VODIČ ZA MEDIJE

ZAŠTITA LIČNIH PODATAKA I NOVINARSKI IZUZETAK

USAID
OD AMERIČKOG NARODA

SHARE FOUNDATION

VODIČ ZA MEDIJE

ZAŠTITA LIČNIH PODATAKA I NOVINARSKI IZUZETAK

VODIČ ZA MEDIJE: ZAŠTITA LIČNIH PODATAKA I NOVINARSKI IZUZETAK
SHARE FONDACIJA, DECEMBAR 2018.

UREDNICI: DANILO KRIVOKAPIĆ, ĐORĐE KRIVOKAPIĆ
AUTORI: JELENA ADAMOVIĆ, MILICA JOVANOVIĆ, PETAR KALEZIĆ, NEVENA KRIVOKAPIĆ, BOJAN PERKOV, ANDREJ PETROVSKI
OBRADA TEKSTA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ: 200

IZRADA OVOG VODIČA OMOGUĆENA JE UZ POMOĆ AMERIČKOG NARODA PREKO AMERIČKE AGENCIJE ZA MEĐUNARODNI RAZVOJ (USAID). ZA SADRŽAJ OVOG VODIČA ODGOVORAN JE IREX I AUTORI I ON NE MORA NUŽNO ODRAŽAVATI STAVOVE USAID-A I VLADE SJEDINJENIH AMERIČKIH DRŽAVA.

CIP - Каталогизација у публикацији

Библиотека Матице српске, Нови Сад

004.738.5:351.083.8

342.721:659.2.012.8

ZAŠTITA ličnih podataka i novinarski izuzetak : vodič za medije / [autori Jelena Adamović ... [et al.] ; urednici Danilo Krivokapić, Đorđe Krivokapić]. - Novi Sad : Share foundation, 2018 (Novi Sad : NS press). - 29 str. : tabele ; 24 cm

Tekst štampan dvostubačno. - Tiraž 200.

ISBN 978-86-89487-16-9

a) Интернет - Заштита података b) Подаци о личности - Заштита

COBISS.SR-ID 327101191

PREDGOVOR

Globalno medijsko tržište se konstantno menja i mediji, bez obzira na veličinu i kapacitete, nailaze na različite izazove i mogućnosti sa ciljem da ostanu relevantni i kompetitivni. U Srbiji, gde je medijska scena prezasićena, neadekvatno regulisana i nedovoljno transparentna, mediji nastoje da opstanu na tržištu, suočavajući se i sa brzim tehnološkim promenama, disbalansom izazvanim finansiranjem iz javnih izvora, ograničenim pristupom komercijalnim prihodima i nedostatkom kapaciteta da razvijaju nove poslovne modele. U posebno teškoj situaciji nalaze se regionalni i lokalni mediji, naročito oni koji nastoje da izveštavaju profesionalno i nepristrasno, zalažući se za zaštitu javnog interesa.

Činjenica da su novi poslovni modeli u digitalnom okruženju i prihodovanje iz novih izvora finansiranja zasnovani na direktnom odnosu sa građanima, otvara brojne mogućnosti za medije, ali ujedno predstavlja i svojevrstan izazov. Nedavno usvojen Zakon o zaštiti podataka o ličnosti, koji je usklađen sa Opštom uredbom o zaštiti podataka o ličnosti (GDPR) Evropske unije, uvodi nova pravila za sve kompanije koje posluju onlajn, uključujući i medije, a koja se odnose na slučajeve prikupljanja, korišćenja i arhiviranja ličnih podataka posetilaca njihovih sajtova.

Primena novog Zakona o zaštiti podataka o ličnosti počinje u avgustu 2019. godine. Nova regulativa, između ostalog, predviđa i potencijalno visoke kazne za nepoštovanje određenih odredbi. S tim u vezi, **Projekat jačanja okruženja za održivost medija**, koji finansira **USAID**, a sprovodi **IREX**, prepoznao je potrebu da medijsku zajednicu u Srbiji obavesti o sadržaju novih pravila, načinima na koji zakonske odredbe utiču na rad medija, ali i ponudi stručnu pomoć radi razumevanja i primene novog zakona.

Ukrštajući rezultate analize nove zakonske regulative sa njihovim potencijalnim uticajem na poslovanje medija, a uz poznavanje postojećih praksi i trendova među onlajn medijima u Srbiji, ovaj vodič sadrži vrlo precizne preporuke za medije u Srbiji kako da se prilagode i ponašaju u novom regulatornom okruženju. Vodič je prvenstveno namenjen medijima koji imaju svoja onlajn izdanja, ali je koristan i upotrebljiv resurs za edukaciju i izgradnju kapaciteta tradicionalnih medija, u cilju tranzicije njihovog poslovanja u digitalno okruženje.

USAID projekat jačanja okruženja za održivost medija

NOVI PRAVNI OKVIR

NOVI PRAVNI OKVIR

U maju 2018. godine u Evropskoj uniji je na snagu stupila Opšta uredba o zaštiti podataka (General Data Protection Regulation, GDPR)[1] koja je lične podatke stavila pod zaštitu bez presedana. Primarna meta nove regulative je protok podataka na internetu koji je, zahvaljujući zastarelim propisima, decenijama bio praktično izvan domašaja zakona – što je omogućilo nagli razvoj korisnih tehnologija, ali i pojavu čitave jedne industrije podataka u kojoj gigantske korporacije ostvaruju velike profite.

Lični podaci prikupljeni iz ponašanja korisnika na internetu - posete određenim sajtovima, interakcije (lajkovi, šerovi, vrste sadržaja koji se ignorišu ili komentarišu, itd), učestalost saobraćaja - ukršteni sa tradicionalnim skupovima podataka u marketingu, postali su industrijski resurs u rangu nafte. Na ovom obilju podataka, održivi model svog poslovanja pronašlo je i savremeno novinarstvo. Bez sumnje, moguća meta GDPR-a biće mediji, tradicionalno poprište bitke između javnog i privatnog, slobode govora i prava na privatnost.

Mada je GDPR opšti okvir koji zemljama članicama Unije ostavlja prostor da mnoge detalje samostalno regulišu u skladu sa svojim nacionalnim propisima, reč je o vrlo kompleksnoj i sveobuhvatnoj regulativi iz čije se primene tek očekuju precizna tumačenja. GDPR štiti prava građana EU, što znači da se njegove odredbe odnose na bilo koju 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 tržištu EU posredno uslovljen poslovanjem usklađenim sa novom regulativom, bez obzira da li je reč o javnim ili privatnim organizacijama, pristupu grantovima, stručnoj saradnji i slično.

U Srbiji je novi zakon o ličnim podacima usvojen početkom novembra 2018. sa odloženom primenom od devet meseci.[2] Tekst zakona u najvećoj meri predstavlja adaptirani prevod nove evropske uredbe, zbog čega se može smatrati da su principi GDPR-a uvedeni i na domaći teren.

Nedostaci novog zakona pre svega se odnose na nejasne odredbe i prepisane mehanizme koji ne postoje u domaćem pravnom sistemu, što dovodi u pitanje primenjivost zakona. Pre ili kasnije, međutim, manjkavosti i praznine će biti rešene naknadnim tumačenjima, 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 temeljno ljudsko pravo.[3]

Odluka savremenih korisnika društvenih mreža da svoja privatna iskustva proživljavaju javno, ili da podatke o svom onlajn ponašanju trampe za tzv. besplatne usluge na internetu, ne znači da društvene i zakonske obaveze prema njihovoj privatnosti prestaju. Vrednost pojedinačnog podatka o ličnosti procenjuje se u zavisnosti od konteksta, ekskluzivnosti informacije ili puke količine prikupljenih podataka iz koje se potom izvodi njihova komercijalna primena. Bez obzira na pojedinačnu vrednost, lični podatak uživa punu pravnu zaštitu.

1 Iako se odnosi na engleski naziv, GDPR je skraćenica koju ćemo koristiti u ovom tekstu, s obzirom da je u tom obliku već u širokoj upotrebi kod nas. Tekst evropskog propisa dostupan je u prevodu na hrvatski jezik: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016L0680&from=EN

2 Zakon o zaštiti podataka o ličnosti http://www.parlament.gov.rs/upload/archive/files/lat/pdf/zakoni/2018/2959-18-lat.pdf

3 U stavu 1 Preambule GDPR zaštita fizičkih lica u odnosu na obradu ličnih podataka tretira se kao fundamentalno pravo. Ovakav stav oslanja se na član 8(1) Povelje o fundamentalnom pravima EU i član 16(1) Ugovora o funkcionisanju Evropske unije, kojima je predviđeno da svako ima pravo na zaštitu ličnih podataka koji se tiču njega ili nje. Vidi: Charter of Fundamental Rights of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT; Treaty on the Functioning of the European Union (TFEU) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

OSNOVNI POJMOVI

PODATAK O LIČNOSTI

Nova evropska regulativa je zadržala načelan pristup i dodatno pojednostavila definiciju ličnog podatka, prema kojoj je ''lični podatak svaka informacija koja se odnosi na identifikovano fizičko lice ili fizičko lice koje se može identifikovati'' (GDPR, član 4).

> Zakon o zaštiti podataka o ličnosti koji je na snazi u Srbiji ovako definiše svoj predmet: ''podatak o ličnosti'' je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta;
> (ZZPL, član 4).

U fokusu je, dakle, ono što neku informaciju bitno određuje kao lični podatak: ona se mora odnositi na pojedinačno ljudsko biće, bez obzira da li je ta osoba već identifikovana ili se na osnovu te informacije može identifikovati.

Stoga će lični podatak biti ime i prezime, adresa, bankovni račun, otisak prsta, zdravstveni karton, opis fizičkih ili psiholoških karakteristika, informacije o ponašanju na internetu, kao i lozinke i nalozi za poruke, mejl ili društvene mreže, istorija aktivnosti na internetu (metapodaci, šerovi, lajkovi, klikovi), istorija pretrage interneta, IP adresa kompjutera ili smartfona, IMEI broj uređaja kojim se pristupa mreži i slično. Ako su uređaj ili pretraživač personalizovani, onda i kolačići (cookies) preuzeti sa sajtova spadaju u podatke o ličnosti.

`Lični podaci su i privatno vlasništvo i sastavni činioci identiteta, intimnog osećanja vlastitog bića. Stoga se i njihova zaštita razvija u odnosu na konkretne zloupotrebe radi protivpravne koristi, ali i kao apsolutna zaštita integriteta i dostojanstva ličnosti bez obzira na eventualne motive narušavanja. Srpski zakonodavac se tradicionalno opredeljuje za izraz ''podatak o ličnosti'', kao informacija koja opisuje pasivan objekt, dok se u svakodnevnom govoru koristi izraz ''lični podatak'' koji možda preciznije prenosi i poruku o značaju kontrole nad podacima koji nam pripadaju.

POSEBNE KATEGORIJE PODATAKA

Određeni podaci o ličnosti su ''ličniji'' od drugih, a njihovom obradom se dublje zadire u privatnost građana kao osnovno ljudsko pravo, te je stoga ovim podacima potrebno dati drugačiji status kako bi mere njihove zaštite bile strože u odnosu na ostale podatke o ličnosti.

Domaći propis naročito osetljive podatke sada naziva ''posebne vrste podataka o ličnosti'' i izričito ih navodi u članu 17 kroz opis restrikcije: ''Zabranjena je obrada kojom se otkriva rasno ili etničko poreklo, političko mišljenje, versko ili filozofsko uverenje ili članstvo u sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u cilju jedinstvene identifikacije lica, podataka o zdravstvenom stanju ili podataka o seksualnom životu ili seksualnoj orijentaciji fizičkog lica.''

Definicija je prevedena iz evropske uredbe, kao i uslovi za izuzetke od zabrane da se ova vrsta podataka obrađuje, što znači da se ovi

podaci mogu obrađivati samo u određenim situacijama i pod strogo propisanim uslovima.

PAPIR ILI SERVER?

Kada se utvrđuje da li rukovanje podacima podleže zakonu, među podacima nema razlike prema vrsti materijala na kom su zabeleženi: kriterijum je samo pitanje da li se podatak odnosi na konkretnu osobu. Kada postavimo pitanje da li je taj podatak zabeležen, gde se nalazi, ko mu ima pristup, ili slično – ulazimo u domen obrade podataka.

Mada bi zaštita podataka trebalo da bude ''tehnološki neutralna'', postoje odredbe koje se po prirodi stvari mogu primeniti samo na elektronske podatke kao što su, na primer, odredbe o automatskoj obradi.

> Bitno pojašenjenje iz tehnološke perspektive odnosi se na razliku između elektronskih i digitalnih podataka, gde su podaci elektronski kada je reč o računarskim fajlovima a digitalni kada govorimo o informacijama izraženim u bitovima. Metapodaci su digitalni podaci, a kada ih generišu uređaji u vlasništvu konkretnih osoba smatraju se podacima o ličnosti.

Rukovanje podacima koji su zabeleženi na fizičkom predmetu (papiru, disku, fleš memoriji) podleže zajedničkim odredbama o načinu skladištenja, prenosa i slično, kada propisi uvode uslov strukturisanog seta podataka i počinju da govore o kolekcijama, odnosno zbirkama ličnih podataka. Bilo da su zabeleženi na digitalnom nosaču, odštampanim ili rukom ispisanim papirima poslaganim u fascikle i registre, ili se nalaze u virtuelnoj bazi, obrada ličnih podataka podleže regulativi koja propisuje, na primer, ko im i kada pristupa, kako i koliko dugo ih čuva.

Prema definiciji u zakonu, zbirka podataka predstavlja sistematizovano, strukturisano grupisanje podataka na jednom mestu, bilo da je reč o ormaru sa fasciklama ili elektronskoj bazi podataka. Uslov da skup podataka bude strukturisan čini kriterijum po kom razlikujemo, recimo, fascikle sa papirima koji sadrže bar po jedan podatak o ličnosti koji je moguće izdvojiti po nekom osnovu, od rasutih papira oko kopir-mašine.

> Privatni adresar sa kontaktima ili porodični foto-album jesu zbirke ličnih podataka, ali ne podležu obavezama iz zakona. Papirni ili elektronski imenik u kom novinari čuvaju kontakte svojih izvora, sagovornika i kolega jesu zbirke sačinjene za potrebe posla i na njih se primenjuju pravila o zaštiti podataka o ličnosti.
>
> Pažnja regulatora usmerena je pre svega na ljude i organizacije kojima je potrebno ovlašćenje da bi pristupili ličnim podacima, za svrhe kojima privatnost nije među prioritetima, bilo da je reč o privatnoj kompaniji koja prikuplja podatke o kupovnim navikama klijenata, ili o javnoj socijalnoj službi koja vodi dokumentaciju o korisnicima pomoći.

OBRADA PODATAKA

Obrada je pojam koji pokriva praktično svaku aktivnost sa ličnim podatkom ili setom ličnih podataka, od prikupljanja, umnožavanja, pretraživanja, organizacije i skladištenja, do izmene, objave ili uništenja – sa svim zamislivim radnjama između. I evropska i domaća regulativa detaljno popisuju sve različite aktivnosti, ne ostavljajući prostor za dilemu: od trenutka kada se dođe u dodir s nečijim ličnim podatkom, to postaje aktivnost koja podleže propisima o zaštiti ličnih podataka.

Pošto proglasi apsolutnu zaštitu ličnih podataka, zakon će osloboditi ove obaveze aktivnosti iz privatnog konteksta koji podrazumeva da podatke o ličnostima iz svog socijalnog kruga štitimo kao deo vlastite privatnosti.

Novinari i medijske organizacije nesumnjivo obrađuju podatke – prikupljaju ih, porede sa drugim podacima, arhiviraju ih u svoje baze i ponovo vade iz arhive; praktično, svaki opis tipova obrade iz zakonske definicije može se naći u medijskoj svakodnevici. Kada se ti podaci odnose na konkretne osobe, sumnje nema, reč je o obradi podataka o ličnosti.

OSNOVNE ULOGE

RUKOVALAC

Novi zakon rukovaoca definiše kao „fizičko ili pravno lice, odnosno organ koji samostalno ili zajedno sa drugima određuje svrhu i način obrade''.

U evropskim jezicima ovaj koncept se izražava terminima koji označavaju kontrolora ili upravljača.[1] Reč je, dakle, pre svega o ulozi koju osobe ili organizacije imaju u odnosu na lične podatke. Rukovalac određuje ''zašto'' i ''kako'' se podaci prikupljaju i čuvaju, kontroliše obradu podataka u svim segmentima: određuje vrstu, svrhu i način prikupljanja i obrade podataka, način i trajanje čuvanja, definiše prava osoba čiji se podaci obrađuju, kao i svoje i obaveze obrađivača.

Ako novinar obavlja svoje aktivnosti u ličnom svojstvu, kao frilenser, smatraće se rukovaocem, a ako radi u okviru medijske organizacije tada će organizacija snositi zakonske obaveze rukovaoca.[2]

OBRAĐIVAČ

Ova uloga se dodeljuje svakome ko obrađuje podatke u ime i za račun rukovaoca, odnosno po njegovim direktnim instrukcijama. To ga, međutim, ne lišava pravne odgovornosti, budući da u znatnoj meri samostalno određuje tehničke i bezbednosne aspekte obrade kao što su, na primer, sredstva i metode prenosa, pristupa, pohranjivanja ili uništavanja podataka.

Kompanije koje pružaju usluge hostinga, na primer, angažovane za potrebe medijske organizacije, ili umetnici koji rade na vizualizaciji podataka koje im dostave medijske organizacije, biće obrađivači.

> Hrvatski prevod GDPR-a ove dve pozicije označava terminima ''voditelj'' (rukovalac) i ''izvršitelj'' (obrađivač) obrade, što može poslužiti kao zgodno sredstvo za proveru uloge koju novinari ili medijske organizacije imaju u odnosu na konkretne lične podatke.
>
> Onaj ko vodi, kontroliše, upravlja procesom obrade - biće rukovalac. Ko god izvršava naloge, biće obrađivač. Ove uloge određuju se u zavisnosti od procesa, u odnosu na svaku konkretnu aktivnost obrade, odnosno stvaranje zbirke podataka.
>
> Novi pravni okvir zahteva jasnu podelu uloga, budući da će od statusa zavisiti i težina pravne odgovornosti koju nose dva aktera.

PRIMALAC

Stari koncept ''korisnika'' podataka u novom zakonu naziva se ''primalac'', a definiše se kao ''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

1 eng. data controller, fr. contrôleur de données, ger. Datencontroller, gr. ελεγκτή δεδομένων, it. controller di dati, mad. adatkezelő, slo. upravljavec podatkov

2 ''Zaštita podataka & frilenseri'' [dostupno na engleskom jeziku] http://www.londonfreelance.org/fl/dataprot.html

biti i drugi rukovalac i obrađivač i tzv. treća strana.

Ovo je uloga u kojoj se medijske organizacije i sami novinari često nalaze kada prikupljaju podatke u bilo kom od dva opisana svojstva, kao rukovaoci ili obrađivači, ili nijedno od ta dva.

Bilo da je reč o medijskoj organizaciji, zaposlenim novinarima ili frilenserima, njihova uloga u odnosu na lične podatke koje obrađuju može se menjati od slučaja do slučaja.

Po prirodi stvari, medijska organizacija je dužna da definiše pravni osnov za svoje aktivnosti kao i da ispita prostor za izuzetke koji su joj neophodni, posebno kada je reč o istraživačkim projektima i objavljivanju osetljivih podataka.

OSNOVNI PRINCIPI I PRAVNI OSNOV ZA OBRADU PODATAKA

OSNOVNI PRINCIPI I PRAVNI OSNOV ZA OBRADU PODATAKA

PRINCIPI OBRADE PODATAKA

Šest osnovnih principa obrade ličnih podataka trebalo bi da su podrazumevano polazište u svakom ophođenju s ljudima, uz dužnu pažnju prema njihovoj privatnosti.

Kada je reč o organizacijama kojima je obrada ličnih podataka sastavni deo poslovanja, bilo da su to javne usluge ili komercijalna delatnost, obziri prema privatnosti individualnih osoba nisu nužno prioritetni u praksi. Stoga ih je potrebno izričito formulisati i zakonski normirati.

Neki od tih principa već su ugrađeni u lokalne zakone, ali je suštinska novina to što se primenjuju na digitalno okruženje.

Medijske organizacije, urednici i novinari, bilo da su slobodni ili zaposleni, dužni su da poštuju osnovne principe zaštite ličnih podataka. Stroža primena i teže sankcije nalažu da se preispita svakodnevna praksa i sa podacima prikupljenim pre usvanja novih propisa.

Sankcije predviđene evropskom regulativom podrazumevaju novčane kazne i do 20 miliona evra ili četiri odsto godišnjeg globalnog prometa u slučaju kršenja prava stanovnika EU. Domaći zakonodavac je nešto blaži i propisuje maksimalnu kaznu do dva miliona dinara.

PODACI SE OBRAĐUJU ZAKONITO, PRAVIČNO I NA TRANSPARENTAN NAČIN.

Pristanak, ugovorne i pravne obaveze, javni i legitimni interesi jesu uslovi zakonite obrade, ali se ovo načelo odnosi i na poštovanje propisa u širem smislu. Pristanak na obradu neće pokriti kršenje zakona o zabrani diskriminacije, na primer, ili zakona o zaštiti autorskih prava. Pravičnost ili "poštenje", kako je prevedeno u domaćem zakonu, oslanja se na društvene vrednosti uvažavanja tuđih interesa; pristanak dobijen obmanom neće omogućiti pravičnu obradu. Sastavni deo ovog principa jeste transparentnost i odnosi se ne samo na informisanje ljudi čiji se podaci prikupljaju o detaljima ove obrade, već na celokupnu proceduru - tako da je uvek jasno šta se i zašto dešava s podacima, ko je odgovoran i kako vlasnici podataka mogu da ostvare svoja prava. To podrazumeva i da jezik informisanja o obradi ličnih podataka bude "sažet, transparentan, razumljiv i lako dostupan", što znači da se koriste jasne i jednostavne reči, "a posebno ako se radi o informaciji koja je namenjena maloletnom licu".

PODACI O LIČNOSTI SE PRIKUPLJAJU ZA KONKRETNE, JASNE I ZAKONITE SVRHE I NE MOGU SE DALJE OBRAĐIVATI NA NAČIN KOJI NIJE USKLAĐEN SA PRIMARNOM SVRHOM.

Ovo je princip ograničenosti svrhe obrade i podrazumeva da se precizno definiše i izričito objasni zbog čega se podaci prikupljaju, te da se tako prikupljeni podaci ne mogu obrađivati za nešto drugo bez jasnog

pravnog osnova. Tako se, na primer, kontakti prikupljeni za potrebe reportaže, ne mogu koristiti za marketing. Izuzetno, dalja obrada u svrhe arhiviranja u javnom interesu, u svrhe naučnog i istorijskog istraživanja i u statističke svrhe dozvoljena je pod određenim uslovima.

PRIKUPLJAJU SE SAMO DOVOLJNI, ODGOVARAJUĆI I PODACI KOJI SU NEOPHODNI.

Takozvana minimizacija podataka znači da se obrada svodi samo na one podatke koji se neposredno tiču svrhe za koju se prikupljaju. Svaki podatak bez kog bi se svrha obrade mogla ispuniti, predstavlja višak i sa sobom nosi kršenje zakona.

PRIKUPLJENI PODACI O LIČNOSTI SU TAČNI I AŽURNI.

Značaj ovog načela očigledan je u medijskoj svakodnevici, bilo da su ljudi čiji se podaci obrađuju izvori vesti ili korisnici medijskih usluga. Kako ovo načelo nalaže da se netačni ili zastareli podaci izbrišu, odnosno isprave, izuzetno je bitno da se u određenim situacijama sačuva istorija grešaka ili promena podataka - poput revidirane presude, promene stranačke afilijacije i slično.

PODACI SE ČUVAJU ONOLIKO DUGO KOLIKO JE NEOPHODNO ZA SVRHU ZA KOJU SE OBRAĐUJU.

Ovaj princip nalaže da se nakon ispunjenja svrhe podaci moraju obrisati ili anonimizovati. Kao i kod ograničenosti svrhe izuzetno se, pod određenim uslovima, ovaj princip ne mora odnositi na arhiviranje podataka u javnom interesu, za naučno ili istorijsko istraživanje i potrebe statističke obrade.

OBRADA PODATAKA O LIČNOSTI SE OBAVLJA U BEZBEDNIM TEHNIČKIM I ORGANIZACIONIM USLOVIMA KOJI OMOGUĆAVAJU ČUVANJE INTEGRITETA I POVERLJIVOSTI PODATAKA.

Ovo načelo podrazumeva mere zaštite od neovlašćene ili nezakonite obrade, od slučajnog gubitka, od uništenja ili oštećenja, i obuhvata tehničke i organizacione mere. To znači da će digitalne baze biti zaštićene enkripcijom, na primer, podaci će biti maskirani ili anonimizovani, pristup će biti moguć samo uz šifru odgovarajućeg nivoa autorizacije, uređaji će biti fizički zaštićeni od oštećenja, itd.

ODGOVORNOST

Ovo je dopunsko načelo zaštite podataka i zahteva da organizacija ili osoba u ulozi rukovaoca podacima bude odgovorna za ispunjenost šest osnovnih principa - što treba da bude u mogućnosti i da dokaže.

PRAVNI OSNOV ZA OBRADU PODATAKA

Novi zakonski okvir predviđa šest mogućih pravnih osnova na koje se rukovaoci mogu osloniti kada obrađuju lične podatke. Nijedan od njih nije "jači" ili "bolji" od drugih, već se za osnov bira onaj koji najviše odgovara konkretnoj svrsi pre početka obrade. Odgovarajući pravni osnov treba da bude sastavni deo informacije o obradi podataka, dok promena pravne osnove u toku obrade zahteva dobro obrazloženje. U slučaju obrade posebnih (osetljivih) podataka, pored pravnog osnova potrebno je ispuniti i uslove predviđene za obradu ove vrste podataka.

PRISTANAK

Verovatno najčešće korišćen pravni osnov u dnevnoj proizvodnji vesti i drugim medijskim uslugama, ali su novom regulativom postavljeni stroži kriterijumi koji bi mogli učiniti ovaj osnov manje poželjnim u okruženju brzog protoka informacija. Da bi bio validan, pristanak mora biti informisan, nedvosmislen i dobrovoljan, što znači da vlasnik podataka razume na šta pristaje i to čini jasnom potvrdnom radnjom, bez prinude. Takođe, pristanak se mora odnositi na konkretnu svrhu, bez uslovljavanja drugim uslugama, pri čemu promena svrhe zahteva novi pristanak. Konačno, pristanak mora biti dokumentovan da bi se mogao dokazati, dok se vlasniku podataka mora omogućiti lako i jednostavno povlačenje pristanka. Pristanak na obradu posebnih, tzv. osetljivih podataka mora biti eksplicitan. Sve potrebne informacije za pristanak moraju biti prilagođene uzrastu korisnika.

UGOVOR

Čest osnov u poslovnim odnosima sa partnerima i korisnicima, kada je obrada neophodna za izvršenje ugovora ili kada vlasnik podataka zahteva konkretne radnje pre zaključenja ugovora.

ZAKONSKE OBAVEZE

Obaveze koje ima rukovalac, a ne odnose se na obaveze iz konkretnog ugovora, mogu uticati na pojedine aspekte obrade podataka kao što je, na primer, dužina čuvanja podataka u skladu sa odredbama finansijskih ili zakona o radu.

VITALNI INTERESI

Životni interes osobe na koju se odnose podaci takođe može biti pravni osnov obrade, u slučajevima kada su ugroženi život ili zdravlje.

JAVNI POSLOVI

Predstavljaju pravni osnov za obradu podataka tokom obavljanja poslova u javnom interesu ili izvršenja zakonskih ovlašćenja rukovaoca, i odnose se pre svega na institucije javne uprave.

LEGITIMNI INTERES

Pravni osnov u slučajevima kada je obrada neophodna da bi se ostvarili opravdani interesi rukovaoca ili treće strane, što je najfleksibilniji modus obrade u poslovanju - ali su mu direktno suprotstavljeni lični interesi, prava i slobode vlasnika podataka, posebno kada je reč o deci. Stoga ovaj osnov povlači i najveću odgovornost rukovalaca prema zaštiti ličnih podataka i izlaže ih riziku merenja komercijalnih sa ličnim interesima ljudi čije podatke obrađuju.

SCENA

Na javnom događaju koji organizujete radi promocije vašeg magazina ostavili ste među učesnicima formular na kome su mogli da ostave mejl adresu ako žele da primaju obaveštenja o vašim aktivnostima. Iz ugla medija postoji legitimni interes da lica koja su im svojevoljno ostavila podatak o ličnosti, kao što je mejl adresa, obaveštavaju o svojim proizvodima i aktivnostima.

PRAVA GRAĐANA

PRAVA GRAĐANA

Svako ima pravo da bude informisan o tome da se njihovi podaci prikupljaju i koriste, kao i za šta se koriste, koliko dugo se čuvaju, s kim se dele i pod kojim uslovima. Primena ovih prava isključiva je obaveza rukovaoca - što podrazumeva interne procedure po kojima se postupa u slučaju zahteva za ostvarivanje prava. Zakon propisuje rok od mesec dana za postupanje po zahtevu, uz dva dodatna meseca kada je to neophodno i pod uslovom da o odlaganju i razlozima obavesti podnosioce zahteva. Ukoliko su zahtevi preterani, neosnovani ili ako se ponavljaju, rukovalac ima pravo da ih odbije ili da naplati obradu, pri čemu snosi teret dokazivanja.

PRAVO NA INFORMISANOST

Kompanije i organizacije su u obavezi da, jasnim i razumljivim jezikom, objasne koje podatke o ličnosti obrađuju, po kom osnovu i za koje svrhe, kako ih koriste i s kim ih dele. Takva obaveštenja moraju biti sažeta, transparentna, razumljiva, lako dostupna i besplatna.

PRAVO PRISTUPA - PRAVO NA UVID

Garantuje se pravo građana na potvrdu o tome da li se, kako i zašto njihovi podaci obrađuju, kao i pravo pristupa tim podacima. Na njihov zahtev, organizacija je dužna da građanima izda kopiju podataka koje o njima obrađuje, besplatno ili samo uz naplatu tehničkih troškova izrade kopije. Ovo pravo može biti ograničeno ukoliko izdavanje kopije povređuje prava i slobode drugih, na primer u slučaju poslovne tajne ili intelektualne svojine.

PRAVO NA ISPRAVKU I DOPUNU

Svako ima bezuslovno pravo na ispravku netačnih i dopunu nepotpunih podataka.

PRAVO NA BRISANJE - PRAVO NA ZABORAV

Primena ovog prava obuhvata slučajeve u kojima podaci više nisu neophodni za svrhe u koje su prikupljeni; ili je povučen pristanak, koji je bio osnov za obradu; ili je uložen prigovor na obradu; ili su podaci nezakonito obrađeni; ili je brisanje u skladu sa zakonskom obavezom rukovaoca; ili su podaci prikupljeni od deteta u vezi s ponudom usluga informacionog društva.

Ako je organizacija javno objavila podatke dužna je da, uzimajući u obzir dostupnu tehnologiju i troškove sprovođenja, obavesti ostale organizacije koje ih obrađuju kako bi bili obrisani svi linkovi do podataka ili kopije podataka.

Izuzeci od ovog prava odnose se na preovlađujući javni interes, uključujući slobodu govora, arhiviranje, naučne i statističke svrhe, ostvarivanje ili odbranu od pravnih zahteva, kada organizacija ne mora da postupi po zahtevu.

Takozvano pravo na zaborav ugrađeno je u pravni okvir EU odlukom Suda pravde EU u slučaju Google Spain iz 2014. Državljanin Španije Mario Kosteha Gonzales zahtevao je da se iz rezultata pretrage na Guglu uklone linkovi koji vode na oglase o prinudnoj naplati duga, objavljene na sajtu lokalnih novina davnih '90-ih.

Kako je španska Agencija za zaštitu ličnih podataka podržala Gonzalesov zahtev, kompanija Gugl i njen španski ogranak podneli su žalbu protiv ove odluke Visokom sudu Španije koji je, zatim, tražio mišljenje Suda pravde. Sud je konstatovao da je kompanija koja servisira pretragu interneta 'rukovalac', odnosno da kontroliše obradu podataka i da je dužna da na zahtev korisnika izbriše podatke, u ovom slučaju linkove, koji su "neadekvatni, nerelevantni ili prekomerni u odnosu na svrhu obrade".

Odluka se ne odnosi na tekst objavljen u novinama, već samo na rezultate pretrage koji vode ka tom tekstu.

PRAVO NA OBUSTAVLJANJE OBRADE

Podsetimo, "obrada" podrazumeva i brisanje podataka pa će obustavljanje biti 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. Organizacija je dužna da obustavi obradu kada je osporena njihova tačnost; kada je obrada nezakonita, ali se ne traži brisanje; kada organizaciji više nisu potrebni podaci, ali vlasnicima podataka jesu (za ostvarivanje pravnih zahteva); kada je uložen prigovor, a još nije potvrđeno da li legitimni razlozi organizacije preovlađuju nad pravima vlasnika podataka.

Ako je organizacija prihvatila zahtev i ograničila obradu, tada se podaci smeju obrađivati samo u jasno definisanim situacijama (uz pristanak, za ostvarivanje pravnih zahteva, za zaštitu prava drugog fizičkog ili pravnog lica).

PRAVO NA PRENOSIVOST PODATAKA

Novo pravilo u propisima izvesno je proširenje prava pristupa, jer zahteva od organizacija da na zahtev obezbede i dostave podatke o ličnosti u strukturiranom, uobičajenom i mašinski čitljivom formatu, tako da se mogu preneti drugoj organizaciji, bez tehničkih smetnji. Od organizacije se takođe može zahtevati da prenese podatke direktno drugoj organizaciji, kada je takav postupak tehnički izvodljiv.

PRAVO NA PRIGOVOR

Ovo pravo testira pravni osnov za obradu koje građanima omogućava da ga ospore. U slučaju prigovora, organizacija je dužna da obustavi obradu, osim ako može da pokaže da legitimni razlozi za obradu preovlađuju nad interesima, pravima i slobodama osobe čije podatke obrađuje ili da je obrada neophodna radi odbrane pravnih zahteva.

U slučaju prigovora direktnom marketingu, tj. u situaciji u kojoj građanin usmenim ili pismenim putem zahteva da više ne prima obaveštenja i reklamne poruke, organizacija mora obustaviti obradu u tu svrhu čim primi prigovor, odnosno prestati sa daljim slanjem poruka ili reklama.

Značajnu inovaciju predstavlja to što se ovo pravo proteže i na odluke donete korišćenjem automatizovanih mehanizama, kada osobe čiji se podaci obrađuju imaju pravo na objašnjenje odluke i ljudsku reviziju automatizovane odluke (što znači da čovek vrši pregled odluke koju je donela mašina).

SCENA

Građanin dobija telefonski poziv na privatni broj mobilnog telefona od internet portala koji je nedavno počeo sa radom, sa pitanjem da li čita navedeni portal. Kako nije siguran da li je dao broj svog mobilnog telefona portalu, postavio je pitanje odakle portalu njegovi podaci. Nakon razgovora, poslao je portalu zahtev da se njegov podatak o ličnosti, odnosno broj mobilnog telefona, obriše iz baze tog portala i da ga više ne kontaktiraju.

NOVINARSKI IZUZETAK

NOVINARSKI IZUZETAK

Novi režim zaštite ličnih podataka predviđa posebne svrhe obrade gde su prava građana ograničena, kao što su zaštita nacionalne bezbednosti, krivična istraga i slično, i detaljno propisuje ova ograničenja i obaveze nadležnih rukovalaca podacima u tim slučajevima. S druge strane, sloboda izražavanja i informisanja tretira se kao poseban slučaj obrade (član 88) i načelno je oslobođeno svih odredbi zakona koji se tiču principa obrade, prava građana i obaveza rukovalaca i obrađivača – pod uslovom da je u konkretnom slučaju to neophodno.

Domaći zakonodavac je tako, po uzoru na evropski regulatorni okvir, predvideo značajan izuzetak od strogih pravila zaštite podataka, imajući u vidu sukob dva fundamentalna prava: slobodu izražavanja i informisanja s jedne, i pravo na privatnost s druge strane. Svaki put kada ovaj sukob pretegne u korist slobode govora i interesa javnosti, novinarsko istraživanje i objavljivanje informacija u medijima biće oslobođeno obaveza zaštite ličnih podataka.

Novinarski izuzetak važi za obavljanje novinarskog posla, što uobičajeno znači da je posao obavljen kada se rezultat objavi. Nakon toga bi trebalo prestati sa obradom podataka, dakle, treba ih ili obrisati ili anonimizovati - ili obezbediti pravni osnov za dalju obradu

ŠTA JE NOVINARSKI IZUZETAK?

GDPR prepušta članicama EU da svojim nacionalnim zakonima bliže urede tenzije između zaštite podataka o ličnosti i slobode informisanja, ali im izdaje bitno uputstvo: "Kako bi se uzeo u obzir značaj prava na slobodu izražavanja u svakom demokratskom društvu, potrebno je tumačiti pojmove koji se na tu slobodu odnose, kao što je novinarstvo, u širem smislu".[1] Budući da je pisan po uzoru na evropsku Uredbu, novi domaći Zakon o zaštiti podataka o ličnosti, u članu 88, preuzima i načelnu zaštitu slobode izražavanja i informisanja u kontekstu obrade podataka o ličnosti koja se vrši u svrhe novinarskog istraživanja i objavljivanja informacija u medijima, ali propušta da bliže uredi ove okolnosti.

Jasno je da će se konkretni slučajevi novinarskog izuzetka testirati u praksi, i to svakako po uzoru na primenu GDPR-a, no već sada je moguće predvideti potencijalne izazove sukoba zaštite podataka o ličnosti i samog novinarskog čina. Za početak, opšti režim zaštite podataka građana EU koji je uspostavljen GDPR-om, doveo je do toga da je više od 1000 sajtova medija iz SAD trenutno nedostupno u članicama EU, pošto se američki izdavači nisu uskladili sa evropskom Uredbom (izvor: Nieman Lab, 2018).

Nedoumice i rizici u primeni izuzetaka ogledaju se u tumačenju pojmova kao što su novinarstvo, novinar, mediji, javni interes i tome slično. Prema smernicama britanske Poverenice za informacije za GDPR izuzecima, prilikom razmatranja da li je objavljivanje nekih informacija u javnom interesu treba da se konsultuju Uređivačke smernice BBC, Kodeks emitera regulatora za elektronske komunikacije Ofkom ili Kodeks urednika Nezavisne organizacije za profesionalne standarde u štampi, u zavisnosti o kojoj vrsti

1 GDPR, recital 135 https://gdpr-info.eu/recitals/no-153/

2 Nadležnost britanskog Povereništva za informacije obuhvata informacije od javnog značaja, otvaranje javnih podataka i privatnost ličnih podataka; više o smernicama za primenu GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex16

medija je reč.[2] U slučaju Srbije, paralela bi mogla da se napravi sa Kodeksom novinara Srbije, Smernicama za primenu Kodeksa u onlajn okruženju i Kodeksom ponašanja emitera.

KOME JE NAMENJEN NOVINARSKI IZUZETAK?

Čini se da je jedno od ključnih pitanja vaganje prava, odnosno procenjivanje da li u konkretnoj situaciji pravo javnosti da zna i sloboda izražavanja i informisanja nose prevagu nad pravom na zaštitu podataka o ličnosti. Takođe, sa razvojem digitalnih platformi i novih vidova izveštavanja, otvoren je zahtev da se definišu novinarstvo i novinarski čin. Pitanja poput onih ko je novinar, kakav sadržaj se može smatrati novinarstvom i šta je javni interes koji novinarstvo ispunjava - postaju sve važnija u kontekstu aktiviranja izuzetka u novinarske svrhe. Dakle, treba imati na umu da obrada ličnih podataka u ovom posebnom slučaju slobode izražavanja i informisanja, ne znači blanko izuzetak za obradu podataka o ličnosti već, kako domaći zakon propisuje, samo "ako su u konkretnom slučaju ova ograničenja neophodna u cilju zaštite slobode izražavanja i informisanja".

U Smernicama britanskog Povereništva za informacije pojašnjava se da, kada se radi o obradi podataka o ličnosti u novinarskom poslu, jedina svrha i isključivi pravac delovanja mora biti novinarstvo. Iako se te Smernice odnose na GDPR, saveti su svakako korisni i za tumačenje domaćeg Zakona o zaštiti podataka o ličnosti. Takođe, objavljivanje informacija mora biti u javnom interesu, koji mora da opravda nivo narušavanja privatnosti.

Značajan izazov primeni novinarskog izuzetka može biti novinarski rad u ličnom svojstvu, odnosno rad frilensera bez podrške medijske organizacije. Medijskim organizacijama će verovatno biti lakše da se oslone na izuzetak ako mogu da prikažu detaljne praktične politike i procedure, usklađivanje sa kodeksima, dobru unutrašnju svest o ulozi Poverenika za zaštitu podataka o ličnosti i adekvatno vođenje baza podataka, kao što se navodi u Smernicama britantskog Povereništva.

NOVINARSKI IZUZETAK U PRAKSI

Zasad su smernice britanskog Povereništva za primenu stare evropske Direktive o zaštiti podataka, još uvek na raspolaganju kao precizni resursi za analizu novinarskog izuzetka koji se može razložiti na četiri elementa:

1. podaci se obrađuju samo za novinarstvo, umetnost ili književnost,
2. sa ciljem objave određenog materijala,
3. uz razumno verovanje da je to objavljivanje u javnom interesu, i
4. uz razumno verovanje da usklađivanje nije kompatibilno sa novinarstvom.[3]

Sakupljanje podataka je bitan deo novinarskog posla i, mada nova pravila podižu nivo zaštite ličnih podataka, položaj novinara koji poštuju pravne i profesionalne standarde ne bi trebalo značajno da se menja. Praktične implikacije može imati prenos tereta na novinare da utvrde da li legitimni interes javnosti prevazilazi pravo na privatnost, posebno u kontekstu istraživačkog novinarstva.[4]

3 "Zaštita podataka i novinarstvo: vodič za medije", ICO [dostupno na engleskom jeziku] https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

4 "Privatnost vs Sloboda izražavanja: Posledice evropske Uredbe na globalne medije", CIMA [dostupno na engleskom jeziku]: https://www.cima.ned.org/blog/privacy-vs-free-expression-global-news-media-implications-eus-general-data-protection-regulation-gdpr/

Međutim, pozicije ostalih aktera će se bitno promeniti. Posebno treba imati u vidu moguće zloupotrebe viših standarda i novih mehanizama zaštite podataka o ličnosti kao sredstva za pritisak na medije i gušenje slobode govora i informisanja. Kazne predviđene GDPR-om su izuzetno visoke, do 20 miliona evra ili 4% globalnog godišnjeg prometa; domaći zakon propisuje kazne do dva miliona dinara za pojedinačni prekršaj, što jeste malo u poređenju sa evropskom regulativom ali u kontekstu prilika u Srbiji i finansijskih mogućnosti medija može teško ugroziti rad medija. U tom smislu, svaka kazna kroz zloupotrebu zakona može izazvati "efekat zebnje" (chilling effect), odnosno samocenzuru.

Jedan od prvih slučajeva zloupotrebe GDPR-a odigrao se u Rumuniji u novembru 2018. Istraživački projekat RISE iz Rumunije[5] objavio je nekolicinu dokumenata koji sadrže lične podatke poznatog političara i s njim povezanih osoba. Odmah nakon objave na Fejsbuk stranici istraživačkog projekta, reagovala je rumunska služba 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.[6]

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, sprovela 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.

5 "Prigovor OCCRP-a zbog pritiska na medije kroz zloupotrebu GDPR-a u Rumuniji", OCCRP [dostupno na engleskom jeziku] https://www.occrp.org/en/40-press-releases/presss-releases/8875-occrp-strongly-objects-to-romania-s-misuse-of-gdpr-to-muzzle-media

6 Engleski prevod pisma rumunske službe za zaštitu podataka upućenog projektu RISE https://www.occrp.org/en/16-other/other-articles/8876-english-translation-of-the-letter-from-the-romanian-data-protection-authority-to-rise-project

TIPIČNE SITUACIJE ZA MEDIJE

TIPIČNE SITUACIJE ZA MEDIJE

POLITIKE PRIVATNOSTI NA SAJTU

Ni GDPR ni domaći zakon ne propisuju eksplicitno obavezu rukovalaca da imaju politike privatnosti (privacy policy), odnosno dokument kojim organizacija javno definiše svoj odnos prema privatnosti i ličnim podacima i obaveštava građane o njihovim pravima. U praksi ne postoji ni ujednačenost termina, pa se kao sinonimi često koriste izrazi kao što su "izjava o privatnosti" (privacy statement) ili "obaveštenje o privatnosti" (privacy notice). Međutim, oba ova propisa imaju detaljno razrađene obaveze za rukovaoce kojima je cilj poštovanje načela transparentnosti. Postoji čitav niz informacija koje rukovaoci moraju unapred da daju licima čije podatke obrađuju, budući da je jedno od ključnih prava - pravo na informisanost.

Usvajanje politika privatnosti se u praksi pokazalo kao dobar alat za poštovanje načela trasnparentnosti i obaveze obaveštavanja lica čiji se podaci prikupljaju. Za većinu medija prisutnih na internetu, dostupnost ovakvog dokumenta predstavlja primer dobre prakse i već uspostavljenih standarda i očekivanja.

ANALIZA

Kako novi pravni okvir ne propisuje ni postojanje dokumenta o privatnosti, ni njegov obavezni sadržaj, organizacije različito odgovaraju na zakonski nalog transparentnosti. U principu, postoje dve osnovne grupe pristupa: (i) pojedine kompanije, pogotovo one koje posluju u onlajn okruženju gde prikupljaju većinu ličnih podataka koje obrađuju, u politikama privatnosti opisuju samo svoje prakse koje se odnose na prikupljanje podataka putem internet sajta, često uz "politike kolačića" (cookie policy) ili kao sastavni deo dokumenta o privatnosti, ili kao zaseban dokument; (ii) od kako je GDPR stupio na snagu, jasna je tendencija određenih kompanija da u svom dokumentu o privatnosti opišu sve glavne postupke obrade ličnih podataka bez obzira na njihovo poreklo, odnosno da li su ih prikupili preko svog sajta, neposredno od lica na koje se podaci odnose ili na neki treći način (npr. mediji u svojim politikama privatnosti mogu objasniti kako postupaju sa podacima o donatorima ili podacima o izvorima).

Prednost drugog pristupa je znatno jasnija demonstracija težnje rukovaoca da bude trasparentan o svojim praksama obrade ličnih podataka, pogotovo što se uz tekst o politikama privatnosti po pravilu objavljuju i kontakti osoba kojima se zainteresovani korisnici mogu obratiti ukoliko imaju dodatna pitanja. Kada se politike privatnosti odnose samo na podatke koji se prikupljaju putem veb sajta, rukovalac nije do kraja izvršio svoju zakonsku obavezu da sva lica čije podatke prikuplja unapred obavesti o svojim praksama obrade ličnih podataka.

PREPORUKA

Svaka medijska organizacija treba da izradi dokument o privatnosti koji odgovara njenom konkretnom poslovanju. Puko prepisivanje tuđih dokumenata izlaže organizaciju pravnom riziku pogrešnog obaveštenja čitalaca o tome šta se stvarno dešava sa njihovim

ličnim podacima, a dodatno će promašiti i smisao ovog dokumenta - da rukovaocu omogući da lako dokaže poštovanje načela transparentnosti i ispunjenje prava čitalaca na informisanost.

Kada se odlučuje šta sve u takvom dokumentu treba da piše, značajno je razmotriti i da li će segment o prikupljanju internet kolačića biti zaseban dokument ili ne.

BESPLATAN GENERATOR POLITIKA PRIVATNOSTI

SHARE fondacija je razvila alat koji može biti od pomoći pri izradi dokumenta o privatnosti u skladu s novim pravilima i specifičnim uslovima poslovanja. Alat je besplatno dostupan na adresi https://gdpr.mojipodaci.rs/generator

POSLEDICE

Rukovaoci koji krše princip transparentnosti i ne ispunjavaju obavezu da informišu građane čije podatke obrađuju, izlažu se riziku kazni od evropskih poverenika u slučaju da se na njih primenjuje GDPR, kao i kazni za prekršaj prema domaćim propisima.

Prema zakonu koji je na snazi u Srbiji, kršenje načela transparentnosti i nepoštovanje obaveze informisanja su dva prekršaja za koje se može posebno odgovarati.

REKLAME NA SAJTU, KOLAČIĆI I TREKERI

Razvoj onlajn medija i njihova sve brojnija publika otvaraju neslućene mogućnosti za dvosmernu komunikaciju, informisanje i obrazovanje, kao i za uspostavljanje profitabilnih modela poslovanja gde se zarada meri brojem klikova. Prihodi se najčešće generišu putem targetiranja korisnika uz pomoć kolačića, odnosno trekera.

Istraživanje SHARE fondacije kojim je obuhvaćeno 70 medija iz Srbije i njihovi biznis modeli, pokazalo je da se prihodi u najvećem broju slučajeva ostvaruju uz pomoć targetiranja korisnika, odnosno prikupljanja njihovih podataka. Onlajn mediji koriste kolačiće da bi merili posetu svojim sajtovima i ponašanje posetilaca, za potrebe analize internet saobraćaja ali i za potrebe marketinga. Profit se uglavnom generiše uz pomoć reklama i kolaćića trećih strana, što znači da mediji u Srbiji omogućavaju trećoj strani, po pravilu velikim kompanijama koje postavljaju kolačiće, ne samo zaradu već i pristup podacima o korisnicima. Analiza poslovanja onlajn medija u Srbiji ukazuje da sajtovi koji imaju najveći broj posetilaca sadrže i najveći broj kolačića, pri čemu kolačići trećih strana u većini slučajeva čine najveći deo ukupnog broja. To znači da kompanije koje se ne bave informisanjem, najčešće globalne korporacije, imaju pristup ličnim podacima čitalaca onlajn medija u Srbiji.

Zabrinjavajuća okolnost je da ni čitaoci ni mediji koji omogućavaju postavljanje kolačića trećih strana, po pravilu nemaju kontrolu nad obradom ličnih podataka, niti imaju uvid u koje se sve svrhe ti podaci koriste. Količina i vrsta podataka koji se prikupljaju na ovaj način predstavlja potencijalno narušavanje privatnosti, pri čemu je proces najvećim delom netransparentan. Prosečan korisnik po pravilu nije upoznat sa tehnologijom koja koristi kolačiće, pa nije ni svestan u kojoj meri različite korporacije prate njegovo surfovanje internetom.

Nova pravila o zaštiti ličnih podataka obavezuju medije da obrađuju podatke na zakonit način, a da svoje čitaoce upoznaju sa praksama obrade podataka koje medijima i trećim stranama donose profit. Posebno je važno napomenuti da pravna odgovornost medija raste ukoliko kolačići i trekeri na njihovom

sajtu doprinose ili omogućavaju profilisanje čitalaca. Profilisanje je posebno regulisano i domaćim zakonom i GDPR-om, podrazumeva niz dodatnih pravila i ograničenja za rukovaoce koji se u ovu praksu upuštaju. Zbog značaja ove teme, u EU je ovlašćeni organ za tumačenje GDPR-a doneo posebno mišljenje u kome rukovaocima daje instrukcije i preporuke ako u svom poslovanju koriste profilisanje.

ANALIZA

Bihejvioralno targetiranje, ili ciljanje prema ponašanju, u marketinškoj industriji se zasniva na eksploataciji digitalnih otisaka koje korisnici ostavljaju prilikom surfovanja internetom. Digitalni otisci mogu sadržati više različitih podataka: IP adresu i tip uređaja, istoriju poseta portalima i stranicama, vreme i trajanje posete, istoriju pretrage interneta, istoriju onlajn kupovine, geolokaciju, starost, pol, seksualne preferencije i mnogo toga još, u zavisnosti od usluga koje se koriste. Kako ponašanje ljudi na internetu i u digitalnim komunikacijama postaje sve prirodnije, i samo surfovanje internetom proizvodi sve veću količinu informacija na osnovu kojih se svaka osoba može jedinstveno okarakterisati kroz šablone nesvesnog ponašanja. Svaka od ovih informacija koja se može dovesti u vezu sa konkretnom osobom, preko vlasničkog uređaja ili softvera, spada pod definiciju podataka o ličnosti kako je utvrđena u evropskoj i domaćoj regulativi.

Kolačići i trekeri koje korisnici pokupe prilikom surfovanja internetom, uključujući i čitanje onlajn medija, deo su tehnologije koja omogućava pravljenje digitalnog otiska putem prikupljanja i obrade podataka o ličnosti.

NAJPOPULARNIJI KOLAČIĆI TREĆIH STRANA

NID, google.com - Uređaju korisnika dodeljuje jedinstvenu identifikaciju koja se koristi za praćenje aktivnosti tog uređaja na svim sajtovima gde je ovaj kolačić implementiran; podaci se koriste za targetirano, ciljano reklamiranje.

R/COLLECT, doubleclick.net - Gugl koristi ovaj kolačić za prikupljanje podataka o aktivnostima korisnika i statističkih podataka za Google Analytics, obuhvatajući različite uređaje i sajtove koje korisnik posećuje.

FR, facebook.com - Fejsbuk koristi ovaj kolačić kako bi korisniku prezentovao razne reklamne proizvode oglašivača trećih strana u realnom vremenu (na primer, onlajn aukcije).

RUD, rfihub.com - Registruje anonimizovane korisničke podatke, kao što su IP adrese, geolokacija, posećeni sajtovi, pregledane reklame, kako bi se preciznije targetovale reklame na osnovu podataka prikupljenih praćenjem kretanja korisnika po različitim sajtovima.

XTC, addthis.com - Registruje sadržaj koji korisnik deli putem društvenih mreža.

PREPORUKA

U prvom planu je pitanje transparentnosti medija koji koriste kolačiće i trekere na svojim sajtovima, budući da se to može smatrati vrstom obrade ličnih podataka na koju se primenjuju sva pravila i načela iz zakona, uključujući i pravo čitalaca da na jasan i nedvosmislen način budu upoznati sa primenom ovih tehnologija. S obzirom na to da su u pitanju teme koje prosečnom ili tehnički manje veštom korisniku mogu biti nejasne, medij- ska organizacija treba da posveti posebnu pažnju načinu na koji pruža relevantne informacije, tako da obaveštenje bude jednostavno i lako razumljivo.

GDPR je podstakao razvoj dobrih praksi i primeri se već mogu naći u različitim industrijama, uključujući i medijsku. Zbog tehničkih specifičnosti i isticanja transparentnosti, neki rukovaoci se odlučuju da ove informacije daju u posebnom dokumentu o kolačićima, iako je on sastavni deo politika

privatnosti i obrade ličnih podataka. Poštovanje načela transparentnosti znači da sastavni deo ovog dokumenta treba da budu i informacije o tome koji se kolačići trećih strana nalaze na sajtu, sa kim se dele lični podaci koje kolačići skupljaju i za koje svrhe se koriste.

Što se tiče načela zakonitosti i obaveze rukovaoca da lične podatke obrađuje samo ako za tu obradu ima valjan pravni osnov, medijske organizacije koje koriste kolačiće treba da utvrde koje kolačiće imaju na sajtu i po kom osnovu obrađuju podatke preko svakog od njih. Neki kolačići se koriste na osnovu legitimnog interesa, što će po pravilu biti kolačići koji omogućavaju funkcionalnost sajta ili za analitičke i statističke svrhe, dok će za druge kolačiće biti neophodan pristanak, neka vrsta potvrdne aktivnosti posetilaca sajta. Takođe, ukoliko se na sajtu nalaze kolačići trećih strana, medijska organizacija bi trebalo da ima regulisan odnos sa svakom od njih gde će, u zavisnosti od konkretnog slučaja, imati status zajedničkog rukovaoca, obrađivača ili primaoca podataka. Ove situacije će se u budućnosti verovatno rešavati tipskim onlajn ugovorima sa velikim kompanijama koje primenjuju ove tehnologije.

Najzad, praksa korišćenja kolačića i trekera mora biti navedena u evidencijama obrade iz kojih je moguće videti, između ostalog, šta je pravni osnov za korišćenje svake vrste/kategorije kolačića i sa kim se sve lični podaci prikupljeni na ovaj način dele.

POSLEDICE

Za nepoštovanje prava korisnika i za kršenje načela transparentnosti i zakonitosti, odnosno za obradu podataka bez odgovarajućeg pravnog osnova, medijska organizacija može snostiti najveću moguću finansijsku odgovornost prema domaćem zakonu i GDPR pravilima.

Dodatno, medijska organizacija koja koristi kolačiće trećih strana, i na taj način omogućava kompanijama obradu podataka svojih čitalaca, može dodatno odgovarati ako sa trećom stranom nije regulisala međusobne odnose odgovarajućim ugovorom (tipski onlajn ugovor).

Kazne za rukovaoce koje ne vode evidencije obrade su, prema GDPR-u, u grupi manje strogih kazni, koje mogu iznositi do 2% ukupnog godišnjeg prometa, dok je domaćim propisima predviđena mogućnost izdavanja prekršajnog naloga u iznosu od 100.000 dinara.

SCENA

U cilju unapređenja sajta vašeg medija, angažovali ste IT firmu da vam razvije novu platformu. Posle izvesnog vremena, od vaših čitalaca dobijate primedbe da na sajtu imate više od 100 kolačića, među kojima su oni koji se koriste za targetirano oglašavanje, iako nemate nikakve oglase na sajtu. Nakon konsultovanja IT firme koja vam je izrađivala sajt, saznajete da su brojni kolačići dodati radi mogućih naprednih opcija za vašu platformu, bez uzimanja u obzir politike prikupljanja podataka.

BAZA INDIVIDUALNIH DONATORA

Pojedini mediji ostvaruju svoje prihode kroz donacije direktno od čitalaca. Donacije se mogu primati kroz organizovanu jednokratnu kampanju, kroz stalno otvoren poziv čitaocima da uplaćuju donacije ili na neki treći način. U svakom slučaju, pored ostalih propisa koje medijska organizacija u ovom slučaju mora da poštuje, kao što su propisi iz oblasti deviznog poslovanja, računovodstveni ili poreski propisi, pravila iz oblasti zaštite ličnih podataka takođe su relevantna. U ovoj prilici je za medijsku organizaciju važno i pitanje da li u svom pozivu za donacije omogućava uplate u valutama koje su u upotrebi u EU, jer ta okolnost može doprineti tumačenju da se na tu medijsku organizaciju direktno primenjuje GDPR, pored domaćih zakona.

ANALIZA

Vrsta podataka o ličnosti koji se prikupljaju od čitalaca-donatora u velikoj meri će biti uslovljena zakonskim obavezama koje rukovaoci imaju po osnovu računovostvenih, poreskih ili deviznih propisa. Ukoliko zakonska regulativa koja reguliše ovu vrstu plaćanja propisuje prikupljanje i obradu određene vrste i količine ličnih podataka uplatilaca, ti propisi će po pravilu za medijsku organizaciju predstavljati pravni osnov za obradu tih podataka.

Međutim, ukoliko prikupljanje ličnih podataka nije utemeljeno na obavezujućoj zakonskoj regulativi, već rukovalac prikuplja dodatne lične podatke za svoje druge svrhe, na primer statističke, analitičke ili marketinške, tada je potrebno da rukovalac za tu obradu pribavi drugi pravni osnov, što će po pravilu biti pristanak ili legitimni interes.

Na primer, ukoliko se od korisnika koji uplaćuje donaciju traži i mejl adresa koja se koristi u svrhu slanja raznih obaveštenja, tada je za takvu obradu adrese potreban izričit pristanak korisnika koji o tome mora biti unapred obavešten.

PREPORUKA

Za medijsku organizaciju koja prikuplja donacije pre svega je korisno da ima pregled propisa po osnovu kojih mora da prikuplja lične podatke - u zavisnosti od toga koji način plaćanja se koristi i odakle uplate dolaze. Na ovaj način je lakše imati uvid u to koji se sve lični podaci moraju obrađivati po osnovu zakona, pa za predmetnu obradu nije potrebno da se traži pristanak donatora.

Takođe, ukoliko medijska organizacija prikuplja od donatora još neke podatke za druge svrhe koje nisu obaveza poštovanja pozitivnih propisa, tada treba da izvrši analizu za šta su joj tačno ti podaci potrebni i da li za njihovo prikupljanje mora da ima pristanak donatora, ili možda može da se osloni na obradu po osnovu legitimnog interesa. Pošto ova pitanja ulaze u polje pravne kvalifikacije, poželjno je da u ovim razmatranjima učestvuju pravnici ili drugi eksperti sa odgovarajućim znanjima. Deo takve analize treba da bude i određenje rokova za čuvanje podataka posle kojih oni treba da se brišu.

Rezultati ovih analiza će biti direktno od pomoći rukovaocu u situacijama kada od donatora dobije zahtev kojim ovaj želi da ostvari neko svoje pravo. Na primer, ukoliko je obrada obavezna po osnovu zakona, podaci mogu biti brisani tek kada isteknu zakonski rokovi čuvanja te se, ukoliko se donator poziva na svoje pravo na brisanje, u takvim slučajevima ovakvom njegovom zahtevu neće udovoljiti.

Sve ove informacije u vezi sa bazom donatora, između ostalog, treba da budu na odgovarajući način unete u evidencije obrade rukovaoca.

POSLEDICE

Ukoliko prilikom prikupljanja i obrade ličnih podataka svojih donatora medijska organizacija krši bilo koje od glavnih načela, kao što su načelo zakonitosti, ograničenje svrhe, minimizacija podataka ili čuvanje podataka duže nego što je to potrebno za svrhu za koju su prikupljeni, može odgovarati po najstrožem režimu, kako po GDPR-u tako i po srpskom zakonu. Isto se odnosi i na nepoštovanje prava donatora.

Kazne za rukovaoce koje ne vode evidencije obrade su, prema GDPR-u, u grupi manje strogih kazni, koje mogu iznose do 2% ukup-

nog godišnjeg prihoda, dok je domaćim propisima predviđena mogućnost izdavanja prekršajnog naloga u iznosu od 100.000 dinara.

SCENA

U okviru vašeg rada prikupljate donacije od građana kao fizičkih lica, od kojih tražite da vam pošalju fotografije ili skenove uplatnica, u svrhu posedovanja dokaza o prijemu sredstava ukoliko to zatraži poreska inspekcija. Osim imena i prezimena donatora, odlučili ste da anonimizujete sve druge podatke o ličnosti koji se mogu videti na uplatnicama, kao što su adresa ili broj računa, jer ti podaci nisu potrebni za ostvarenje svrhe.

BAZA PRETPLATNIKA

Određeni mediji su kao svoj glavni biznis model odabrali preplatu, koja se sprovodi u različitim modalitetima. Jedan od njih je "freemium", gde su osnovne usluge besplatno dostupne, dok se pun pristup svim ili dodatnim sadržajima plaća. Zatim, kod "sotfwall" modela za određen, unapred definisan broj članaka (na primer, tri mesečno) dozvoljen je pun pristup, ali je za čitanje većeg broja članaka neophodno plaćanje. "Hardwall" model pruža samo delimičan pristup sadržaju, obično uvodnim pasusima članka, dok je za čitanje celog teksta neophodno plaćanje. U ovaj model spada i članstvo, posebno u medijima koji kod svoje publike razvijaju osećaj pripadnosti, te uz potpuni pristup sadržaju članovi obično dobiju i neke dodatne pogodnosti, na primer pristup posebnim sadržajima, bazama podataka, određenim alatima, ili poklone kao što su majice, kačketi i slično sa logom medija.

Svaki od ovih modela podrazumeva da se čitaoci u određenim okolnostima moraju registrovati i platiti za sadržaje koji na drugi način nisu dostupni. Tako mediji stvaraju baze preplatnika na koje se primenjuju propisi o ličnim podacima koji su u tim bazama sadržani.

ANALIZA

Bez obzira na modalitet, pretplata znači da nastaje ugovorni odnos između medija i čitaoca - preplatnika. Obaveza medija je da isporuči plaćeni sadržaj, a preplatnika da izvrši plaćanje i preuzme sadržaj preko svog naloga. Podaci koji su potrebni za izvršenje ovog ugovora sa preplatnikom će se uglavnom smatrati njegovim ličnim podacima. Međutim, pravni osnov za njihovu obradu će biti izvršenje ugovora, te u tom smislu nije potreban pristanak preplatnika na obradu. Naravno, pod uslovom da se poštuje princip minimizacije, odnosno da se zaista prikupljaju samo podaci koji su potrebni radi izvršenja ugovora; na primer, podaci neophodni za isporuku sadržaja i izvršenje plaćanja. Ukoliko će se podaci koristiti i za druge svrhe, potrebno je odrediti da li ta druga svrha podrazumeva i traženje odgovarajućeg pristanka, na primer za sprovođenje raznih anketa. Ponekad, u određenim okolnostima, korišćenje ovih podataka u svrhe direktnog marketinga može biti legitimni interes medija, ali se pri ovoj proceni svakako preporučuje oprez i konkretan pravni savet.

Ukoliko je dugogodišnji pretplatnik prilikom kreiranja naloga ostavio svoj mejl, verovatno se može smatrati da postoji legitimni interes medija da tu adresu iskoristi da mu s vremena na vreme, u razumnim intervalima, pošalje obaveštenje o aktivnostima medija za koje se može pretpostaviti da su tom preplatniku zanimljive ili korisne. Međutim, ukoliko je neki čitalac bio pretplaćen samo na određeno vreme i zatim otkazao pretplatu, slanje marketinških poruka na njegov mejl posle toga

će teže biti opravdano legitimnim interesom, te je za ovu vrstu komunikacije preporučljivo da se od takvog čitaoca pribavi odgovarajući pristanak.

PREPORUKE

Mediji bi trebalo da unapred, pre prikupljanja podataka od pretplatnika, utvrde koje su sve svrhe za koje će podaci o ličnosti biti korišćeni, da li za svaku od tih svrha imaju odgovarajuće pravne osnove, koji su obim i vrsta podataka potrebni za ostvarenje svake konkretne svrke, kao i koji su rokovi čuvanja podataka. Kao i za druge zbirke podataka, i za ovu je potrebno da medijska organizacija izradi i redovno ažurira evidencije obrade, u kojima će takođe navesti i da li podatke prikupljene na ovaj način sa nekim dalje deli.

Takođe je važno da medijska organizacija obezbedi i reguliše interni postupak za ostvarivanje prava pretplatnika po osnovu njihovih zahteva, pri čemu u ovoj situaciji posebno može biti značajno pravo na prenos podataka drugom rukovaocu, odnosno mediju.

POSLEDICE

Ukoliko prilikom prikupljanja i obrade ličnih podataka svojih pretplatnika medijska organizacija krši bilo koje od glavnih načela, kao što su načelo zakonitosti, ograničenje svrhe, minimizacija podataka ili čuvanje podataka duže nego što je to potrebno za svrhu za koju su prikupljeni, može odgovarati po najstrožem režimu i po evropskom i po srpskom zakonu. Isto se odnosi i na nepoštovanje prava pretplatnika.

Kazne za rukovaoce koji ne vode evidencije obrade, prema GDPR-u, iznose do 2% ukupnog godišnjeg prometa, dok je domaćim propisima predviđena mogućnost izdavanja prekršajnog naloga u iznosu od 100.000 dinara.

BAZA IZVORA

Mediji će u određenim slučajevima moći da se oslone na novinarski izuzetak, što će im omogućiti da ne primenjuju propise o zaštiti podataka o ličnosti. S obzirom na to da su granice novinarskog izuzetka u ovom trenutku još uvek nejasne, te da se izuzeci u načelu usko tumače, uputno je primenjivati pravila iz regulative uvek kada to ne ugrožava novinarski posao. U tom smislu, od značaja za medije može biti pitanje u kom su režimu lični podaci o medijskim izvorima, odnosno da li za njihovo prikupljanje, korišćenje i čuvanje važe sva pravila kao i za obradu drugih ličnih podataka.

Kratak odgovor bi mogao da glasi: da, u velikoj meri, odnosno većina pravila koja su relevantna za sve ostale zbirke pod kontrolom rukovaoca, važiće i za zbirku sa ličnim podacima izvora. Suštinski, u odnosu na ove podatke medijska organizacija ima status rukovaoca, jer ona sama određuje za koje svrhe se mogu korisiti podaci o izvorima, koji se podaci prikupljaju, koliko dugo se čuvaju i na koji način se obezbeđuje njihova sigurnost i poverljivost.

ANALIZA

S obzirom na to da zbirku koja sadrži lične podatke izvora ustanovljava medij, odnosno nije regulisana nikakvim zakonom, propisom ili ugovorom, mediji treba da poštuju princip minimizacije podataka o izvorima, dakle, da prikupljaju samo one lične podatke koji su relevantni za obavljanje novinarskog posla. Pri tome će se ličnim podatkom smatrati sve one informacije koje mogu, pojedinačno ili u kombinaciji sa drugim informacijama kojima rukovalac raspolaže, služiti identifikaciji konkretnog fizičkog lica.

PREPORUKA

Kako bi poštovala sve zahteve iz propisa o zaštiti ličnih podataka, medijska organizacija bi svojim internim pravilima i procedurama trebalo da utvrdi sve svrhe za koje će koristiti podatke o izvorima, te da odredi odgovarajuće pravne osnove, vrstu i obim podataka koje prikuplja kao i rokove čuvanja. Po pravilu, ove podatke će biti moguće prikupljati ili po osnovu pristanka koji može biti dat u odgovarajućoj formi; to bi moglo biti i kroz tzv. konkludentnu radnju - pristankom na razgovor sa novinarem, ali uvek afirmativno i sa mogućnošću povlačenja pristanka. U zavisnosti od konkretnih okolnosti, može biti moguće da ovakvu obradu za određene svrhe mediji mogu da opravdaju i svojim legitimnim interesom koji preovladava nad interesima i pravima izvora.

Takođe, ukoliko smatra da se na ove podatke ili određene postupke obrade ovih podataka primenjuje novinarski izuzetak - medijska organizacija bi to pitanje trebalo da unapred razmotri i analizira, te da interno predvidi pravila koja taj izuzetak mogu da opravdaju, u skladu sa načelom odgovornosti.

U svakom slučaju, mediji bi trebalo da obezbede svojim izvorima postupak za ostvarivanje prava, među kojima poseban značaj za ovu vrstu podataka predstavlja pravo na brisanje.

Zbog osetljivosti ovakve zbirke, preporuka je da tehničke i organizacione mere koje služe čuvanju poverljivosti i sigurnosti podataka budu pažljivo planirane i primenjene.

POSLEDICE

Što se tiče same obrade ličnih podataka izvora u Srbiji, na obradu ovih podataka se verovatno neće primenjivati direktno GDPR, pa ne postoji ni veliki rizik od GDPR kazni. Međutim, povrede bilo kog načela obrade ili pravila zasnovanih na načelima, kao i kršenje prava vlasnika podataka, mogli bi biti predmet prekršajnog postupka.

I u ovom slučaju, prema GDPR-u, kazne za rukovaoce koji ne vode evidencije obrade iznose do 2% ukupnog godišnjeg prometa, dok je domaćim propisima predviđena mogućnost izdavanja prekršajnog naloga u iznosu od 100.000 dinara.

Pored zakonskih sankcija, čini se da za medije dramatičnija negativna posledica kompromitovanih podataka o izvorima može biti narušavanje poverenja, što je još jedan važan podsticaj da se sa ovakvim podacima postupa oprezno i uz poštovanje svih zakonsih pravila o zaštiti ličnih podataka koja ne ulaze u teren novinarskog izuzetka.

DIREKTNI MARKETING - MEJLING LISTE

Jedan od načina komunikacije sa postojećim i potencijalnim čitaocima može biti i putem direktnog oglašavanja koje, umesto na široku publiku, usmerava promotivnu poruku direktno na pojedinca - mejlom, konvencionalnom poštom, SMS porukama, telefonskim pozivima, itd.

U digitalnoj eri je za većinu onlajn poslovanja od posebnog značaja oglašavanje mejlom. Popularnost je steklo kao jeftin način komunikacije čiju je efikasnost lako utvrditi. Mejl marketing može značiti (1) slanje poruka već postojećim klijentima i korisnicima, i (2) slanje poruka sa reklamno-propagandnim oglasima radi sticanja novih korisnika.[1]

1 Wikipedia, Imejl marketing https://sr.wikipedia.org/wiki/Imejl _ marketing

2 Mišljenje je dala i Radna grupa 29 koja je bila ovlašćena za tumačenje EU Direktive o zaštiti podataka [dostupno na engleskom jeziku]: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217 _ en.pdf

ANALIZA

Podaci potrebni rukovaocima koji u svojim marketinškim strategijama koriste alate direktnog marketinga, uglavnom su kontakti - ime, prezime, elektronska ili fizička adresa, broj telefona - u zavisnosti od kanala komunikacije koji se koriste. U svakom slučaju, potrebno je da se prikuplja samo minimalna količina podataka, primerena sredstvu komunikacije. Ukoliko se promotivne aktivnosti sprovode mejlom, dovoljno je prikupljati samo ime i mejl, a ne i broj telefona.

PREPORUKE

Pravni osnov je glavno pitanje za rukovaoce koji koriste direktan marketing, a u igri su najčešće pristanak ili legitimni interes. Različita su mišljenja o tome u kojim se situacijama za direktan marketing mora tražiti pristanak korisnika, a kada ne mora jer se može smatrati da postoji legitiman interes rukovaoca.[2] Na osnovu dosadašnje prakse čini se da preovlađuje stav da je slanje poruka sa reklamno-propagandnim oglasima radi sticanja novih korisnika moguće samo ako su korisnici pristali da primaju takve poruke. Međutim, ukoliko se promotivne poruke šalju već postojećim korisnicima, a sadržaj poruke je relevantan za odnos koji je sa njima već uspostavljen, onda je moguće korisititi kontakte korisnika za ovaj vid komunikacije i po osnovu legitimnog interesa. Konačna odluka o tome da li je potrebno tražiti pristanak za direktan marketing treba da da bude doneta u svakom konkretnom slučaju, jer može zavisiti i od niza faktora koje je nemoguće unapred predvideti.

Ako je zauzela stav da je potrebno tražiti pristanak lica kojima se šalju promotivne poruke, medijska organizacija koja koristi ovaj vid komunikacije treba da obezbedi način na koji će pribaviti pristanak kao i način na koji će da čuva dokaze da je pristanak slobodno dat. Takođe, u tom slučaju je potrebno korisnicima obezbediti lako povlačenje pristanka.

Ustanovljena praksa za komunikaciju mejlom jeste da se u svakoj poruci nalazi link na stranu na kojoj korisnik može da povuče svoj pristanak (unsubscribe link) i to bez obzira da li je pravni osnov za obradu mejl adrese bio pristanak ili legitimni interes.

Kao i za ostale procese obrade ličnih podataka, potrebno je u evidencijama obrade opisati u kom su režimu podaci koji se koriste za direktan marketing, sa informacijama o tome sa kime se sve ti podaci dele dele i zašto, kao i koliko se dugo čuvaju.

POSLEDICE

Ukoliko prilikom slanja direktnih marketinških poruka medijska organizacija krši bilo koje od glavnih načela, kao što su načelo zakonitosti, ograničenje svrhe, minimizacija podataka ili čuvanje podataka duže nego što je to potrebno za svrhu za koju su prikupljeni, može odgovarati po najstrožem režimu, kako po GDPR tako i po srpskom zakonu. Isto se odnosi i na nepoštovanje prava korisnika.

U ovoj situaciji posebno je važno da medijska organizacija vodi računa o tome da je pristanak korisnika dat u skladu sa svim pravilima i da o tome postoje dokazi. Takođe, ako se izuzetno rukovalac opredelio za legitimni interes kao pravni osnov, on mora biti dobro obrazložen i argumentovan. Ukoliko ovi preduslovi nisu zadovoljeni, postoji rizik da korisnik podnese žalbu na rukovaoca povereniku ili upotrebi druga pravna sredstva protiv rukovaoca.[3]

Kazne za rukovaoce koji ne vode evidencije obrade mogu da iznose do 2% ukupnog godišnjeg prometa po GDPR-u, dok je domaćim propisima predviđena mogućnost izdavanja prekršajnog naloga u iznosu od 100.000 dinara.

3 U Britaniji su rukovaoci više puta kažnjavani zbog neovlašćenog slanja mejlova; više detalja o uticaju nove regulative na marketing [dostupno na engleskom jeziku]: https://www.superoffice.com/blog/gdpr-marketing/

PODACI ZAPOSLENIH

U principu, na podatke zaposlenih u medijima primenjuju se ista pravila kao i na bilo koju drugu kategoriju lica. GDPR ostavlja mogućnost državama da domaćim propisima uvedu dodatna ili drugačija pravila koja bi se odnosila samo na zaposlene, ali prema srpskom zakonu o ličnim podacima ne postoji odvojen režim za podatke koji se obrađuju u radnopravnim situacijma.

To znači da važe isti principi, ista prava lica na koje se podaci odnose i iste formalne obaveze rukovaoca da vode evidencije o tome kako obrađuju podatke zaposlenih, kao i da imaju zaključene ugovore sa obrađivačima koji mogu imati tehničke mogućnosti pristupa tim podacima.

ANALIZA

Usled vrlo detaljne radnopravne regulative u Srbiji, postoji veliki broj zakona koji regulišu koje sve podatke o ličnosti poslodavci moraju da prikupljaju i dalje obrađuju (radnopravna regulativa, evidencije u oblasti rada, propisi iz oblasti obaveznih osiguranja i poreski propisi, regulativa o bezbednosti i zaštita na radu). Prilikom poštovanja svih tih propisa, medijske organizacije se oslanjaju na zakon kao pravni osnov za obradu ličnih podataka, što znači da za ovakve obrade nije potrebno tražiti pristanak zaposlenih.

Dodatno, sa zaposlenima se zaključuju odgovarajući ugovori o radu, te je za njihovo zaključenje i izvršenje takođe potrebno obrađivati neke lične podatke. Dok god su ti podaci zaista neophodni za zaključenje i izvršenje radnopravnih ugovora, to će biti pravni osnov obrade.

Zatim, pored poštovanja zakona i izvršenja ugovora sa zaposlenim, moguće je da rukovalac ima neki legitimni interes zbog koga mora da prikuplja još širi krug podataka, van minimuma po zakonu i ugovoru. Ukoliko je takav interes rukovaoca zaista opravdan i ne ugrožava interese i prava zaposlenih, medijska organizacija može da se osloni i na ovaj pravni osnov.

Na primer, radi kontrole ulaska i izlaska iz prostorija rukovaoca, zaposleni koriste identifikacione kartice koje registruju vreme kad su ušli i izašli. U tom slučaju, ove kartice zaista treba da obrađuju samo minimum podataka, a o svrsi ovakve obrade zaposleni moraju biti jasno informisani, pri čemu se prikupljeni podaci ne smeju koristiti za neke druge namene.

Najzad, postojaće određene situacije kada medijska organizacija želi da obrađuje neke lične podatke svojih zasposlenih, ali se ta obrada ne zasniva ni na zakonu, ni na ugovoru, niti postoji opravdan legitimni interes poslodavca koji preovladava - tada se lični podaci zaposlenih mogu obrađivati samo ukoliko su oni dali slobodan pristanak, koji mogu da povuku u bilo kom trenutku bez ikakvih negativnih posledica po svoj položaj. To mogu biti situacije kada poslodavac, kao dodatnu pogodnost za svoje zaposlene, ugovora dobrovoljna osiguranja pa prikuplja i obrađuje podatke u tom cilju, ili pribavlja bilo koje slične povlastice za zaposlene.

Za poslodavce je od posebnog značaja da vode računa o podacima o svojim zaposlenima koji se svrstavaju u kategoriju osetljivih podataka (posebne vrste podataka o ličnosti), kao što su podaci o zdravstvenom stanju ili verskom ubeđenju. Po pravilu će ovakve podatke medijska organizacija moći da obrađuje samo ukoliko ima zakonsku obavezu ili ukoliko se zaposleni izričito saglasio. Takođe, preporučljivo je da se prilikom primene odgovarajućih tehničkih i organizacionih mera ima u vidu ko sve može da ima pristup ovim osetljivim podacima, bez obzira da li se nalaze na papiru ili u elektronskom obliku.

U posebnu kategoriju podataka se mogu donekle svrstati i podaci o članovima porodice zaposlenih i podaci o bivšim zaposlenim i penzionerima, koji takođe zaslužuju posebne mere zaštite i po pravilu se mogu obrađivati samo kada postoji takva zakonska obaveza. Ovde je važno napomenuti da zaposleni ne može dati pristanak u ime članova svoje porodice, u slučaju kada je pristanak potreban.

PREPORUKE

Za sve rukovaoce, pa i medijske organizacije, preporučljivo je da najpre identifikuju koje podatke obrađuju jer je to zakonska obaveza rukovaoca kao poslodavca, a zatim i koji su podaci neophodni za izvršenje radnog ugovora. Ukoliko postoje situacije kada se neki podaci zaposlenih obrađuju po osnovu legitimnog interesa, taj interes bi trebalo da bude jasno definisan, i ne sme da preteže nad interesima zaposlenih. Ukoliko se podaci obrađuju po osnovu pristanka, treba da bude sastavljen tekst tog pristanka koji će zaposleni potvrditi (potpisati) i koji bi trebalo da se čuva kao dokaz da je pristanak dat. U ovom slučaju je takođe potrebno obezbediti zaposlenima lak način da pristanak povuku u bilo kom trenutku.

Kao i ostale procese obrade ličnih podataka, i podatke zaposlenih treba na odgovarajući način opisati u evidencijama obrade, a preporuka je da se ovi procesi razdvoje posebno po svakom pravnom osnovu, odnosno svrsi obrade.

Kako bi zaposleni mogli da iskoriste svoja prava i kako bi bili upoznati sa praksama obrade ličnih podataka kod konkretnog poslodavca, preporuka je da oni budu obavešteni na odgovarajući način i o podacima koji se obrađuju i o načinu na koji mogu da ostvare svoja prava koja imaju po osnovu zakona o zaštiti podataka o ličnosti. Na primer, poslodavac može da odredi jedno lice kao kontakt osobu kojoj zaposleni mogu da se obrade ako imaju bilo kakva pitanja ili zahteve u ovom smislu.

Prilikom određivanja odgovarajućih organizacionih i tehničkih mera koje treba da obezbede sigurnost i poverljivost velike količine ličnih podataka, treba da bude jasno definisano ko sve i na koji način može da pristupa podacima, pogotovo ako su u pitanju osetljivi podaci.

POSLEDICE

Zbog velike količine podataka o zaposlenima koje poslodavci moraju da obrađuju u različite svrhe, rastu rizici od pravnih sankcija. Takođe, za poslodavce može biti osetljiv teren ukoliko bivši zaposleni uđu u spor sa poslodavcem pa se, pored radnopravnih povreda, mogu pozvati i na povrede koje se tiču obrade njihovih ličnih podataka.

Što se tiče same obrade ličnih podataka zaposlenih u Srbiji, tu je teško zamisliv scenario da se primenjuje direktno GDPR, pa ne postoji ni veliki rizik od relevantnih kazni. Međutim, povrede bilo kog načela obrade ili pravila zasnovanih na načelima, kao i kršenje prava zaposlenih, mogli bi biti predmet prekršajnog postupka.

Takođe, kazne predviđene GDPR-om za rukovaoce koji ne vode evidencije obrade mogu da iznose do 2% ukupnog godišnjeg prometa, dok je domaćim propisima predviđena mogućnost izdavanja prekršajnog naloga u iznosu od 100.000 dinara.

VELIKE BAZE PODATAKA

Značaj razumevanja pravila o zaštiti ličnih podataka dolazi do izražaja u situacijama kada novinari u svom poslu koriste velike baze podataka, odnosno podatke iz javno dostupnih baza. Novi Zakon o zaštiti podata-

ka o ličnosti se odnosi i na takve podatke, te je bitno razumeti obaveze i mere koje novinari moraju preduzeti kada rukuju javnim i velikim bazama podataka.

Novinari se velikim delom u svom poslu oslanjaju na internet, naročito kada je reč o velikim bazama podataka dostupnim onlajn koje predstavljaju neprocenjiv izvor za istraživačko novinarstvo. Jedan od globalno najupečatljivijih primera ovakvih baza jesu "Panamski papiri" - baza podataka na osnovu koje su novinari širom sveta objavljivali priče, od kojih su neke rezultirale ostavkama državnih funkcionera.

ANALIZA

Javno dostupne baze državnih organa, kao i baze koje na različite načine postaju dostupne na internetu, u većini slučajeva sadrže veliku količinu podataka o ličnosti čija je zaštita regulisana novim pravnim okvirom. Podsetimo, lični podaci su i one informacije koje za sebe ne upućuju na konkretnu osobu, ali u kombinaciji sa drugim podacima mogu dovesti do identifikacije ličnosti. Čak i kada su podaci javno dostupni, zaštićeni su zakonom, te se mogu koristiti samo za svrhu zbog koje su prikupljeni, imajući u vidu izuzetak koji predviđa novi zakon kada se podaci obrađuju u novinarske svrhe.

Jedna od prvih velikih baza podataka u Srbiji je baza imovine političara medijske organizacije KRIK, u kojoj se nalazi velika količina podataka o ličnosti prikupljenih iz javno dostupnih baza (APR, Republički geodetski zavod, osnovni i viši sudovi). Mere zaštite podataka koji su prikupljeni za potrebe ove baze ali nisu objavljeni, kao i podaci o povezanim licima, čuvaju se u enkriptovanom formatu, ne dele sa drugim licima niti se objavljuju na druge načine. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti je imao uvid u bazu, te je izdao zvanično pozitivno mišljenje, stoga Krikova baza predstavlja primer pozitivne prakse ophođenja prema javno dostupnim podacima i velikim količinama podataka.

PREPORUKE

Obilje informacija u velikim bazama predstavlja ozbiljan izazov za novinare prilikom razlikovanja podataka potrebnih za istraživanje i svih ostalih. Nerelevantni podaci osoba koje su predmet istraživanja ili podaci osoba koje nisu obuhvaćene istraživanjem, neće podrazumevati pravni osnov za obradu. S takvim podacima treba biti obazriv i oni se ne smeju koristiti, deliti, ostavljati nezaštićenim, i tome slično. Zakon predviđa da već i samo zadržavanje ili čuvanje ovih podataka predstavlja obradu, te bi u takvim slučajevima bilo korisno obratiti se pravnoj službi i uredništvu.

Važno je podsetiti da novinarski izuzetak pokriva samo podatke koji su deo konkretnog novinarskog zadatka. Posle objavljivanja, sirovi podaci se brišu ili anonimizuju. Za dalju obradu, kao što je čuvanje u arhivama, potreban je poseban pravni osnov. Podaci prikupljeni iz javnih baza i velikih baza na internetu, a koji nisu deo istraživanja, spadaju pod redovan režim zaštite podataka o ličnosti i stoga na njih treba obratiti posebnu pažnju. To, između ostalog, podrazumeva i tehničke mere zaštite i druge uslove propisane zakonom.

TEHNIČKE MERE ZA ZAŠTITU PODATAKA

TEHNIČKE MERE ZA ZAŠTITU PODATAKA

Pored organizacionih i kadrovskih, šesti princip obrade ličnih podataka podrazumeva i odgovarajuće tehničke mere za zaštitu bezbednosti podataka, ali ni evropski okvir ni domaći zakon ne propisuju šta te mere treba konkretno da znače. Standardi bezbednosti u digitalnom okruženju neprestano se menjaju, dok se druge sigurnosne mere definišu u skladu sa potrebama ljudi i organizacija koji obrađuju podatke. Što se zakona tiče, važno je da se podaci zaštite "od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja". O metodama kojima se to postiže staraju se rukovaoci i obrađivači.

Osnovni nivo tehničkih mera podrazumeva i fizičku i informacionu bezbednost podataka, kao i dobro poznavanje okruženja u kom se posluje.

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.

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 OSE- TLJIVI?	MERE ZAŠTITE
Baza izvora	Zaštićena datoteka na klaud serveru	Samo novinar koji je vlasnik baze	Strogo poverljivi/Posebni	Procedura za zaštitu poverljivih i posebnih podataka
Baza podataka o imovini političara	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 bi svaka od njih mogla biti izložena specifičnim 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, organizciona 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, koje bi mogle 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 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 - lozinke, kvalifikovani sertifikat, biometrijske informacije. 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, novi nivo kontrolisanog pristupa. U slučaju krađe kompjutera ili diskova, enkripcija je solidna prepreka neovlašćenom pristupu podacima.

PSEUDONIMIZACIJA I ANONIMIZACIJA

Tokom čitavog procesa obrade ličnih podataka, ukoliko se 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
Vuk Karadžić	Dsa Tueaotc	XXX XXX
Ivo Andrić	Fge Daleit	XXX XXX
Vuk Andrić	Dsa Daleit	XXX XXX

ORGANI-ZACIONE I OSTALE MERE ZA ZAŠTITU PODATAKA

ORGANIZACIONE I OSTALE MERE ZA ZAŠTITU PODATAKA

INTERNE PROCEDURE ZA RUKOVANJE PODACIMA O LIČNOSTI

Iako propisi o zaštiti podataka o ličnosti ne nameću obavezu kompanijama da imaju interne politike i procedure kojima je regulisano kako će poštovati propise, u praksi se pokazalo da je za rukovaoce i obrađivače jako korisno da ih imaju.

Prema GDPR-u i prema srpskom zakonu, osnovni princip je da rukovalac sam treba da primenjuje zakon na taj način da je u svakom trenutku u mogućnosti da ponudi dokaze da poštuje sva pravila - da može da predoči primenu zakona. U tom smislu, propisivanje i poštovanje internih procedura kojih moraju da se drže svi zaposleni kod rukovaoca, može poslužiti kao koristan dokaz da je rukovalac zaista preduzeo mere i praktične korake koji su direktno usmereni ka primeni propisa o zaštiti ličnih podataka.

Materija ovih akata mogu biti interna pravila o postupanju po zahtevima za ostvarenje prava korisnika i čitalaca, zatim procedure u slučaju raznih vrsta povrede integriteta podataka i propisivanje konkretnih organizacionih mera kojih moraju da se pridržavaju svi zaposleni ili samo oni koji imaju pristup osetljivim vrstama podataka. I ovde je preporuka da ovakva interna dokumenta budu prilagođena prilikama rukovaoca i regulišu pravila koja su u okviru konkretne organizacije zasta sprovodiva i sprovode se.

EVIDENCIJA OBRADE

Zakon o zaštiti podataka o ličnosti propisuje obavezu vođenja evidencije obrade koja se odnosi na rukovaoce i obrađivače. Ovakva 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:

1. obrada može da prouzrokuje visok rizik po prava i slobode lica na koje se podaci odnose;

2. obrada nije povremena;

3. 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, svaki medij bi trebalo da vodi evidencije obrade podataka, jer će na taj način razumeti koje sve podatke ima u svom posedu i moći lakše da se prilagodi novim pravilima.

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 je to od njih zatraženo.

> Prethodni zakon o zaštiti podataka o ličnosti propisivao je obavezu vođenja evidencija o obradi podataka o ličnosti, kao i prijavu ovakvih evidencija kod Poverenika za zaštitu podataka o ličnosti koji je bio zadužen za vođenje centralnog registra zbirki podataka. Novi Zakon o zaštiti podataka o ličnosti u članu 102 navodi da obaveza vođenja ovakvog registra prestaje danom stupanja na snagu zakona. Ipak, na osnovu mišljenja Poverenika, ovakva obaveza postoji sve do početka primene novog zakona, odnosno 21. avgusta 2019. godine, nakon čega će ova obaveza prijavljivanja evidencija o obradi podataka i formalno prestati da postoji.[1]

GDPR postavlja nešto manje obaveza, pa propisuje samo obavezu vođenja ovih evidencija uz izuzetke za manje rukovaoce i one koji ne prikupljaju osetljive podatke.

PREDSTAVNIK U EU

Ukoliko se na organizaciju koja nema sedište u EU ekstrateritorijalno primenje GDPR, imaće obavezu da imenuje predstavnika u EU.

Predstavnik mora da ima sedište u jednoj od država članica u kojoj se nalaze lica čiji se podaci o ličnosti obrađuju. Rukovalac ili obrađivač ovlašćuje predstavnika da mu se nadzorni organi i lica na koja se podaci odnose obraćaju u vezi sa svim pitanjima koja se tiču obrade. Ovo fizičko ili pravno lice će biti dodirna tačka za zahteve nadređenih lica ili subjekata podataka o ličnosti i predstavlja rukovaoca ili obrađivača podataka u pogledu njihovih obaveza sa aspekta GDPR-a. Ovaj predstavnik ne mora biti advokat, ali mora odlično poznavati zakon EU o zaštiti podataka.

Obaveza se ne primenjuje na obradu koja je povremena, ne podrazumeva u većoj meri obradu posebnih kategorija podataka o ličnosti ili obradu podataka o ličnosti koji se odnose na krivičnu i prekršajnu osuđivanost i za koju nije verovatno da će prouzrokovati rizik za prava i slobode fizičkih lica uzimajući u obzir prirodu, okolnosti, obim i svrhe obrade; kao ni na organe vlasti.

LICE ZA ZAŠTITU PODATAKA O LIČNOSTI

Ova uloga predviđena je za osobu iz organizacije čiji je glavni zadatak da se stara da organizacija primenjuje sva pravila u vezi sa zaštitom podataka o ličnosti, odnosno da nadzire usklađenost poslovanja sa zahtevima novih pravila.

Organizacije su u obavezi da imenuju lice za zaštitu podataka o ličnosti u sledećim slučajevima:

1. Kada obradu vrši organ javne vlasti, osim sudova koji postupaju u okviru svoje sudske nadležnosti.

2. Kada se osnovne delatnosti rukovaoca ili obrađivača sastoje iz radnji obrade koje zbog svoje prirode, obima i/ili svrha zahtevaju redovno i sistematsko praćenje lica na koja se podaci odnose.

3. Kada se osnovne delatnosti rukovaoca ili obrađivača sastoje iz masovne obrade posebnih kategorija podataka o ličnosti i podataka o ličnosti koji se odnose na krivičnu i prekršajnu osuđivanost.

Mediji najčešće neće imati formalnu obavezu da imenuju osobu odgovornu za zaštitu ličnih podataka, ali bi to moglo olakšati upravljanje podacima u organizaciji i ojačati poverenje zajednice.

Osoba koja ima ovu vrstu zaduženja, stara se da svi zaposleni znaju i mogu da demonstriraju usklađenost sa propisima u svakom trenutku kada se to od organizacije traži. Drugim rečima, ona vodi evidenciju:

1. Održanih treninga i revizija.

2. Primenjenih mera za zaštitu ličnih podataka.

3. Saglasnosti za obradu podataka o ličnosti.

4. Aktivnosti obrade ličnih podataka.

5. Zahteva lica na koje se odnose podaci o ličnosti kao i radnjama preduzetim za rešavanje tih zahteva.

6. Povreda zaštite podataka o ličnosti i mera preduzetih za njihovo rešavanje.

7. Komunikacije sa licima na koje se odnose podaci.

UGOVORI SA OBRAĐIVAČIMA

Dok će se mediji po pravilu nalaziti u ulozi rukovaoca, često mogu biti u situaciji da angažuju druge ljude i organizacije za određene obrade podataka o ličnosti. Hosting kompanija će im pružati usluge čuvanja podataka, na primer, dok im stručnjak sa specifičnim znanjima može rešavati pojedine segmente obrade podataka. Saradnja sa marketinškom kompanijom koja bi koristila bazu pretplatnika smatra se angažovanjem obrađivača.

U ovakvim situacijama, prava i obaveze rukovaoca i obrađivača treba da se urede ugovorom u pisanom obliku čiji je sadržaj detaljno uređen članom 45 Zakona o zaštiti podataka o ličnosti, a koji između ostalog treba da sadrži sledeće odredbe:

1. obavezu obrađivača da obrađuje podatke samo u okviru dobijenog ovlašćenja;

2. podaci se ne smeju koristiti u svrhe koje nisu ugovorene;

3. obavezu obrađivača da obezbedi organizacione i tehničke mere zaštite podataka;

4. zaposleni kod obrađivača imaju obaveze čuvanja poverljivosti podataka;

5. obaveze koje obrađivač ima po okončanju ugovorene obrade podataka.

IZVOZ PODATAKA IZ SRBIJE

Izvoz podataka o ličnosti treba razumeti kao akt prenošenja ličnih podataka čija je obrada u toku ili su namenjeni daljoj obradi nakon prenošenja iz Srbije u drugu državu ili međunarodnu organizaciju, bez obzira da li su podaci zabeleženi na papiru ili u elektronskom obliku, da li se šalju običnom ili e-poštom. Za izvoz podataka neophodno je obezbediti bar jedan od mogućih pravnih osnova:

1. **PRIMERENI NIVO ZAŠTITE** - smatra se da je primereni nivo zaštite obezbeđen u državama i međunarodnim organizacijama koje su članice Konvencije Saveta Evrope o zaštiti lica u odnosu na automatsku obradu ličnih podataka[2] odnosno sa kojima je zaključen međunarodni sporazum o prenosu podataka o ličnosti;

1 Mišljenje poverenika u vezi sa vođenjem evidencija o obradi podataka o ličnosti https://tinyurl.com/y932v833

2 Tekst Konvencije je dostupan na srpskom jeziku: https://tinyurl.com/y9zxscvp

2. **ODGOVARAJUĆE MERE ZAŠTITE** - ukoliko rukovalac, odnosno obrađivač obezbedi ostvarivost prava i pravnu zaštitu licu na koje se odnose podaci. To se može urediti pravno obavezujućim aktom sačinjenim između organa vlasti; standardnim ugovornim klauzulama koje izrađuje poverenik, a kojima se u celini uređuje odnos između rukovaoca i obrađivača; ugovornim odredbama između rukovaca i/ili obrađivača sa rukovaocem, obrađivačem i primaocem u drugoj državi, odnosno međunarodnoj organizaciji, uz posebno odobrenje poverenika.

3. **POSEBNE SITUACIJE** - u članu 69 Zakona o zaštiti podataka o ličnosti, ove situacije su taksativno opisane: 1) lice na koje se podaci odnose je 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) izvoz je neophodan za zaključenje ili izvršenje ugovora zaključenog u interesu lica na koje se podaci odnose; 3) izvoz je neophodan za podnošenje, ostvarivanje ili odbranu pravnog zahteva.

ZAKONSKA ODGOVOR-NOST

ZAKONSKA ODGOVORNOST

NOVČANE KAZNE

Mada se za rukovaoce u Srbiji podrazumeva nadležnost novog zakona iz 2018. godine, njihovo poslovanje može biti predmet razmatranja u odnosu na GDPR ukoliko svojim poslovanjem naruše zaštitu ličnih podataka stanovnika država članica EU. Kazne predviđene domaćim zakonom mnogo su manje od kazni iz evropske regulative, mada su značajno povećane u odnosu na pravila starog zakona.

Mediji 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 iznostiti i 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, od kojih su za medije relevantne 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, i tako dalje.

Međutim, ukoliko se na medije primenjuje GDPR, važno je imati u vidu da na teritoriji Unije 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. Ovakva kazna se svakako ne odnosi na uobičajene vrste prekršaja u poslovanju medijskih organizacija, ali dobro ilustruje raspon predviđenih kazni i za manje povrede.

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. Za medije koji svoj ugled grade na

nepristrasnom informisanju i otkrivanju događaja koji se neopravdano kriju od javnosti, odnos prema ličnim podacima "običnih" građana može biti od vitalnog značaja.[1]

Onlajn mediji su često posebno osetljivi na ovu vrstu poverenja, te reputacioni rizici mogu doći u prvi plan i pre opasnosti od novčanih kazni. Rad na snižavanju tih rizika je kontinuiran proces i, pored poštovanja minimalnih zakonskih pravila, podrazumeva posvećenost višim standardima, posebno u domenu dobijanja validnog pristanka i dostupnosti relevantnih informacija, efikasnosti odgovora na zahteve čitalaca, kao i primene pažljivo odabranih mera za zaštitu bezbednosti podataka.

NAKNADA ŠTETE

Evropski i domaći pravni okvir predviđaju 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 medija, može u parničnom postupku dokazivati i dokazati postojanje i visinu takve štete. S druge strane, mediji se mogu osloboditi odgovornosti za štetu ako dokažu da za njen nastanak nisu odgovorni 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).

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 postupanja 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 zakonom koji je na snazi u Srbiji i GDPR-om.

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 (ii) protivno zakonu prikuplja podatke o ličnosti građana ili tako prikupljene podatke koristi.

Krug radnji obuhvaćenih ovim krivičnim delom je veoma širok, te se može odnositi na bilo koju situaciju nezakonite obrade ličnih podataka. Primer ovakve primene može se naći u praksi domaćeg suda kada je ustanovljena krivična odgovornost u slučaju izvoza ličnih podataka iz Srbije bez validnog pravnog osnova za prenos.

PRIMER

Organ za zaštitu podataka o ličnosti nemačke pokrajine Baden-Virtemberg je u novembru 2018. kaznio kompaniju za pružanje usluge društvene mreže sa 20.000 evra zbog kršenja obaveza o bezbednosti podataka iz člana 32 GDPR-a. Kompanija je bila meta tehničkog napada tokom leta 2018, i tom prilikom je ostvaren neovlašćen pristup šiframa i mejl adresama više od 300.000 korisnika, koji su bili i objavljeni.

1 Prema pojedinim anketama, čak 59% čitalaca bi prestalo da konzumira medije koji ne poštuju propise o zaštiti ličnih podataka (slajdovi 30, 31): https://edelman.kr/wp-content/uploads/insight/eprilaunchdeckfinal-121109151241-phpapp01.pdf

RESURSI:

Pribor za lične podatke - gdpr.mojipodaci.rs

Baza znanja - resursi.sharefoundation.info

Istraživačka laboratorija - Labs.rs

2018