putem (ako je to moguće) onda kada je lice na taj način i podnelo zahtev, osim ako podnosilac traži da se informacija pruži na drugi način.

Što se tiče rokova, rukovalac je dužan da podnosiocu pruži informacije o postupanju na osnovu njegovog zahteva najkasnije u roku od 30 dana od dana prijema zahteva. Taj rok može biti produžen za još 60 dana ako je to neophodno. U slučaju da rukovalac ne postupi po zahtevu, dužan je da o razlozima za nepostupanje obavesti podnosioca najkasnije u roku od 30 dana od dana prijema zahteva, kao i o pravu na podnošenje pritužbe Povereniku, odnosno tužbe sudu.

U principu, rukovalac pruža informacije bez naknade. Ukoliko su zahtevi nekog lica šikanozni i očigledno neosnovani, pogotovo ako se ponavljaju, rukovalac ima pravo da ih odbije ili da naplati obradu (teret dokaza je na rukovaocu).

PRAVO NA INFORMISANJE

Pravo na informisanje je svojevrsni derivat načela transparentnosti. ZZPL jasno reguliše koje sve informacije licu moraju biti date pre nego što uopšte započne obrada, bez obzira na to da li je lice zahtevalo te informacije. Spisak obaveznih informacija nalazi se u članovima 22 i 23 Zakona. Ukoliko se podaci o ličnosti prikupljaju direktno od lica na koje se odnose, ovaj spisak obuhvata identitet i kontakt podatke rukovaoca, svrhu obrade i pravni osnov za obradu, primaoce podataka, izvoz podataka, rok čuvanja ili kriterijume za njegovo određivanje, postojanje svih prava lica na koje se podaci odnose i prava da se podnese pritužba Povereniku, postojanje automatizovanog donošenja odluke, itd. Ako se prikupljaju od trećeg lica, spisku su dodate informacije o licu od kog su dobijeni podaci, o vrsti podataka koji se obrađuju, itd.

U praksi, rukovaoci usvajaju politike privatnosti u kojima su u velikoj meri sadržane informacije koje zahteva ZZPL, što svakako doprinosi ostvarivanju prava na informisanost.[60] Međutim, ukoliko je broj obrada ličnih podataka kod rukovaoca veliki, teško je zamislivo da politike privatnosti mogu obuhvatiti sve što je potrebno. Stoga rukovaoci moraju voditi računa da u odgovarajućim okolnostima dostave licima minimum zahtevanih informacija na drugi primeren način (elektronski ili u papirnom obliku).

Smernice

Radna grupa 29 izdala je smernice u kojima su date detaljne preporuke rukovaocima oko pitanja o kojima treba da vode računa kada postupaju u cilju ispunjenja prava na informisanje.[61] Jedno od kompleksnih tema u tom smislu je svakako određivanje prave mere između zahteva da informacije o relevantnoj obradi treba da s jedne strane budu potpune (dakle da se ništa od važnih informacija ne sakrije) ali i da, s druge strane, te informacije budu date na jasan i sažet način (umesto dosadašnje prakse pisanja dugih i nerazumljivih politika privatnosti). Predlog razrešenja ove tenzije jeste "slojevit pristup". On podrazumeva da se u prvom sloju daju zbirne informacije o glavnim pitanjima obrade kao što su svrha obrade, identitet rukovaoca i prava nosilaca podataka, a da se u drugom sloju nosiocu podataka omogući da detaljnije pročita o pojedinom segmentu obrade koji ga posebno zanima. Tehničko rešenje ovakvog pristupa opet treba da bude jasno i intuitivno za korisnike (*user friendly*) a ne napravljeno da bi korisnike dovodilo u zabludu i otežavalo im dolazak do željene informacije.

PRAVO NA PRISTUP

Pravo na pristup podacima (ili pravo na uvid u podatke) najpre podrazumeva da lice ima pravo da od rukovaoca traži potvrdu o tome da li rukovalac uopšte obrađuje njegove podatke. Ako je odgovor pozitivan, lice ima pravo da dobije pristup tim podacima, kao i pravo da dobije određene informacije u vezi sa njihovom obradom koje se, u velikoj meri, poklapaju sa informacijama koje rukovalac i bez posebnog zahteva mora da obelodani pre započinjanja obrade u okviru poštovanja prava na informisanost.

Takođe, komponenta ovog prava je i pravo na kopiju. Rukovalac je dužan da licu na njegov zahtev dostavi kopiju podataka koje obrađuje. U tom slučaju, rukovalac može da zahteva naknadu nužnih troškova za izradu dodatnih kopija, ako ti troškovi postoje. Rukovalac takođe treba da se postara da ostvarivanjem prava na dostavljanje kopije ne budu ugrožena pra-

60 SHARE Fondacija je pripremila besplatan alat koji rukovaocima može pomoći da izrade svoju politiku privatnosti u skladu sa novim pravilima zaštite podataka o ličnosti, dostupan na: gdpr.mojipodaci.rs

61 Radna grupa 29, 2018, Smernice za transparentnost prema Uredbi 2016/679, dostupno na: ec.europa.eu

va i slobode drugih lica (na primer, prava intelektualne svojine ili poslovna tajna).[62]

PRAVO NA ISPRAVKU I DOPUNU

Svako lice ima bezuslovno pravo na ispravku netačnih i dopunu nepotpunih podataka o ličnosti. Ovo pravo je naročito važno, jer kad se podaci o ličnosti građana jednom prikupe često se ne vodi računa o njihovoj ažurnosti, što može predstavljati veliki problem u praksi (na primer, prilikom razmene podataka između državnih organa, od kojih zavisi ostvarivanje nekih prava građana). Kako bi rukovalac mogao da efikasno ispuni zahtev za ostvarenje ovog prava, važno je da zna gde se sve u okviru njegovog poslovanja nalaze podaci o jednom licu.

PRAVO NA BRISANJE

Rukovalac je dužan da bez nepotrebnog odlaganja izbriše lične podatke po zahtevu lica u sledećim slučajevima:

- podaci više nisu neophodni za ostvarivanje svrhe zbog koje su obrađivani;
- lice je opozvalo pristanak na osnovu kojeg se obrada vršila, a nema drugog pravnog osnova za obradu;
- podnet je prigovor na obradu;
- podaci su nezakonito obrađivani;
- podaci moraju biti izbrisani u cilju izvršenja zakonskih obaveza rukovaoca;
- podaci su prikupljeni od deteta u vezi sa korišćenjem usluga informacionog društva.

Ako je rukovalac javno objavio podatke o ličnosti, njegova je obaveza i da preduzme sve razumne mere u skladu sa dostupnim tehnologijama u cilju obaveštavanja drugih rukovalaca koji te podatke obrađuju o zahtevu za brisanje svih kopija ovih podataka i upućivanja, odnosno elektronskih veza prema ovim podacima.

Postoje određeni izuzeci od ovog prava kada rukovalac ne mora da postupi po zahtevu, a koji uključuju slobodu govora, arhiviranje u javnom interesu, obradu u naučne i statističke svrhe, ostvarivanje ili odbranu od pravnih zahteva.

PRAVO NA OGRANIČENJE OBRADE

Situacije u kojima nosilac podataka može da ostvari ovo pravo su sledeće:

- ako osporava tačnost podataka, za vreme koje omogućava rukovaocu proveru tačnosti;
- obrada je nezakonita, ali se lice protivi brisanju i zahteva ograničenje upotrebe podataka;
- rukovaocu više nisu potrebni podaci, ali jesu nosiocu da bi ostvario neki pravni zahtev;
- podnet je prigovor na obradu, a u toku je procenjivanje da li pravni osnov rukovaoca preteže nad interesima tog lica.

Pošto obrada podrazumeva i brisanje podataka, treba naglasti da je obustavljanje obrade prekid gotovo svih aktivnosti u vezi sa ličnim podacima, uključujući i zabranu brisanja. Logično, u ovom slučaju jedina moguća aktivnost koja se ne sme prekinuti jeste čuvanje. Takođe, prema pravilima ZZPL, ako je rukovalac prihvatio zahtev i ograničio obradu, tada se podaci smeju obrađivati samo u jasno de-

62 SHARE Fondacija je 2016. godine sprovela istraživanje na temu obrade geolokacijskih podataka od strane operatora elektronskih komunikacija, sa predlogom kako korisnici ovih usluga mogu da od operatora dobiju kopiju ove vrste svojih podataka. Istraživanje je dostupno na: resursi.sharefoundation.info

finisanim situacijama: uz pristanak, za ostvarivanje pravnih zahteva, za zaštitu prava drugog fizičkog ili pravnog lica.

PRAVO NA PRENOSIVOST PODATAKA

Pravo na prenosivost je novo pravo u evropskom zakonodavstvu, sa ciljem da ojača kontrolu koju građani imaju nad svojim ličnim podacima, dok ga u naš pravni sistem uvodi ZZPL. Na izvestan način, to je proširenje prava pristupa, jer nalaže rukovaocu da na zahtev lica obezbedi lične podatke u strukturiranom, uobičajenom i mašinski čitljivom formatu, a lice ima pravo da ih prenese drugom rukovaocu, bez ometanja. Rukovalac mora da udovolji ovom pravu samo ako su zajedno ispunjeni sledeći uslovi: (1) obrada je zasnovana na pristanku ili na osnovu ugovora, i (2) obrada se vrši automatizovano. Od rukovaoca se takođe može zahtevati da prenese podatke direktno drugom rukovaocu, kada je takav postupak tehnički izvodljiv.

Ovo pravo posebno dobija na značaju u onlajn okruženju pružanja usluga, gde jedna osoba ima niz različitih naloga ili profila, od društvenih mreža, preko servisa za strimovanje sadržaja do aplikacija koje obrađuju osetljive podatke kao što su zdravstveni podaci (razne trening i fitnes aplikacije). U svim ovim slučajevima, koristeći pravo na prenosivost, lice bi imalo pravo da zahteva da se njegovi podaci prebace, na primer, na novu društvenu mrežu ili na konkurentsku platformu.

Kao i kod prava na kopiju podataka, ZZPL reguliše da ostvarivanje ovog prava ne može štetno uticati na ostvarivanje prava i sloboda drugih lica.

PRAVO NA PRIGOVOR

Pravo na prigovor zapravo testira legitimni interes ili javni interes kao pravni osnov za obradu, i ono nosicu podataka pruža mogućnost da takav osnov za obradu ospori. Kada primi ovakav zahtev, rukovalac je dužan da prekine sa obradom podataka, osim ako može da pokaže da postoje zakonski razlozi za obradu koji pretežu nad interesima, pravima ili slobodama lica ili su u vezi sa podnošenjem, ostvarivanjem ili odbranom pravnog zahteva. Da bi ovo pravo bilo efikasno, ZZPL zahteva od rukovaoca da najkasnije prilikom uspostavljanja prve komunikacije sa nosiocem podataka upozori to lice na postojanje ovog prava, na način koji je izričit, jasan i odvojen od svih drugih informacija koje mu pruža.

U slučaju prigovora direktnom marketingu, što uključuje profilisanje, rukovalac mora obustaviti obradu u tu svrhu čim primi prigovor. Dakle, rukovaoci koji šalju promotivne poruke mejlom ili SMS-om ili na drugi način kontaktiraju lica u cilju sprovođenja marketinških akcija, moraju da obezbede mehanizam potpunog prekida takve prakse čim neko lice uputi takav zahtev.

AUTOMATIZOVANO DONOŠENJE ODLUKA

Pošto se obrada ličnih podataka sve više vrši u digitalnom okruženju, nova evropska i domaća regulativa prepoznaje odgovornost i u situacijama kada ličnim podacima "rukuju" mašine, kao i komplementarna prava fizičkih lica. Automatizovano donošenje odluka odnosi se na situacije kada je odluka u potpunosti doneta bez ljudskog učešća. Automatski prikupljeni i obrađeni podaci koji se tiču neke konkretne osobe, njenih navika, sklonosti i ponašanja na internetu ("profilisanje") i dalje su podaci o ličnosti. Često su ti podaci i posebno osetljivi, pa zbog toga uživaju dodatnu zaštitu. Prava koja se tradicionalno vezuju za podatke o ličnosti

moraju biti na snazi i kada je reč o automatizovanoj obradi, uključujući informisani pristanak, uvid, izmenu ili brisanje, kao i sva temeljna načela obrade.

Posebna prava koja postoje u slučajevima automatizovane obrade omogućavaju licima da zadrže kontrolu nad svojim podacima ukoliko u njihovoj obradi učestvuju samo mašine i softveri. ZZPL najpre predviđa da lice na koje se podaci odnose ima pravo da se na njega ne primenjuje odluka doneta isključivo na osnovu automatizovane obrade, uključujući i profilisanje, ako se tom odlukom proizvode pravne posledice po to lice ili ta odluka značajno utiče na njegov položaj (osim ukoliko se primenjuju jasno definisani izuzeci). Pravne posledice moraju biti značajne, odnosno moraju uticati na neko temeljno pravo kao što su pravo na okupljanje i udruživanje, biračko pravo i slično. Takođe, u odluke sa pravnim posledicama treba uvrstiti i odluke koje mogu dovesti do raskida ugovora, uskraćivanja neke pomoći garantovane zakonom, kao i do odbijanja vize, ulaska u zemlju i slično. Odluke koje značajno mogu uticati na nečiji položaj su one koje imaju dugotrajne posledice, mogu dovesti do diskriminacije ili uticati na izbor i ponašanje pojedinca. Ovakve odluke mogu uticati na pristup zdravstvenoj zaštiti, procenu kreditne sposobnosti, radna prava ili pravo na obrazovanje.[63]

Takođe, rukovalac je dužan da primeni odgovarajuće mere zaštite prava, sloboda i legitimnih interesa lica. Minimum tih prava uključuje pravo da se obezbedi učešće fizičkog lica pod kontrolom rukovaoca u donošenju odluke, zatim pravo lica na koje se podaci odnose da izrazi svoj stav u vezi sa odlukom, i najzad pravo lica na koje se podaci odnose da ospori odluku pred ovlašćenim licem rukovaoca.

Automatizovane odluke se svakako ne mogu zasnivati na posebnim vrstama podataka o ličnosti, osim u izuzetnim situacijama predviđenim Zakonom.

OGRANIČENJE PRAVA

Po uzoru na GDPR, ZZPL sadrži pravila o tome pod kojim okolnostima neka od prava mogu da budu ograničena. Ovo je moguće samo ukoliko ograničenja ne zadiru u suštinu osnovnih prava i sloboda i ako to predstavlja neophodnu i srazmernu meru u demokratskom društvu za zaštitu (1) nacionalne bezbednosti, (2) odbrane, (3) javne bezbednosti, (4) sprečavanja, istrage i otkrivanja krivičnih dela, gonjenja učinilaca krivičnih dela, ili izvršenje krivičnih sankcija, uključujući sprečavanje i zaštitu od pretnji po javnu bezbednost, (5) drugih važnih opštih javnih interesa, (6) nezavisnosti pravosuđa i sudskih postupaka, (7) sprečavanja, istraživanja, otkrivanja i gonjenja za povredu profesionalne etike, (8) funkcije praćenja, nadzora ili vršenja regulatorne funkcije koja je stalno ili povremeno povezana sa vršenjem službenih ovlašćenja, (9) lica na koje se podaci odnose ili prava i sloboda drugih lica, (10) ostvarivanja potraživanja u građanskim stvarima.

Iako tekst ZZPL ne navodi eksplicitno da se ograničenja mogu uvoditi samo putem posebnih zakona, kao što to navodi član 23 GDPR, čini se da bi isto pravilo moralo da važi i kod nas, u skladu sa članom 42 Ustava Republike Srbije koji predviđa da se prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuju zakonom.

Praksa

Od kako je GDPR stupio na snagu, nadležni poverenici u zemljama Evropske unije doneli su par značajnih odluka. Prema veličini kazne izdvaja se odluka iz Francuske, kojom je Gugl kažnjen sa 50 miliona evra. Povod za kažnjavanje je bila prijava zbog nepoštovanja prava građana po nekoliko osnova. Prijavu su u ime korisnika podnele dve organizacije,

63 Radna grupa 29, 2018, Smernice za automatizovano donošenje odluka o pojedincima i profilisanje za potrebe Uredbe 2016/679, dostupno na: ec.europa.eu

"None Of Your Business" (NOYB) i "La Quadrature du Net" (LQDN), pri čemu je LQDN zastupao 10.000 ljudi. Nakon sprovedene istrage, utvrđeno je da je Gugl povredio više prava svojih korisnika, pre svega pravo na informisanost. Ocenjeno je da informacije nisu bile lako dostupne na Guglovom sajtu jer su bile raštrkane na više mesta, nekoherentno i netransparentno predstavljene, dok određene informacije nisu bile jasne ili su bile nepotpune. Zbog svega ovoga, pristanak koji je trebalo da bude pravni osnov za obradu nije bio zakonit, jer je jedan od osnovnih uslova zakonitog pristanka da on bude u dovoljnoj meri informisan (tj. da lica na osnovu raspoloživih informacija bude jasno na šta pristaje).[64]

Pravo na zaborav ugrađeno je u pravni okvir EU presudom Suda pravde EU u slučaju *Google Spain v AEPD and M. C. González* iz 2014. godine. Državljanin Španije Mario Kosteha Gonzalez je od kompanije Gugl tražio da se iz rezultata pretrage uklone informacije o njegovim dugovima koje su bile objavljene na sajtu lokalnih novina 1990-ih godina. Iako je dugove davno vratio, kada se guglalo njegovo ime ponovo je u rezultatima izlazio isti članak iz lokalnih novina, koji više nije bio relevantan. Sud je presudio u Gonzalesovu korist, čime je praktično uspostavljeno pravo građana EU da od servisa za pretraživanje (Gugl, Jahu, Bing, itd) traže da se iz rezultata pretrage brišu veze ka podacima koji su "neadekvatni, nerelevantni ili prekomerni u odnosu na svrhu obrade". Ipak, valja napomenuti to da, pošto naša zemlja još uvek nije članica EU, na naše građane se ova presuda ne primenjuje, odnosno Gugl nema obavezu da postupa po zahtevima za "pravo na zaborav" ako zahtev dolazi iz Srbije.

U slučaju *Rijkeboer* CJEU je razmatrao pitanje da li se nacionalnim propisima država članica može ograničiti pravo na pristup informacijama o tome ko su bili primaoci podataka i koji su im sve podaci bili dati na raspolaganje, samo na period do godinu dana pre datuma kada je nosilac podataka podneo zahtev za pristup. Sud je stao na stanovište da ograničavanje prava na pristup na ovaj način nije opravdano ukoliko se svi ostali podaci o tom licu čuvaju u znatno dužem periodu. Sud je takođe naglasio da pravo na pristup ima, između ostalog, svrhu da omogući nosiocu podataka ostvarivanje svih drugih prava, te da se nacionalnim propisima pravo na pristup može ograničiti samo izuzetno, ukoliko konkretne okolnosti to opravdavaju.[65]

Pravo na brisanje i pravo na prigovor razmatrao je Sud pravde u slučaju *Manni*. Italijanski građanin je zahtevao od nacionalnog privrednog registra (koji je bio uspostavljen u skladu sa EU regulativom) da izbriše podatke, u tom trenutku stare oko 10 godina, o tome da je bio upravnik kompanije koja je bankrotirala. CJEU je ovde ličnom pravu na brisanje podataka suprotstavio pravo javnosti da zna, koje je i bilo zaštićeno uspostavljanjem privrednog registra u koji su uvid imala sva treća zainteresovana lica. U konačnom zaključku, Sud je dao prednost pravu javnosti da zna, ali je ostavio mogućnost da se nacionalnim propisima predvide pravila da se nakon isteka određenog vremenskog perioda pravo javnosti da zna ograniči, odnosno da se udovolji pravu na prigovor na određene vrste obrade podataka. Pritom, tvrdnje italijanskog građanina da njegov trenutni posao trpi zbog toga što svi njegovi potencijalni klijenti imaju uvid u sporni podatak, Sud nije cenio kao okolnost koja je od značaja za pravo na brisanje i pravo na prigovor. Drugim rečima, prava i interesi lica koje zahteva brisanje moraju biti takve prirode da štite

64 Sažetak odluke se može naći na sajtu francuskog nadležnog organa (CNIL): cnil.fr

65 Sud pravde EU, 2009, Slučaj C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, dostupno na: curia.europa.eu

neke značajnije vrednosti koje pretežu nad pravom trećih lica da imaju uvid u sporne informacije.[66]

Dileme

Pre GDPR ere, zahtevi za ostvarivanje prava su bili retki, između ostalog i zato što su građani imali utisak da su nemoćni pred velikim i bogatim kompanijama, na šta su i same kompanije često računale. Međutim, značajnu promenu unosi pravilo koje preuzima i naš ZZPL da fizička lica ne moraju u postupcima za ostvarivanje svojih prava da učestvuju sami. Naime, prema članu 85 Zakona, lice na koje se podaci odnose ima pravo da ovlasti predstavnika ovlašćenih organizacija da ga zastupa u postupcima pred sudovima i Poverenikom. Uvođenje ovog prava je dovelo do značajnog osnaživanja građana. U Evropi već postoje organizacije koje na strateški način pristupaju ostvarivanju prava građana, koje po pravilu počinje dostavljanjem odgovarajućeg zahteva rukovaocu.

66 Sud pravde EU, 2017, Slučaj C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, dostupno na: eur-lex.europa.eu

POVERENIK ZA INFORMACIJE OD JAVNOG ZNAČAJA I ZAŠTITU PODATAKA O LIČNOSTI

POVERENIK ZA INFORMACIJE OD JAVNOG ZNAČAJA I ZAŠTITU PODATAKA O LIČNOSTI

ISTORIJAT INSTITUCIJE POVERENIKA I NJEGOV STATUS

Institucija Poverenika za informacije od javnog značaja ustanovljena je Zakonom o slobodnom pristupu informacijama od javnog značaja (ZSPIJZ) iz 2004. godine.[67] Kao fundamentalni mehanizam za povećanje transparentnosti rada organa vlasti, taj propis je građanima omogućio da aktivno traže informacije od javnog interesa, a ne samo da ih pasivno primaju u zavisnosti od dobre volje organa vlasti i javnih funkcionera. Najveću korist su svakako imali novinari, posebno oni koji se bave dubinskim istraživačkim novinarstvom i temama od najvišeg interesa za društvo, poput korupcije i organizovanog kriminala. Danas je teško zamisliti bilo kakvo ozbiljno novinarsko istraživanje bez učestalog pozivanja na Zakon o slobodnom pristupu informacijama od javnog značaja. Iako su se novinari u početku najviše interesovali za ostvarivanje ovog prava, tokom godina su zahteve aktivno počeli da podnose i drugi građani.

ZSPIJZ ustanovljava instituciju Poverenika kao samostalnog državnog organa koji je nezavisan u vršenju svoje nadležnosti. Poverenika bira Narodna skupština, na predlog odbora Narodne skupštine nadležnog za informisanje, na vreme od sedam godina, a isto lice može biti izabrano za Poverenka najviše dva puta. Poverenik mora biti lice koje je završilo pravni fakultet, ima najmanje deset godina radnog iskustva i uživa priznati ugled i stručnost u oblasti zaštite i unapređenja ljudskih prava.

Donošenjem Zakona o zaštiti podataka o ličnosti 2008. godine, nadležnost Poverenika se širi i na ovu oblast. Tako je njegova nadležnost raspoređena u dva nivoa: jedan se odnosi na zaštitu prava na slobodan pristup informacijama i nadzor nad sprovođenjem ZSPIJZ, dok se drugi nivo odnosi na zaštitu prava na privatnost, odnosno zaštitu podataka o ličnosti i nadzor nad sprovođenjem ZZPL. Ova dva nivoa nadležnosti su, po prirodi stvari, suprotstavljena i predstavljaju dve strane jedne medalje - odnos prava javnosti da zna i prava na privatnost, pa je u vršenju optimalne zaštite ova dva prava uvek potrebno vagati i naći adekvatan balans. To je, između ostalog, jedna od obaveza Poverenika.

Narodna skupština je 2004. imenovala Rodoljuba Šabića za prvog Poverenika u Srbiji, da bi 2011. bio reizabran na ovaj položaj, tako da mu je mandat istekao krajem 2018. godine. Srbija u trenutku pisanja ovog Vodiča čeka izbor novog Poverenika, pred kojim će biti veliki izazov primene novog Zakona o zaštiti podataka o ličnosti koji uvodi niz novih instituta u domaći pravni sistem i zahteva strožu primenu. To će od službe Poverenika iziskivati napor da razvije potrebne dobre prakse i smernice kako bi ZZPL mogao da zaživi na pravi način.

67 Zakon o slobodnom pristupu informacijama od javnog značaja ("Sl. glasnik RS", br. 120/2004, 54/2007, 104/2009 i 36/2010)

Poverenik je, dakle, samostalan organ vlasti nadležan za sprovođenje dva zakona i obavljanje drugih zakonom propisanih poslova, a koji bi u vršenju svojih ovlašćenja trebalo da bude potpuno nezavisan od bilo kakvih političkih ili drugih uticaja. Njegova je uloga nadzornog karaktera - on vrši poslove praćenja primene zakona i u tom smislu ima brojne nadležnosti.

Poverenik je obavezan da sačini godišnji izveštaj o svojim aktivnostima, koji podnosi Narodnoj skupštini, a dostavlja ga i Vladi i stavlja na uvid javnosti.

NADLEŽNOSTI POVERENIKA

Po novom Zakonu o zaštiti podataka o ličnosti, Poverenik ima širok spektar nadležnosti. On najpre vrši nadzor i obezbeđuje primenu ZZPL-a; stara se o podizanju svesti javnosti o rizicima, merama zaštite i pravima u vezi sa obradom podataka o ličnosti kao i o podizanju svesti rukovaoca i obrađivača u vezi sa njihovim zakonskim obavezama; pruža informacije o zakonskim pravima za zahtev lica na koje se podaci odnose; postupa po pritužbama lica na koje se podaci odnose i utvrđuje da li je došlo do povrede ZZPL; sarađuje sa nadzornim organima drugih država u vezi sa zaštitom podataka o ličnosti, u razmeni informacija i pružanju uzajamne pravne pomoći; sačinjava i javno objavljuje na svojoj internet stranici listu vrsta radnji obrade za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti; vodi evidenciju lica za zaštitu podataka o ličnosti koje mu dostavlja rukovalac ili obrađivač; i tome slično.

Poverenik vrši i inspekcijska ovlašćenja, pa je tako ovlašćen da, između ostalog, naloži rukovaocu i obrađivaču, odnosno njihovim predstavnicima, da mu pruže sve potrebne informacije, da od njih dobije pristup svim podacima o ličnosti i ostalim informacijama potrebnim za vršenje ovlašćenja, kao i pristup svim prostorijama, sredstvima i opremi rukovaoca i obrađivača, da obaveštava rukovaoca i obrađivača o mogućim povredama Zakona, itd.

Poverenik može da preduzme i određene korektivne mere, poput izricanja opomene rukovaocu odnosno obrađivaču u slučaju da se obradom krše odredbe Zakona, da im naloži da posutupe po zahtevu lica na koje se podaci odnose u vezi sa ostvarivanjem prava tog lica, da naloži rukovaocu i obrađivaču da usklade radnje obrade sa ZZPL-om na tačno određeni način i u određenom roku, da naloži rukovaocu da obavesti lice na koje se podaci odnose da je došlo do povrede njegovih podataka o ličnosti, da izrekne privremeno ili trajno ograničenje vršenja radnje obrade i zabranu obrade, da izrekne novčanu kaznu na osnovu prekršajnog naloga ako je prilikom inspekcijskog nadzora utvrđeno da je došlo do prekršaja, itd.

U vršenju svojih ovlašćenja, Poverenik može da pokrene postupak pred sudom, a sud vrši kontrolu akata Poverenika koje donese u vršenju svojih inspekcijskih nadležnosti.

SARADNJA SA POVERENIKOM

Lice na koje se podaci odnose ima pravo da Povereniku podnese pritužbu, ukoliko smatra da obrada njegovih podataka o ličnosti nije u skladu sa Zakonom, pri čemu iskorišćavanje prava na podnošenje pritužbe ne sprečava to lice da pokrene druge upravne ili sudske postupke. Poverenik je dužan da podnosioca pritužbe obavesti o toku i rezultatima postupka po pritužbi, kao i o njegovom pravu da tužbom protiv odluke Poverenika pokrene upravni spor u roku od 30 dana od dana prijema odluke.

Lice na koje se podaci odnose, dakle, ima pravo pokretanja upravnog spora protiv odluke Poverenika koja se na njega odnosi, a pokretanje upravnog spora ne utiče na njegovo pravo da pokrene i neki drugi postupak pravne zaštite.

Sa stanovišta organizacije koja obrađuje podatke te se javlja u svojstvu rukovaoca ili obrađivača, veoma je bitno da uspostavi dobru saradnju sa službom Po-

verenika, budući da će po novom Zakonu na sebe morati da preduzme čitav niz obaveza. Štaviše, član 49 ZZPL eksplicitno propisuje obavezu rukovaoca, obrađivača i njihovih predstavnika (ukoliko su određeni) da sarađuju sa Poverenikom u vršenju njegovih ovlašćenja.

Primera radi, rukovaoci i obrađivači će morati da na zahtev Poverenika njemu učine dostupnim evidencije o obradi koje vode u skladu sa Zakonom; rukovalac ima obavezu da ga obavesti u slučaju povrede podataka o ličnosti, te da u slučaju izrade procene uticaja na zaštitu podataka o ličnosti zatraži prethodno mišljenje Poverenika; Poverenik se mora konsultovati u situacijama koje se odnose na nove institute samoregulacije (kodeks postupanja, sertifikacija, obavezujuća poslovna pravila) i u mnogim drugim slučajevima.

Ukoliko rukovalac ima imenovano lice za zaštitu podataka o ličnosti, zakonska je obaveza takvog lica da sarađuje sa Poverenikom, predstavlja kontakt tačku za saradnju sa Poverenikom i savetuje se sa njim u vezi sa pitanjima koja se odnose na obradu podataka o ličnosti, kao i da ga obaveštava i od njega pribavlja odgovarajuća mišljenja. U praksi, upravo će lice za zaštitu podataka o ličnosti biti to koje će najviše komunicirati sa Poverenikom. Ukoliko takvo lice nije imenovano, svakako je poželjno da se unutar organizacije odredi lice koje će biti zaduženo za komunikaciju sa Poverenikom, imajući u vidu veoma širok spektar nadležnosti koje on ima u skladu sa ZZPL-om.

Rukovaoci i obrađivači bi trebalo da teže uspostavljanju što bolje saradnje sa službom Poverenika, da ga konsultuju kada za to imaju potrebe, kao i da prate sajt Poverenika i čitaju njegova mišljenja i odluke, jer će im to u velikoj meri pomoći u procesu usaglašavanja sa Zakonom, kao i u procesu monitoringa i demonstriranja takve usaglašenosti.[68]

68 Zvanični sajt Poverenika: poverenik.rs

POSEBNI SLUČAJEVI OBRADE PODATAKA

POSEBNI SLUČAJEVI OBRADE PODATAKA

SLOBODA IZRAŽAVANJA I INFORMISANJA

U velikoj meri, Zakon se ne primenjuje na obradu koja se vrši u svrhe novinarskog istraživanja i objavljivanja informacija u medijima, kao i u svrhe naučnog, umetničkog ili književnog izražavanja ukoliko su, u svakom konkretnom slučaju, ograničenja primene ZZPL neophodna u cilju zaštite slobode izražavanja i informisanja. Na ovaj način, Zakon daje prednost slobodi izražavanja i informisanja u odnosu na striktnu zaštitu podataka o ličnosti. Konkretnije, u ovim situacijama se neće primenjivati odredbe ZZPL koje se odnose na: (1) načela obrade; (2) prava lica na koja se podaci odnose; (3) rukovaoca, obrađivača i zajedničkog rukovaoca, kao i njihove obaveze; (4) prenos podataka o ličnosti u druge zemlje i međunarodne organizacije; (5) ostale posebne slučajeve obrade.

Domaći zakonodavac je tako, po uzoru na GDPR, predvideo značajan izuzetak od strogih pravila zaštite podataka, imajući u vidu sukob dva fundamentalna prava: slobode izražavanja i informisanja s jedne, i prava na privatnost s druge strane. Svaki put kada ovaj sukob pretegne u korist slobode govora i interesa javnosti, konkretne aktivnosti će biti oslobođene obaveza zaštite ličnih podataka.

Izuzetak od primene određenih odredbi Zakona važi tokom konkretne aktivnosti koja za svrhu ima novinarsko istraživanje i objavljivanje informacija u medijima, odnosno naučno, umetničko ili književno izražavanje. Nakon što je konkretna aktivnost gotova, sve podatke koji više nisu potrebni trebalo bi obrisati ili anonimizovati.[69]

Praksa

Jedan od prvih slučajeva zloupotrebe GDPR-a odigrao se u Rumuniji u novembru 2018. godine. Novinarsko-istraživački projekat RISE iz Rumunije objavio je nekolicinu dokumenata koji sadrže lične podatke poznatog političara i s njim povezanih osoba.[70] Odmah nakon objave na fejsbuk stranici istraživačkog projekta, reagovala je rumunska agencija za zaštitu podataka o ličnosti i izdala nalog projektu da dostavi sve informacije u vezi sa ovim slučajem, uključujući i svoje izvore, pod pretnjom novčane kazne od 650 evra za svaki dan zakašnjenja u izvršenju obaveze, do maksimalnog iznosa od 20 miliona evra.[71]

Rumunski zakon o zaštiti podataka o ličnosti sadrži odredbu koja se odnosi na obradu podataka o ličnosti u novinarske svrhe, odnosno novinarski izuzetak koji bi morao biti primenjen u ovom slučaju. Nadležna služba je, međutim, rešila da drugačije tumači zakon čime je, svesno ili omaškom, izvršila pritisak na istraživačke novinare. O slučaju se oglasila i Evropska komisija napomenom da primena opštih propisa o zaštiti podataka koja krši osnovna prava, poput slobode govora i informisanja, predstavlja zloupotrebu GDPR-a.

69 Adamović, J. et al., 2018, Vodič za medije: zaštita ličnih podataka i novinarski izuzetak, SHARE Fondacija, str. 42, dostupno na: resursi.sharefoundation.info

70 OCCRP, 2018, OCCRP Strongly Objects to Romania's Misuse of GDPR to Muzzle Media, dostupno na: occrp.org

71 Engleski prevod pisma rumunske službe za zaštitu podataka upućenog projektu RISE, dostupno na: occrp.org

SLOBODAN PRISTUP INFORMACIJAMA OD JAVNOG ZNAČAJA

Na obradu informacija od javnog značaja koje sadrže podatke o ličnosti primenjuje se, pored Zakona o zaštiti podataka o ličnosti, i Zakon o slobodnom pristupu informacijama od javnog značaja. To znači da organ javne vlasti koji tražiocu informacije čiji dostupnim takve informacije, a da one pritom sadrže podatke o ličnosti, mora voditi računa o tome da uspostavi balans između prava javnosti da zna s jedne, i prava na zaštitu podataka o ličnosti s druge strane.

Organ javne vlasti od koga su tražene informacije od javnog značaja koje sadrže podatke o ličnosti, trebalo bi da, pre nego što tražene informacije učini dostupnim, anonimizuje sve one lične podatke koji nisu apsolutno neophodni za konkretnu informaciju i njen kontekst. To dalje znači da će organ javne vlasti u svakom konkretnom slučaju morati da pronađe odgovarajući balans između dva suprotstavljena prava - prava javnosti da zna i prava na zaštitu podataka o ličnosti.

ZSPIJZ propisuje da organ vlasti neće tražiocu omogućiti ostvarivanje prava na pristup informacijama od javnog značaja ukoliko bi time povredio pravo na privatnost, ugled ili koje drugo pravo lica na koje se tražena informacija odnosi, osim (1) ako je lice na to pristalo, (2) ako se radi o ličnosti, pojavi ili događaju od interesa za javnost, a naročito o nosiocu državne i političke fukncije i ako je informacija važna s obzirom na funkciju koju to lice vrši, ili (3) ako se radi o licu koje je svojim ponašanjem, a naročito u vezi sa privatnim životom, dalo povoda za traženje informacije.[72]

OBRADA JMBG-A

Na obradu jedinstvenog matičnog broja građana (JMBG) primenjuju se odredbe posebnog zakona koji reguliše JMBG,[73] uz primenu odredbi ZZPL u delu koji se odnosi na zaštitu prava i sloboda lica na koje se podaci odnose.

Zakon o jedinstvenom matičnom broju građana propisuje da se JMBG određuje elektronski, u skladu sa pravilima propisanim ovim zakonom, i unosi se u jedinstvenu elektronsku evidenciju o matičnim brojevima koju vodi Ministarstvo unutrašnjih poslova. Zakon o JMBG propisuje da se na obradu podataka o ličnosti i evidencije koje vodi MUP, kao i na sadržinu tih evidencija, ažuriranje, brisanje, rokove čuvanja i mere zaštite podataka, primenjuju odredbe onih zakona kojim se uređuju evidencije i obrada podataka u oblasti unutrašnjih poslova.[74]

JMBG služi za vođenje evidencije podataka o ličnosti, kao i za povezivanje s drugim evidencijama državnih organa i korisnika koji imaju zakonski osnov za korišćenje matičnog broja.

OBRADA U OBLASTI RADA I ZAPOŠLJAVANJA

Na obradu u oblasti rada i zapošljavanja, uz primenu odredbi ZZPL, primenjuju se i odredbe Zakona o radu.[75]

Po Zakonu o radu, podaci o ličnosti zaposlenog koji se obrađuju u svrhu zaključenja ugovora o radu jesu ime i prezime, adresa prebivališta/boravišta, vrsta i stepen stručne spreme, kao i podaci koji se odnose na radno mesto zaposlenog (naziv i opis poslova, mesto rada, vrsta

72 Član 14 ZSPIJZ
73 Zakon o jedinstvenom matičnom broju građana ("Sl. glasnik RS", br. 24/2018)
74 Zakon o evidencijama i obradi podataka u oblasti unutrašnjih poslova ("Sl. glasnik RS", br. 24/2018)
75 Zakon o radu ("Sl. glasnik RS", br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - odluka US, 113/2017 i 95/2018 - autentično tumačenje)

radnog odnosa, trajanje ugovora, dan početka rada, radno vreme, iznos zarade). Ovi podaci se prikupljaju prilikom zaključenja ugovora o radu, prikuplja ih poslodavac, ali nije bliže određen rok čuvanja podataka. Pritom, pravni osnov za obradu konkretno ovih podataka je zakon, ali se u praksi često dešava da poslodavci prikupljaju mnogo širi spektar podataka o svojim zaposlenima. U tom slučaju poslodavci treba da razmisle da li mogu da obradu pojedinih podataka svrstaju pod neki drugi pravni osnov kao što je, na primer, legitimni interes. Poslodavci treba da budu naročito oprezni kada o svojim zaposlenima prikupljaju posebno osetljive podatke i podatke o krivičnoj osuđivanosti, svesni da moraju jasno odrediti svrhu i pravni osnov obrade. U suprotnom, ne bi trebalo da obrađuju ovakve podatke.

ZZPL propisuje da ako zakon koji uređuje rad i zapošljavanje ili kolektivni ugovor sadrže odredbe o zaštiti podataka o ličnosti, moraju se propisati i posebne mere zaštite dostojanstva ličnosti, legitimnih interesa i osnovnih prava lica na koje se podaci odnose, posebno s obzirom na transparentnost obrade, razmenu podataka o ličnosti unutar multinacionalne kompanije, odnosno grupe privrednih subjekata, kao i sistem nadzora u radnoj sredini. Imajući u vidu da ZZPL predviđa da se odredbe drugih zakona koje se odnose na obradu podataka o ličnosti moraju uskladiti sa ZZPL do kraja 2020. godine, Zakon o radu bi trebalo da propiše i posebne mere koje će štititi prava zaposlenih čiji se podaci obrađuju.

OBRADA U SVRHU ARHIVIRANJA, ISTRAŽIVANJA I STATISTIKE

Ukoliko se obrada podataka o ličnosti vrši u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, primenjuju se odgovarajuće tehničke, organizacione i kadrovske mere u cilju obezbeđivanja minimizacije podataka. Primera radi, ukoliko se svrha obrade može ostvariti uz primenu pseudonimizacije, onda bi trebalo primeniti ovu tehničku meru zaštite podataka o ličnosti.

Namera zakonodavca je da obaveže onog ko vrši obradu ličnih podataka za neku od ovih svrha, da anonimizuje podatke o ličnosti tako da se lice o čijim se podacima radi ne može identifikovati, pod uslovom da se na ovakav način može ostvariti svrha obrade.

Ukoliko se obrada vrši u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, ne primenjuju se odredbe ZZPL koje regulišu pravo na pristup lica na koje se podaci odnose, pravo na ispravku i dopunu, pravo na ograničenje obrade i pravo na prigovor, ukoliko je takvo ograničenje neophodno za ostvarivanje ovih svrha obrade, odnosno ukoliko bi primena odredbi o pravima onemogućila ili značajno otežala ostvarenje ovih svrha obrade. Isto važi i za obradu u svrhu arhiviranja u javnom interesu, s tim što se u tom slučaju ne primenjuju ni odredbe ZZPL koje se odnose na pravo na prenosivost podataka, pravo na brisanje ili ograničenje obrade koju vrši nadležni organ u posebne svrhe, obavezu rukovaoca da vrši obaveštavanje u vezi sa ispravkom ili brisanjem podataka i ograničenjem obrade, obavezu obaveštavanja rukovaoca u vezi sa ispravkom ili brisanjem podataka i ograničenjem obrade koju vrše nadležni organi u posebne svrhe, kao i ostvarivanje prava lica na koje se odnose podaci kada obradu vrše nadležni organi u posebne svrhe i provera Poverenika.

OBRADA OD STRANE CRKAVA I VERSKIH ZAJEDNICA

ZZPL propisuje da, ukoliko crkve i verske zajednice primenjuju sveobuhvatna pravila u pogledu zaštite fizičkih lica u odnosu na obradu, ta postojeća pravila se mogu i dalje primenjivati pod uslovom da se usklade sa ZZPL. U tom slu-

čaju, primenjuju se odredbe ZZPL koje se odnose na inspekcijska i druga ovlašćenja Poverenika, osim ukoliko crkva, odnosno druga verska zajednica ne obrazuje posebno nezavisno telo koje će vršiti ta ovlašćenja, pod uslovom da takvo telo ispunjava uslove predviđene Poglavljem VI Zakona, a koje se odnosi na uslove za izbor Poverenika.

OBRADA U HUMANITARNE SVRHE OD STRANE ORGANA VLASTI

ZZPL propisuje da organ vlasti može da obrađuje podatke o ličnosti u cilju prikupljanja sredstava za humanitarne svrhe, ali da tom prilikom mora primeniti odgovarajuće mere zaštite prava i sloboda lica na koje se podaci odnose u skladu sa ZZPL. Tako prikupljene podatke, organ vlasti ne može da ustupa drugim licima.

ODGO-VORNOST

ODGOVORNOST

PREKRŠAJNE KAZNE

Mada se za rukovaoce u Srbiji podrazumeva nadležnost ZZPL, njihovo poslovanje može biti predmet razmatranja i u odnosu na GDPR, ukoliko to poslovanje spada u krug aktivnosti koje su pod nadležnošću GDPR. Kazne predviđene domaćim zakonom znatno su niže od kazni iz evropske regulative, mada su bitno povećane u odnosu na pravila starog Zakona.

Rukovaoci koji krše domaći Zakon mogu u prekršajnom postupku da budu kažnjeni iznosom od najviše 2.000.000 dinara, dok je najmanja zaprećena novčana kazna za prekršaje iz ove oblasti 50.000 dinara. Ukoliko je rukovalac izvršio više prekršaja istovremeno, maksimalna kazna bi prema trenutnim prekršajnim propisima mogla iznositi do 4.000.000 dinara.

Pored kazni koje prekršajni sud izriče rukovaocu u prekršajnom postupku, Zakon predviđa i da Poverenik može da kazni rukovaoca putem prekršajnog naloga, u iznosu od 100.000 dinara. Poverenik može da kažnjava za šest tačno definisanih vrsta povreda, među kojima su praktično značajne situacije u kojima rukovalac-pravno lice (1) nastavi sa obradom u cilju direktnog oglašavanja, a lice na koje se podaci odnose je podnelo prigovor na takvu obradu; (2) ne vodi propisane evidencije o obradi; i (3) ne objavi kontakt podatke lica za zaštitu podataka o ličnosti i ne dostavi ih Povereniku (kada je ovo lice imenovano).

Po uzoru na GDPR, i naš Zakon predviđa određene parametre koji se moraju uzeti u obzir kada se određuje visina novčane kazne, a što je prema trenutnom stanju stvari relevantno u eventualnom prekršajnom postupku. To uključuje okolnosti kao što su:

- priroda, težina i trajanje povrede,
- vrsta podataka,
- postojanje namere ili nepažnje prekršioca,
- šta je rukovalac preduzeo da smanji štetu,
- da li su postojali prethodni slučajevi kršenja propisa o zaštiti ličnih podataka,
- da li rukovalac sarađuje sa Poverenikom u cilju otklanjanja posledica povrede,
- način na koji je Poverenik saznao za povredu, itd.

Međutim, ukoliko se na rukovaoca iz Srbije primenjuje i GDPR, važno je imati u vidu da na teritoriji EU kazne ne izriče prekršajni sudija u prekršajnom postupku, već direktno nadležni poverenici u vidu administrativnih kazni. Takođe, te kazne su neuporedivo veće nego u Srbiji. Maksimalna kazna koja se može izreći rukovaocu iznosi 20.000.000 evra, ili 4% globalnog godišnjeg prometa, uz opredeljenje za viši iznos.

NENOVČANA ODGOVORNOST

Pored novčanih sankcija, protiv rukovalaca koji krše propise o zaštiti ličnih podataka mogu da budu preduzete i razne druge mere. Prema novom Zakonu Poverenik je ovlašćen, između ostalog, da (1) proverava primenu Zakona korišćenjem inspekcijskih ovlašćenja; (2) zatraži i dobije od rukovaoca pristup svim podacima o ličnosti, kao i ostalim relevantnim informacijama, ali i pristup svim prostorijama rukovaoca, svim sredstvima i opremi; (3) da upozori rukovaoca o povredama Zakona; (4) da izrekne opomenu; (5) da naloži postupanje po zahtevu lica na koje se podaci odnose u vezi sa ostvarivanjem njegovih prava; (6) da naloži usklađivanje radnje obrade sa Zakonom, na tačno

određeni način i u tačno određenom roku; (7) da izrekne privremeno ili trajno ograničenje vršenja radnje obrade i zabranu obrade; (8) da naloži ispravljanje, odnosno brisanje podataka o ličnosti; ili (9) da obustavi prenos podataka o ličnosti primaocu u drugoj državi ili međunarodnoj organizaciji.

Pored žalbe Povereniku koji može da odredi neku od ovih mera kada pokrene postupak protiv rukovaoca, građani se za povredu svojih prava mogu obratiti i sudu u parničnom postupku. U tom smislu, gotovo identična pravila predviđena su i domaćim Zakonom i GDPR-om.

NAKNADA ŠTETE

Zakon, po uzoru na GDPR, predviđa da osoba koja je pretrpela materijalnu ili nematerijalnu štetu zbog povrede odredaba propisa o zaštiti ličnih podataka, ima pravo na novčanu naknadu ove štete od rukovaoca koji je štetu prouzrokovao. Dakle, ukoliko fizičko lice smatra da je takvu štetu pretrpelo zbog određenog nezakonitog postupanja rukovaoca, može u parničnom postupku dokazivati i dokazati postojanje i visinu takve štete. S druge strane, rukovalac se može osloboditi odgovornosti za štetu ako dokaže da za njen nastanak nije odgovoran ni na koji način.

Visina štete će uvek zavisiti od okolnosti konkretnog slučaja. Važno je napomenuti da u oblasti zaštite ličnih podataka od posebnog značaja nije sama visina štete za pojedinačno lice, već mogućnost da se veliki broj lica uključi u postupak. U takvom slučaju ukupan iznos štete za sva lica čije su pojedinačne štete male, može biti značajno veći od prekršajnih kazni (bar što se tiče prekršajne odgovornosti prema srpskim propisima). Tužbeni zahtev za nadoknadu štete podnosi se po opštim pravilima iz Zakona o obligacionim odnosima, dok ZZPL u tom smislu ne reguliše dodatne zahteve. Prema obligacionim propisima, šteta čija se naknada zahteva može biti matrijalna i nematerijalna, a u svakom slučaju se mora dokazati da bi bila nadoknadiva. Što se tiče nematerijalne štete, važno je naglasiti da se ne može svaka povreda privatnosti, odnosno povreda ličnih podataka, smatrati nematerijalnom štetom koja mora da se nadoknadi. Naknada se prema Zakonu o obligacionim odnosima može dosuditi samo za pretrpljene fizičke bolove, za pretrpljene duševne bolove zbog umanjenja životne aktivnosti, naruženosti, povrede ugleda, časti, slobode ili prava ličnosti, smrti bliskog lica, kao i za strah. Dakle, lice može zahtevati da mu se pored materijalne štete, i nezavisno od nje, utvrdi i nematerijalna šteta koja je nastala nezakonitom obradom, ako je to dovelo do povrede nekog od ličnih prava. Takođe, propisano je da sud prilikom odlučivanja o zahtevu za naknadu nematerijalne štete i o visini njene naknade, vodi računa o značaju povređenog dobra i cilju kome služi ta naknada, ali i o tome da se njome ne pogoduje težnjama koje nisu spojive sa njenom prirodom i društvenom svrhom.

REPUTACIONI RIZIK

Poslednjih godina u najširoj javnosti raste svest o značaju ličnih podataka na internetu, razmerama industrije podataka i bogatstvu globalnih korporacija stečenom na podacima, kao i o rizicima po privatnost građana koje uzrokuju javni i privatni akteri. Nova evropska regulativa postavila je standarde zaštite podataka u skladu sa novim društvenim vrednostima i očekivanjima, suočavajući kompanije sa ozbiljnim izborom između profitabilnog poslovnog modela i etičkih zahteva zajednice.

Stalno praćenje ponašanja korisnika, profitiranje na preprodaji ili nemaran odnos prema bezbednosti ličnih podataka, postaju sve teže podnošljivi rizici po poslovnu reputaciju. Odnos prema ličnim podacima "običnih" građana može biti od vitalnog značaja za sve rukovaoce čiji se poslovni modeli pretežno zasnivaju na upotrebi i korišćenju ličnih podataka, ili u kojima obrada ličnih podataka ima veliki značaj zbog njihovog broja, vrste i obima (na primer, hoteli, zdravstvene ustanove, osiguravajuća društva i banke, mediji, društvene mreže i slično).

U slučajevima kada je za poslovni model rukovaoca važan odnos poverenja sa korisnicima i klijentima, reputacioni rizici mogu doći u prvi plan i pre opasnosti od novčnih kazni. Rad na snižavanju tih rizika je kontinuiran proces i, pored poštovanja zakonskih pravila, podrazumeva posvećenost višim standardima. To se posebno ogleda u domenu dobijanja validnog pristanka i dostupnosti relevantnih informacija, efikasnosti odgovora na zahteve korisnika, kao i primene pažljivo odabranih mera za zaštitu bezbednosti podataka.

KRIVIČNA ODGOVORNOST

Fizička lica koja krše propise o zaštiti ličnih podataka mogu i krivično odgovarati. Naime, Krivični zakonik Srbije propisuje novčanu kaznu ili kaznu zatvora do jedne godine ukoliko neko (1) neovlašćeno pribavi, saopšti drugom ili upotrebi u svrhu za koju nisu namenjeni podatke o ličnosti koji se prikupljaju, obrađuju i koriste na osnovu zakona, kao i kada (2) protivno zakonu prikuplja podatke o ličnosti građana ili tako prikupljene podatke koristi. Kvalifikovani oblik ovog krivičnog dela, koje se kažnjava zatvorom do tri godine, postoji ako delo učini učini službeno lice u vršenju službe.

Krug radnji obuhvaćenih ovim krivičnim delom je veoma širok, te se može odnositi na bilo koju situaciju nezakonite obrade ličnih podataka. Na osnovu pravila iz ZZPL, može se zaključiti da svaka obrada podataka koja je suprotna načelima obrade predstavlja radnju ovog krivičnog dela. Isto možemo da pretpostavimo i za obradu podataka kojom se krše ona pravila ZZPL koja su zapravo razrada svih načela. Među takva pravila, na primer, spadaju ona o postojanju zakonskih osnova za obradu ili, još konkretnije, pravila o dobijanju pristanka kada je taj pravni osnov relevantan. S druge strane, postoje neka zakonska pravila iz ZZPL čije kršenje verovatno ne bi moglo dovesti do krivične odgovornosti, jer zbog svoje formalne prirode suštinski ne ugrožavaju prava i interese lica na koje se podaci odnose, kao što su formalna pravila o vođenju evidencija radnji obrade.

Smernice

Preporuka za rukovaoce koji su u dilemi oko primene ZZPL na svoje poslovanje, jeste da svakako konsultuju prethodnu praksu putem javno dostupnih izvora. Na sajtu Poverenika moguće je pronaći informacije i dokumentaciju u vezi sa raznim postupcima iz oblasti zaštite ličnih podataka i njihovim rezultatima, uključujući odluke i mišljenja Poverenika, odluke domaćih sudova, odluke Ustavnog suda Srbije kao i odluke međunarodnih sudova i tela. U pitanju je neformalni izvor ovakve prakse, mada veoma koristan, pre svega u domenu prekršajnog prava.

Praksa

Praksa domaćih parničnih i krivičnih sudova je u ovoj oblasti još uvek nerazvijena. S obzirom na okolnost da tekst novog Zakona praktično uvodi GDPR u Srbiju, može se očekivati da se praksa razvija u skladu sa relevantnom praksom evropskih sudova. Što se tiče oblasti krivičnog prava, ona ostaje nacionalno specifična i u Evropi. Prema javno dostupnoj praksi srpskih sudova krivični postupci su još uvek retki, dok je postojanje krivične odgovornosti, na primer, utvrđeno u slučaju izvoza ličnih podataka iz Srbije bez validnog pravnog osnova za prenos.

Praksa evropskih sudova je po pravilu mnogo lakše i ažurnije dostupna na odgovarajućim internet stranicama samih institucija.

Dileme

Rukovaoci i obrađivači koji posluju u Srbiji, ali na koje se primenjuju i pravila GDPR zbog toga što nude robu ili usluge na EU teritoriji ili prate ponašanje subjekata u EU, često su u nedoumici da li postoji stvarna opasnost da budu kažnjeni prema GDPR pravilima. Naime, evropska regulativa je predvidela da će se primenjivati i van EU granica u konkretnim slučajevima, što podrazumeva da licima van EU mogu biti izrečene maksimalne kazne koje predviđa GDPR. Praktično je, međutim, pitanje na koji način i kojim mehanizmima bilo koji organ iz neke države članice EU može izreći kaznu i naplatiti je od lica koje nema ni sedište niti bilo kakvu imovinu u EU. Zbog toga što se čini da je malo verovatno da se ova kazna praktično izvrši, rukovaoci iz Srbije mogu steći (pogrešan) utisak da su u takvim okolnostima bezbedni od drakonskih kazni. Međutim, važno je imati na umu nekoliko činjenica:

- Svi rukovaoci koji nemaju sedište u EU, a na koje se GDPR primenjuje, moraju da imaju svog EU predstavnika, koga sami biraju. Evropski odbor za zaštitu podataka je potvrdio da se predstavniku mogu izreći propisane kazne i da se prema njemu može sprovesti izvršenje, ukoliko pravila krše lica koja su ga postavila kao predstavnika.[76] To je mehanizam direktnog kažnjavanja lica van EU.
- Ukoliko lica van EU prekrše i obavezu da imenuju svog EU predstavnika, praktično je onemogućeno direktno izvršenje (naravno, na ovaj način je prekršena još jedna GDPR obaveza za koju je takođe predviđena administrativna kazna), ali još uvek su na raspolaganju indirektni mehanizmi. Naime, teško je zamislivo da se obrada podataka lica sa teritorije EU vrši bez uspostavljanja neke vrste saradnje sa licima koja jesu u EU, kao što su IT provajderi i posrednici, servisi koji omogućavaju plaćanje i slično. Uspostavljanjem direktne nadležnosti nad ovim licima, EU organi mogu da faktički spreče prikupljanje podataka ili dostupnost servisa i sajtova u EU, koristeći se izvršnim i ostalim ovlašćenjima koja imaju prema svojim nacionalnim propisima. Takođe, ne treba očekivati da će rukovaoci i obrađivači koji su u direktnoj nadležnosti evropske regulative, rizikovati da sami budu kažnjeni jer sarađuju sa licima koja očigledno ne poštuju GDPR pravila.[77]

76 EDPB, 2018, Smernice 3/2018 o teritorijalnoj primeni GDPR-a, dostupno na: edpb.europa.eu

77 Madge, R., 2018, GDPR's global scope: the long story, MyData Journal, dostupno na: medium.com

2019