

**Od čitalaca
do profita:**

**Upravljanje
podacima
korisnika u
digitalnim
medijima**



Od čitalaca do profita:

Upravljanje podacima
korisnika u digitalnim
medijima



Od čitalaca do profita:

Upravljanje podacima korisnika u digitalnim medijima

Autorke:

Ana Toskić Cvetinović

Gordana Andrić

Milica Tošić

Tanja Maksić

Urednica: Kristina Obrenović

Maj 2026.



Organizacija za evropsku
bezbednost i saradnju
Misija u Srbiji

Ovaj projekat finansira
Evropska unija



#EY
ЗА ТЕБЕ

Izradu ove publikacije omogućila je Misija OEBS-a u Srbiji u okviru projekta koji sprovodi organizacija Partneri Srbija „Više od klikova: Redefinisanje poslovnih modela srpskih medija u skladu sa standardima privatnosti“, a koji je finansijski podržan od strane Evropske unije.

Stavovi izrečeni u publikaciji pripadaju isključivo autorima i ne predstavljaju nužno zvaničan stav Misije OEBS-a u Srbiji, kao ni stavove Evropske unije.

Svi pojmovi koji su u publikaciji upotrebljeni u muškom gramatičkom rodu obuhvataju muški i ženski rod lica na koja se odnose.

Sadržaj

Lista skraćenica	5
Uvod.....	7
Metodologija.....	9
Deo I - Analiza modela i praksi upravljanja podacima	11
Upotreba podataka u poslovnim procesima onlajn medija.....	11
<i>Klasifikacija podataka u redakcijama</i>	<i>12</i>
<i>Upotreba podataka i saradnja sa publikom.....</i>	<i>16</i>
<i>AI u redakcijama.....</i>	<i>18</i>
Deo II - Regulatorni okvir	22
Propisi i politike upravljanja podacima u medijima.....	22
Zaštita privatnosti korisnika onlajn medija	23
<i>Vrste podataka koje mediji prikupljaju o korisnicima</i>	<i>24</i>
<i>Pravni osnov obrade podataka korisnika</i>	<i>26</i>
<i>Transparentnost i informisanje korisnika</i>	<i>27</i>
Upravljanje podacima i interne prakse medija	29
Prava korisnika medijskih sadržaja (publike) i njihova ostvarivost u praksi	32
Bezbednost podataka	34
<i>Interna pravila i bezbednosna kultura.....</i>	<i>35</i>
<i>Tehničke mere i testiranje novih alata</i>	<i>35</i>
<i>Revizija ugovornih obaveza i dobavljača.....</i>	<i>36</i>
<i>Upravljanje povredama podataka.....</i>	<i>36</i>
Nadzor i regulatorni okvir	36
Nalazi analize prakse	37
<i>Uporedna iskustva i primeri dobre prakse.....</i>	<i>37</i>
<i>Prakse i iskustva u Srbiji.....</i>	<i>39</i>

Obrade podataka o ličnosti prilikom izveštavanja - Balans između prava na privatnost i javnog interesa	41
<i>Regulatorni okvir i etičke norme</i>	42
<i>Pravo na brisanje podataka i pravo na zaborav</i>	43
<i>Zloupotreba prava</i>	45
<i>Test javnog interesa</i>	46
Zaključak	47
Deo III - Set koraka za usklađivanje poslovanja medija	48
Kontrolna lista za redakcije	53
Prilog 1- Onlajn anketa za medijske radnike	56

Lista skraćenica

AI	Artificial Intelligence/Veštačka inteligencija
BIRN	Balkanska istraživačka mreža Srbije
DSA	Uredba (EU) 2022/2065 Evropskog parlamenta i Veća o jedinstvenom tržištu digitalnih usluga i izmeni Direktive 2000/31/EZ (Akt o digitalnim uslugama)
EMFA	Uredba (EU) 2024/1083 Evropskog parlamenta i Veća o uspostavljanju zajedničkog okvira za medijske usluge na unutarnjem tržištu (Evropski akt o slobodi medija) i izmeni Direktive 2010/13/EU
GDPR	Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka te o stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka)
EU	Evropska unija
OEBS	Organizacija za evropsku bezbednost i saradnju
Poverenik	Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti
Partneri Srbija	Partneri za demokratske promene Srbija
RATEL	Regulatorno telo za elektronske komunikacije i poštanske usluge
ZZPL	Zakon o zaštiti podataka o ličnosti

Uvod

Savremeni onlajn mediji istovremeno su novinarske organizacije, digitalne platforme i poslovni subjekti koji zavise od podataka. Svaki put kad korisnik posećuje sajt, pretplati se na *newsletter*¹ ili ostavi komentar, medij dolazi do podataka koji mogu usmeriti uredničke odluke - koje teme pokrivati, kojim kanalima ih distribuirati - ali i menadžerske: kako monetizovati sadržaj, kako izgraditi lojalnu publiku i kako se nositi sa sve strožim regulatornim zahtevima. Podaci koji nastaju iz algoritamske distribucije sadržaja pregledi, angažovanje, viralnost, postali su nova digitalna moneta koja snažno oblikuje i urednički i upravljački rad medija.

Novo okruženje nameće i novi pristup: mediji nisu samo organizacije koje proizvode sadržaj, već složeni sistemi koji moraju da upravljaju celim „životnim ciklusom“ podatka, od trenutka nastanka i prikupljanja, kroz skladištenje i analizu, do arhiviranja ili brisanja. Bez jasnih pravila i interne kulture upravljanja podacima, mediji izlažu sebe pravnim rizicima, a svoju publiku povredama privatnosti.

Imajući to u vidu, ovaj dokument namenjen je onlajn i hibridnim medijima u Srbiji koji se, u digitalnom okruženju, istovremeno nalaze u ulozi nosilaca slobode izražavanja, rukovalaca podacima o ličnosti i tržišnih aktera koji zavise od različitih modela monetizacije. Polazeći od važećeg pravnog okvira i identifikovanih praksi u Srbiji i uporednom kontekstu, vodič ima za cilj da pokaže kako se zakonita i transparentna obrada podataka o korisnicima može uskladiti sa ekonomskom održivošću medija, bez narušavanja poverenja publike i osnovnih prava na privatnost.

1 Newsletter (takođe poznat i kao bilten) je vrsta periodične elektronske pošte (email-a) koju preduzeća, mediji, organizacije ili pojedinci šalju grupi pretplatnika. Njegova osnovna svrha je informisanje publike o najnovijim vestima, ponudama, edukativnom sadržaju i dr.

Umesto pristupa koji zaštitu podataka posmatra kao prepreku poslovanju, vodič polazi od pretpostavke da su odgovorno upravljanje podacima, jasno razgraničenje svrha obrade i poštovanje prava korisnika ključni preduslovi dugoročne stabilnosti medija, njihove reputacije i otpornosti u uslovima regulatornih i tržišnih promena. U tom kontekstu, vodič tumači Opštu uredbu o zaštiti podataka (*General Data Protection Regulation - GDPR*), Akt o digitalnim uslugama (*Digital Services Act - DSA*) i Evropski akt o slobodi medija (*European Media Freedom Act - EMFA*) kao komplementarne delove istog regulatornog okvira, u kojem se zaštita podataka o ličnosti, odgovornost digitalnih platformi i zaštita uredničke nezavisnosti i medijskog pluralizma međusobno nadopunjuju, a ne isključuju.

Dokument se sastoji od tri dela. **Deo I** obuhvata analizu modela i praksi upravljanja podacima u onlajn medijima, uključujući upotrebu podataka o ličnosti. **Deo II** donosi analizu važećeg pravnog i regulatornog okvira. **Deo III** predstavlja praktičan set koraka za usklađivanje poslovanja medija. Dokument je namenjen urednicima, menadžerima i svima koji u medijima donose odluke o digitalnim alatima, monetizaciji i odnosu sa publikom.

Vodič je izrađen uz podršku Misije OEBS-a u Srbiji, u okviru projekta „Više od klikova: Redefinisanje poslovnih modela srpskih medija u skladu sa standardima privatnosti“, koji doprinosi primeni Strategije razvoja sistema javnog informisanja u Republici Srbiji za period 2020–2025. godine.²

2 Službeni glasnik RS, broj 148/2020

Metodologija

Ovaj dokument se oslanja na više međusobno dopunjujućih metodoloških pristupa.

Polaznu osnovu za izradu dokumenta predstavljaju potrebe prepoznate u **Strategiji razvoja sistema javnog informisanja u Republici Srbiji za period 2020–2025**,³ naročito u okviru Mere 5.3 koja se odnosi na unapređenje informacione bezbednosti građana u medijskom okruženju. Ova mera, između ostalog, ukazuje na potrebu jačanja transparentnosti medija u vezi sa pravilima o privatnosti (uključujući korišćenje kolačića i obradu podataka korisnika), unapređenja postupanja po zahtevima za ostvarivanje prava na brisanje podataka, kao i podizanja svesti o rizicima po privatnost u digitalnom okruženju, posebno za osetljive društvene grupe. Ove potrebe dodatno su potvrđene kroz istraživanja i analize organizacija civilnog društva, poput Indeksa privatnosti u medijima (IPM)⁴, koji kontinuirano prati zaštitu prava građana na privatnost u onlajn medijskoj sferi Srbije.

U metodološkom smislu, dokument se primarno zasniva na **analizi pravnog okvira i prakse medija**, na osnovu javno dostupnih izvora. Analizirani su važeći nacionalni propisi relevantni za rad onlajn medija u Srbiji, pre svega Zakon o zaštiti podataka o ličnosti, Zakon o javnom informisanju i medijima, Zakon o elektronskim komunikacijama i Kodeks novinara i novinarki Srbije, kao i ključni propisi Evropske unije (GDPR, DSA i EMFA), imajući u vidu obaveze usklađivanja sa međunarodnim standardima koja proizlaze iz strateških ciljeva Vlade Republike Srbije u sklopu procesa pristupanja EU i poslovanje medija prema publici u EU.

3 Strategiji razvoja sistema javnog informisanja u Republici Srbiji za period 2020–2025 https://www.media.srbija.gov.rs/medsrp/dokumenti/medijska_strategija210_cyr.pdf

4 Indeks privatnosti i u medijima, SHARE Fondacija, <https://indeks.onlajnmediji.rs/>

Analiza je dopunjena **uporednim pristupom**, kroz razmatranje praksi stranih medija, sa fokusom na primere koji prevazilaze zakonske minimume i razvijaju naprednije i etički ambicioznije modele upravljanja podacima korisnika.

Poseban doprinos istraživanju dali su uvidi prikupljeni kroz aktivnosti realizovane u okviru istog projekta - radionice za medije i prateći upitnik. Tokom januara i februara 2026. godine organizovane su tri radionice za medijske radnike u Beogradu, Novom Sadu i Nišu, na kojima je učestvovalo ukupno 49 predstavnika medija. Diskusije sa učesnicima ukazale su da pitanja zaštite privatnosti korisnika ne mogu biti posmatrana isključivo kroz prizmu upravljanja podacima i usklađenosti sa propisima, već i kroz širi kontekst odnosa između prava na privatnost i slobode izražavanja. Na osnovu ovih nalaza i potreba koje su učesnici iskazali, dodatno je prilagođen i proširen sadržaj ovog dokumenta kroz poglavlje „Obrada podataka o ličnosti prilikom izveštavanja“.

Kako bi se dodatno sistematizovala i dokumentovala saznanja prikupljena tokom radionica, sprovedena je i **onlajn anketa**⁵ o poznavanju i razumevanju praksi zaštite podataka u onlajn medijima. Upitnik je distribuiran učesnicima radionica, kao i širem krugu medija putem direktne komunikacije i kroz relevantna novinarska i medijska udruženja. Ukupno su prikupljena 34 odgovora, pri čemu većina ispitanika (gotovo 65%) dolazi iz lokalnih i regionalnih medija. Nalaze iz upitnika treba tumačiti sa oprezom, imajući u vidu da uzorak nije reprezentativan i zasniva se na dobrovoljnom učešću. Njegova svrha nije bila statistička generalizacija, već dodatna kontekstualizacija i potvrda uvida prikupljenih kroz direktan rad sa medijskim profesionalcima.

Zaključci i preporuke oblikovani su na osnovu kombinacije normativne analize, uvida iz prakse, rezultata istraživanja i profesionalnog iskustva autorki u oblasti medija, novinarstva i zaštite podataka o ličnosti.

5 Na kraju ovog dokumenta nalaze se pitanja onlajn ankete- Prilog 1.

Deo I – Analiza modela i praksi upravljanja podacima

Upotreba podataka u poslovnim procesima onlajn medija

Proizvodnja vesti, njihova distribucija i interakcija medija i publike u savremenom okruženju odvija se u velikoj meri u digitalnoj sferi. Podaci Republičkog zavoda za statistiku za 2025. godinu⁶ pokazuju da 90% stanovnika Srbije svakodnevno koristi internet za pristup vestima i informacijama, a da njih 84,7% ima profile na društvenim mrežama.

Novinarstvo i digitalni mediji zavise od globalnih tehnoloških kompanija, pretraživača i drugih digitalnih posrednika koji „kroje“ novi informacijski sistem. Od njihovih poslovnih politika, programa i algoritama zavisi koliko će određeni medijski sadržaj biti (ne)vidljiv i do koje publike će stići, koliko će biti naplativ ili pak biti potpuno uklonjen.

Prilagođavajući se uslovima koje diktira novo okruženje, mediji su preuzeli dizajn i logiku platformi i proizvodnju i distribuciju medijskog sadržaja podredili platformama i pretraživačima. Ove okolnosti su fundamentalno promenile neke od bazičnih standarda u radu medija:

6 Upotreba IKT – pojedinci | Republički zavod za statistiku Srbije. <https://www.stat.gov.rs>

- Vesti, naročito na naslovnoj strani, brzo se menjaju kako bi publika stalno dobijala novi sadržaj, a algoritmi dobijali signale „viralnosti“, kao i lične i druge podatke.
- Klikbejt⁷ sadržaj donosi najveći broj pregleda, generiše veliku publiku i veliki broj poseta sajtovima.
- Najprofitabilnija vrsta novinarstva je ona koja prati logiku velikih brojeva i ume da se prilagodi algoritamskoj optimizaciji.
- Mediji se pretvaraju u fabrike proizvodnje velikog broja sadržaja niskog kvaliteta, a najuticajnije medijske i izdavačke kuće proizvode više od 200 tekstova dnevno.
- Veliki broj tekstova otvara i mogućnost za plasiranje velikog broja banera i digitalnih oglasa.

Ovom okruženju najbrže su se prilagodili tzv. tabloidni mediji, dok ostali mediji u srpskom medijskom sistemu - lokalni, specijalizovani, istraživački - ne mogu da se takmiče na takvom tržištu. Ostali mediji koriste digitalno okruženje, pre svega, da bi došli do publike i prevazišli nedostatke zatvorenog i strogo kontrolisanog medijskog sistema.

Klasifikacija podataka u redakcijama

U svom radu mediji se susreću sa nekoliko ključnih tipova podataka, koji se razlikuju po poreklu, nivou kontrole koji redakcija nad njima ima i rizicima koje nose.

7 Klikbejt (engl. *clickbait*) je senzacionalistički naslov koji preuveličava, obmanjuje ili pogrešno predstavlja sadržaj članka. Cilj je veštačko privlačenje pažnje kako bi se korisnik naterao da klikne na link.

Podaci dobijeni od izvora su podaci nastali novinarskim i istraživačkim radom, za koje mediji snose punu etičku i pravnu odgovornost. To su, na primer, svedočanstva ili izjave dobijene direktno od izvora, podaci nastali pretragama registara i sudske dokumentacije ili upotrebom digitalnih alata za pretragu, kreiranje i analizu podataka. Standardi zaštite ove vrste podataka razrađeni su u odeljku o upotrebi podataka u kontekstu uredničkih odluka.

First party data (podaci prve strane) su podaci koje publika/korisnici svojevolljno dele, uz pristanak. Obično se nalaze na serverima i platformama samih medija, kojima mediji upravljaju i nad kojima imaju visok nivo kontrole. Ova vrsta podataka se ponekad zove i „zero party data (podaci nulte strane)“, upravo zbog svesnog pristanka i aktivnog učešća korisnika.

Second-party data (podaci druge strane) podrazumevaju deljenje podataka prve strane (*first party data*) između partnerskih organizacija. Ova vrsta razmene je u medijskom sektoru trenutno najređa. Primer ovakve saradnje bila bi razmena podataka o publici između dva medija - razmena podataka o pretplatnicima ukoliko oba medija zajednički razvijaju projekat *newsletter*-a.

Third party data (podaci treće strane) su podaci koje prikupljaju druge kompanije, organizacije i posrednici. Mediji nad njima obično imaju mali nivo kontrole, a ovakvi podaci dolaze sa bezbednosnim i reputacionim rizikom, uglavnom su obimni, nedovoljno selektivni, anonimizovani i dostupni u formatu koji određuju kompanije posrednici.

Podaci prve strane - najpoželjniji tip podataka

Tri vrste podataka se najčešće smatraju podacima prve strane: **kontakt podaci** (ime, prezime, imejl adresa, broj računa i sl.), **podaci o ponašanju publike** (IP adresa, broj poseta, posećene stranice, istorija kupovine, pretplate i donacija) i **podaci o preferencijama publike** (prikupljeni putem onlajn formulara, anketa, upitnika i kvizova).

Podaci prve strane su ključni podaci koje mediji zaista poseduju i nad kojima imaju kontrolu, i zato se smatraju „zlatnim standardom“. Trendovi pokazuju da će sve veći akcenat biti upravo na ovoj vrsti podataka, jer mnogo preciznije prikazuju preferencije publike od neselektivnih podataka koji stižu od posrednika. Uz to, zbog sve strožih regulatornih zahteva i razvoja veštačke inteligencije, mediji će sve više insistirati na prikupljanju i obradi ove vrste podataka, a sve manje na podacima treće strane.

Sve zajedno uvod je u globalni trend personalizacije informisanja, u kom će sadržaj medija biti sve više prilagođen svakom pojedinačnom korisniku i njegovim preferencijama.

Prikupljanje ove vrste podataka zahteva određenu infrastrukturu, potpunu transparentnost i jasnu svrhu. Mediji koji prikupljaju ovu vrstu podataka **moraju tražiti saglasnost korisnika** i jasno definisati namenu - da li će se podaci koristiti za slanje *newsletter*-a, prikupljanje donacija ili stimulisanje pretplate. Bez jasne namene i izričite saglasnosti, podaci mogu biti prikupljeni, ali beskorisni za donošenje uredničkih ili menadžerskih odluka, a njihova obrada nezakonita. Za učešće u deljenju podataka, mediji mogu korisnicima ponuditi pogodnosti: personalizovano iskustvo, manje oglasa ili mogućnost da predlažu teme istraživanja.

Podaci treće strane - „rupa“ u upravljanju

Mediji se u svom radu oslanjaju na veliki broj posredničkih servisa koji generišu obimne skupove podataka, a među kojima dominiraju servisi „Google“-a i „Meta“-e. Ove tehnologije se često nazivaju „digitalnim posmatračima“ jer im je svrha da prate ponašanje korisnika na internetu.

Mediji najčešće koriste:

Statističke i analitičke servise koji pružaju kvantitativne podatke o interakciji publike sa sajtom (broj poseta, dužina boravka, klikovi, podeljeni sadržaji).

Oglašivačke servise („Ads“) koji omogućavaju medijima da reklamiraju sopstveni sadržaj ili da zarađuju od komercijalnih oglasa i banera.

Embed-ovani sadržaj (od engl. *embed* - ugraditi, umetnuti) koji podrazumeva praksu direktnog umetanja postova sa društvenih mreža unutar novinarskih tekstova. Embedovi predstavljaju kod ili elemente ugrađene u internet stranicu koji omogućavaju prikazivanje sadržaja (video zapisa, mapa, objava) sa drugih sajtova. Oni omogućavaju da se sadržaj sa platformi poput „YouTube“-a, „Instagram“-a ili „X“-a direktno reprodukuje bez napuštanja trenutne stranice.

Posredničke platforme za newsletter, što su najčešće strani servisi poput „MailChimp“, „MailerLite“ i „Brevo“ koji omogućavaju kreiranje i slanje sadržaja.

Servise za komentarisanje koji su integrisani u sajtove, omogućavaju korisnicima da ostavljaju povratne informacije i diskutuju o medijskom sadržaju.

Svaki od ovih servisa prikuplja i obrađuje veliki broj podataka o publici, ali mediji nad njima nemaju dovoljnu kontrolu - niti znaju kako su podaci prikupljeni, niti u kojoj meri su korisnici dobrovoljno učestvovali u prikupljanju podataka. Najveći problem je što mediji vide *izlazni rezultat*, ali ne i *proces i metodologiju* prikupljanja i obrade. To nosi i određene rizike:

- Podaci su mahom anonimizovani i masovni, te daju ograničene uvide u trendove i mogu dovesti do pogrešnih odluka.
- Mnogi servisi funkcionišu bez jasnog odobrenja redakcije ili korisnika, što stvara „upravljačku prazninu“. Ova praznina nastaje kada se na sajtovima medija nalaze različiti servisi koji prikupljaju podatke, a redakcija nema pun uvid niti kontrolu nad tim procesima, nema jasnu internu politiku njihove primene niti razumevanje šta ovi servisi tačno rade sa podacima korisnika.

- Kada se koristi više različitih servisa, podaci često nisu međusobno usklađeni i teško ih je objediniti.
- Oslanjanje na podatke treće strane ponekad je etički upitno i nije u skladu sa standardima profesije.
- Korisnici su sve svesniji prava na privatnost i koriste alate koji blokiraju praćenje, što dovodi do podataka lošijeg kvaliteta.
- Algoritmi društvenih mreža su „nevidljivi urednici“ koji rade za interes platformi, a ne medija - favorizuju klikbejt i senzacionalizam, što dugoročno urušava brend ozbiljnog medija.

Treba imati u vidu i bezbednosni rizik: mogućnost da se neki od ovih servisa zaraze malverom⁸ i prenesu ga dalje na sajtove ili korisnike. Pored toga, samo jedan skandal u vezi sa curenjem podataka može imati dugoročne posledice po reputaciju medija i poverenje publike, uz sve strožu regulatornu praksu koja podrazumeva veće kazne i složene sudske postupke.

Upotreba podataka i saradnja sa publikom

U digitalnom okruženju podaci predstavljaju jedan od ključnih resursa za razvoj i održivost medija. Njihova vrednost ne ogleda se samo u analizi publike i unapređenju distribucije sadržaja, već i u mogućnosti da se kroz podatke bolje razumeju potrebe zajednice kojoj se medij obraća.

Sve više se razvijaju modeli koji kombinuju sistematsko upravljanje podacima sa aktivnijom saradnjom sa publikom. U takvom pristupu zajednica ne predstavlja samo pasivnog primaoca sadržaja, već može postati važan partner u procesu prikupljanja informacija, interpretacije poda-

8 Malver (engl. *malware*) je reč izvedena od dve reči – “Malicious Software”, i predstavlja svaki softver koji je napisan u maliciozne svrhe, odnosno koji ima cilj da nanese štetu računarskim sistemima ili mrežama.

taka i razvoja novih medijskih proizvoda. U nastavku su navedene ključne strategije, koje svaki medij treba da prilagodi sopstvenim resursima i potrebama.

Sistematizacija i upravljanje podacima

Prvi korak je razvoj sistema za centralizaciju i strukturiranje podataka, kako bi informacije bile dostupne, pretražive i ponovo upotrebljive. Sistematsko upravljanje podacima omogućava redakcijama da efikasnije organizuju sadržaj, prate tok informacija i dugoročno grade sopstvene baze znanja.

Prema „News Product Alliance“, mediji često ne znaju šta sve već imaju⁹. Strateški korak je uvesti proces „popisa podataka“ (*Data Census*) - redakcija, marketing i IT zajedno popisuju: gde se sve skupljaju podaci (CRM¹⁰, *newsletter* platforma, CMS¹¹, analitika sajta), ko ima pristup tim podacima (interni timovi ili eksterni saradnici) i kako se podaci „čiste“ (higijena podataka), **jer loši podaci vode do loših uredničkih odluka.**

Rad sa zajednicom

Savremeni digitalni mediji sve češće uključuju svoju publiku i širu zajednicu u proces kreiranja vesti i sadržaja. Zajednica može imati ulogu ko-kreatora sadržaja, ali i doprineti kao etički korektiv, izvor stručnog znanja ili ekspertska baza za određene teme. Pored toga, redakcije mogu razvijati

9 Više informacija dostupno na sledećem linku: <https://newsproduct.org/blog/how-to-structure-and-centralize-audience-data-for-a-strong-integrated-data-foundation>

10 CRM je skraćenica od engl. Customer Relationship Management i podrazumeva sistem za upravljanje odnosima sa korisnicima koji omogućava medijima da prate, analiziraju i koriste podatke o svojoj publici (npr. pretplatnici, članovi, donatori).

11 CMS je skraćenica od engl. Content Management System, a odnosi se na softver koji omogućava medijima da kreiraju i objavljuju sadržaj na veb sajtovima.

različite modele angažovanja publike, poput elemenata gejmfikacije¹² ili prepoznatljivih novinarskih „ličnosti“ koje funkcionišu kao brendovi unutar medija.

AI i upravljanje podacima

Razvoj veštačke inteligencije (engl. artificial intelligence - AI) otvara nove mogućnosti za analizu i upravljanje podacima u redakcijama. AI alati mogu pomoći u razumevanju potreba i ponašanja publike, optimizaciji distribucije sadržaja i organizaciji baza podataka. Posebnu vrednost imaju sistemi veštačke inteligencije prilagođeni specifičnim potrebama redakcije i njenim novinarskim procesima.

Razvoj novih proizvoda i formata sadržaja

Digitalni mediji sve više razvijaju fleksibilne forme sadržaja koje se mogu lako menjati i prilagođavati različitim platformama i potrebama publike. Takav pristup opisuje se kao „*liquid content*“ - sadržaj koji se kontinuirano ažurira, nadograđuje i prilagođava različitim kontekstima distribucije. To bi, na primer, značilo da se dugački tekst sa medijskog portala, lako pretvara u audio sadržaj prilagođen *podcast*-ima ili pak video sadržaj za društvene mreže. Paralelno sa tim, redakcije mogu razvijati specijalizovane publikacije ili tematske proizvode namenjene određenim segmentima publike.

AI u redakcijama

Novi krug promena u radu medija očekuje se sa uvođenjem AI, koja sve više pretenduje da bude osnovna infrastruktura digitalnog novinarstva. Kako

12 Gejmifikacija je termin nastao od engleske reči „gaming“, a podrazumeva kreiranje medijskog sadržaja koji u sebi ima elemente igranja igrice (na primer, osvajanje bodova, prelazak nivoa, različite vrste interakcije publike i sl.)

je pokazalo istraživanje BIRN- a¹³, postoje bar dva ključna tipa poslova koje AI preuzima:

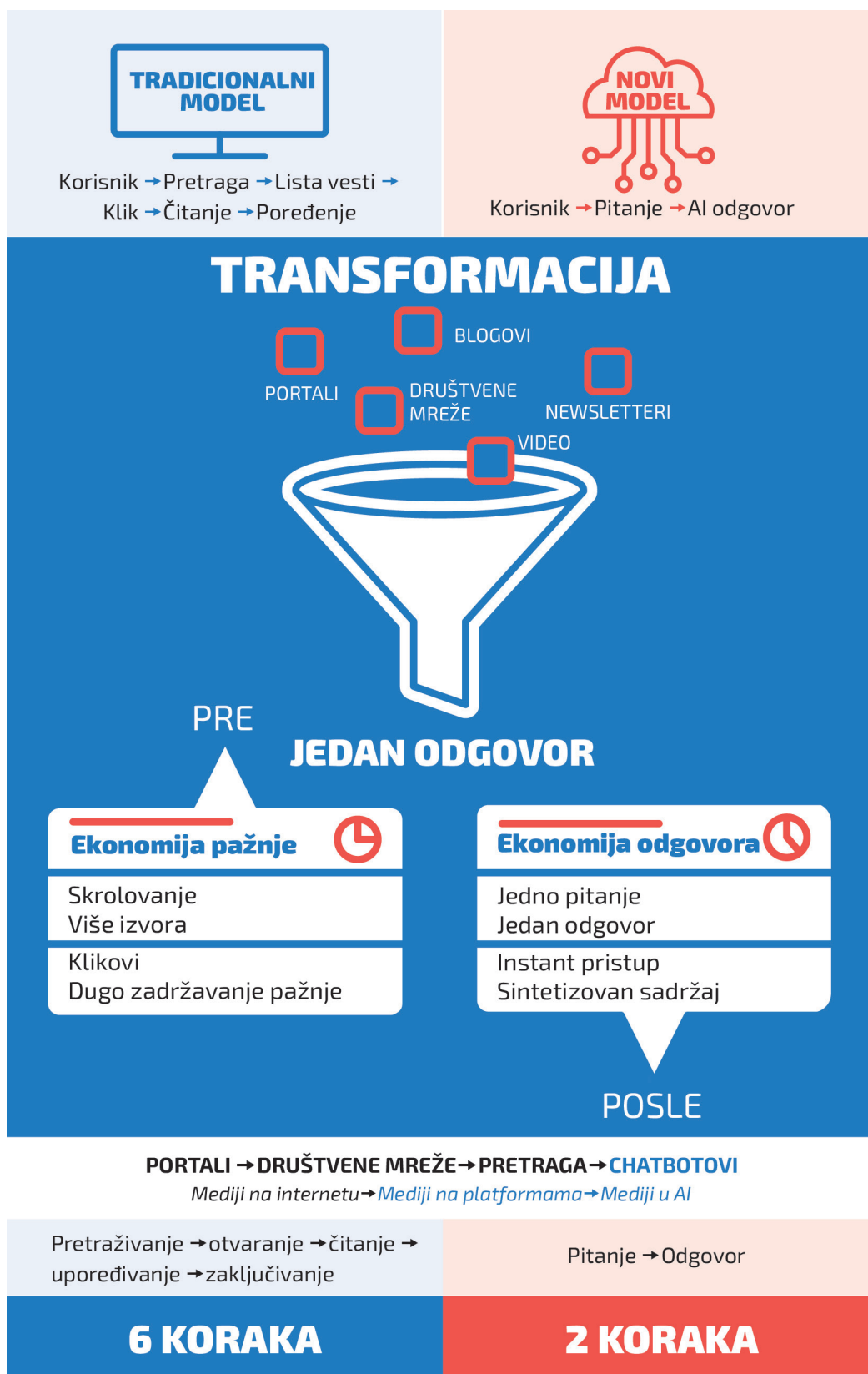
- **Rutinski poslovi** koji ne traže striktan urednički nadzor: prevod i lektura tekstova, sažimanje sadržaja, transkripcija, titlovanje, kreiranje AI-generisanih ilustracija, testiranje naslova, SEO (engl. Search Engine Optimization) odnosno optimizacija za pretraživače, generisanje glasa koji čita tekstualne sadržaje, predlog postova za društvene mreže.
- **Osetljiviji poslovi** koji zahtevaju veću pažnju novinara i urednika, a mahom se tiču podataka - njihovog sakupljanja, organizacije i analize.

Prema projekcijama Reuters Institute for the Study of Journalism¹⁴, do 2026. godine očekuju se tri ključna pomaka:

- **Dominacija „Answer Economy“ (ekonomije odgovora):** korisnici će sve manje skrolovati kroz liste vesti, a sve više tražiti direktne odgovore od *chatbotova*. Očekuje se otklon od „AI u medijima“ ka „medijima u AI“.
- **Pad tradicionalne SEO optimizacije:** optimizacija za pretraživače postaće optimizacija za AI modele. Poverenje će postati važnija metrika od klika, a biće izražena potreba za mnogo više „čistih“ podataka prve strane.
- **Hibridne redakcije:** više neće postojati jasna granica između IT tima i redakcije; novinari će morati da postanu „AI-pismeni“.

13 BIRN Srbije „Digitalna transformacija i veštačka inteligencija“: <https://serbia.osce.org/sites/default/files/f/documents/f/5/590435.pdf>; videti više i ovde: BIRN Srbija, „Veštačka inteligencija u redakcijama: Novinari u Srbiji nepripremljeni za tehnološke promene“: <https://birn.rs/vestacka-inteligencija-u-novinarstvu-u-srbiji/>

14 Više informacija je dostupno na linku: <https://reutersinstitute.politics.ox.ac.uk/journalism-media-and-technology-trends-and-predictions-2026>



AI treba da služi novinaru da oslobodi vreme za dubinska istraživanja i rad na terenu, a ne da zameni novinarski i urednički posao. Odgovornost za podatak ostaje isključivo na čoveku, bez obzira na to koji je alat korišćen za njegovu obradu. Kako bi se očuvao integritet novinarstva, BIRN je osmislio set internih protokola pri uvođenju AI alata¹⁵:

- Mediji ne koriste i ne razvijaju AI modele u saradnji sa privatnim kompanijama ukoliko takva saradnja zahteva deljenje neobjavljenih, osetljivih ili urednički poverljivih podataka.
- Razvoj internih ili prilagođenih AI rešenja dozvoljen je samo uz prethodnu formalnu procenu rizika, potpisane sporazume o obradi podataka i odobrenje glavnog urednika ili direktora medija.
- Eksterni partneri nikada ne mogu pristupiti izvorima, internim komunikacijama redakcije, nacrtima tekstova niti bilo kom sadržaju koji može ugroziti uređivačku autonomiju ili zaštitu izvora.
- Sa podacima o publici mediji postupaju sa dužnom pažnjom, u skladu sa internim politikama privatnosti koje su javno dostupne na sajtu.
- Podaci dobijeni od izvora dele se sa AI sistemima samo nakon prethodne provere i izričite saglasnosti novinara i urednika.
- Svi podaci koje samostalno generiše AI podležu proverbi od strane novinara i urednika pre nego što se mogu koristiti u redakcijskom radu.
- Pre upotrebe alata, redakcija proverava poreklo podataka na kojima su AI modeli obučeni.

15 Celokupne Smernice za upotrebu veštačke inteligencije u medijima dostupne su na linku: <https://birn.rs/o-birn-u/>

Deo II – Regulatorni okvir

Propisi i politike upravljanja podacima u medijima

Da bi se lakše razumelo poreklo pravila i obaveza za medije koje su predstavljene u prethodnom poglavlju, u ovom poglavlju je sistematizovan pravni okvir koji uređuje zaštitu podataka o ličnosti publike u onlajn prostoru.

Pre svega je važno napraviti razliku između:

- Obrade podataka o ličnosti publike (zaštita privatnosti korisnika medijskog sadržaja);
- Obrade podataka o ličnosti prilikom izveštavanja, odnosno kreiranja medijskih sadržaja (zaštita privatnosti onih o kojima se izveštava).

Najveći deo ove pravne analize odnosi se na pravila i obaveze onlajn medija prilikom obrađivanja podataka o ličnosti publike. U manjem delu na kraju ovog poglavlja biće predstavljen i pravni okvir koji uređuje zaštitu privatnosti onih o kojima se izveštava.

Zaštita privatnosti korisnika onlajn medija

Onlajn mediji su, u odnosu na podatke svojih korisnika, najčešće **rukovaoci**¹⁶ u smislu Zakona o zaštiti podataka o ličnosti (ZZPL)¹⁷, jer sami određuju svrhu i način obrade podataka - da li će uvoditi registraciju, koje podatke prikupljaju, koliko dugo ih čuvaju, da li uključuju analitiku i oglašne tehnologije. Upravo status rukovaoca povlači i punu pravnu odgovornost za zakonitost obrade.

Pored rukovaoca, ZZPL poznaje i druge uloge. Obradivač je subjekt koji obrađuje podatke u ime rukovaoca i po njegovim uputstvima - tipično eksterni pružalac usluga poput *hosting* kompanije, *newsletter* platforme ili analitičkog alata. Zajednički rukovaoci su dva ili više subjekata koji zajedno određuju svrhe i načine obrade, što može biti slučaj kada medij koristi određene platforme trećih strana na način koji prevazilazi puku tehničku uslugu. Razumevanje ovih uloga neophodno je za pravilnu primenu obaveza koje zakon nameće medijima, i služi kao osnov za sve što sledi u ovoj analizi.

To važi i kada se obrada odnosi na „obične“ posete sajtu i bez kreiranja naloga, jer čak i korisnik koji samo učita stranicu ostavlja za sobom podatke o ličnosti: IP adresu, informacije o uređaju i pregledaču, vreme i trajanje posete. **Medij te podatke prikuplja automatski, često i bez svesti korisnika da se to dešava, što znači da su obaveze iz ZZPL-a aktivirane već samim pristupom sajtu.** Medij je pri tome dužan da poštuje načela obrade podataka - to su osnovna pravila koja važe za svaku obradu, bez obzira na njenu svrhu ili obim, a obuhvataju između ostalog zakonitost, ograničenje svrhe, tačnost podataka, kao i obavezu da se obradom ne zadire u prava lica više nego što je neophodno. U skladu sa tim, obrada se mora ograničiti na ono što je nužno i razumno u odnosu na konkretnu svrhu.

16 Zakon o zaštiti podataka o ličnosti, član 4, stav 1, tačka 8.

17 „Sl. glasnik RS», br. 87/2018.

Korisno je od početka razlikovati tri tipa obrade. **Osnovna funkcionalna obrada** obuhvata ono što je potrebno da bi usluga radila, odnosno ograničena je na minimum podataka koji su neophodni za ostvarivanje svrhe (prikaz stranice, sesija prijave, isporuka *newsletter*-a, bezbednosna zaštita). **Analitička i marketinška obrada** ide korak dalje - meri ponašanje, segmentira publiku, gradi profil interesovanja i povezuje aktivnosti radi optimizacije sadržaja i monetizacije. Kod ovakve obrade je naročito važno da medij jasno odredi **pravni osnov** i pruži korisniku mogućnost za informisano donošenje odluka. **Obrada putem trećih strana** nastaje kada medij uključi spoljne alate (analitika, oglasne mreže, *embed*-ovani sadržaj, *newsletter* platforme) u svoj sadržaj. Ako treće lice obradu vrši u ime medija, ono je obrađivač,¹⁸ dok u pojedinim modelima može postojati i zajedničko određivanje svrha, kada se uspostavlja režim zajedničkih rukovalaca.¹⁹

Ovo je naročito važno kada medij ima profile na društvenim mrežama, jer se podaci publike tada obrađuju i na osnovu pravila funkcionisanja platforme. U kontekstu propisa EU, DSA dodatno uređuje obaveze platformi kao posrednika, ali ne menja činjenicu da medij i dalje snosi odgovornost za zakonitost i transparentnost obrade koju sam pokreće.

Vrste podataka koje mediji prikupljaju o korisnicima

Kao što je pojašnjeno u Delu I, onlajn mediji prikupljaju više različitih kategorija podataka, među kojima su i podaci o ličnosti.²⁰ Važno je imati u vidu da se podatkom o ličnosti smatra svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv - i tehnički identifikatori ili zapisi o ponašanju mogu omogućiti identifikaciju konkretnog lica. U tom smislu, nekoliko tipova podataka koje onlajn mediji prikupljaju jesu, ili mogu spadati u kategoriju podataka o ličnosti:

18 Zakon o zaštiti podataka o ličnosti, član 45.

19 Zakon o zaštiti podataka o ličnosti, član 43.

20 Zakon o zaštiti podataka o ličnosti, član 4, stav 1, tačka 1.

- **Identifikacioni i kontakt podaci** koje korisnik najčešće sam ostavlja: ime i prezime, korisničko ime, imejl adresa, broj telefona, kao i podaci o nalogu i pretplati (adresa za račun, podaci o plaćanju).
- **Podaci o ponašanju i navikama čitanja** koji nastaju tokom korišćenja sajta: posećene stranice, dužina boravka, klikovi, praćene rubrike, istorija pretraga, indikatori skrolovanja i interakcije sa video sadržajem. Ovi podaci se koriste za uredničku analitiku, optimizaciju sajta i oglašavanje, a mogu prerasti u profilisanje²¹ ako se povezuju kroz vreme i različite uređaje.
- **Tehnički podaci** koji se prikupljaju automatski: IP adresa, tip uređaja, operativni sistem i pregledač, rezolucija ekrana, jezik i vremenska zona, identifikatori sesije, logovi o pristupu i bezbednosni zapisi.

U praksi se ove kategorije najčešće prikupljaju kroz sledeće mehanizme: **kolačiće**²² i slične tehnologije (pamte podešavanja, mere posećenost, prate ponašanje i omogućavaju oglasne funkcije); **newsletter i paywall sisteme** (podaci o prijavi/odjavi, preferencije, statistike otvaranja, status pretplate, autentifikacioni zapisi); i **komentare i sadržaj koji generišu korisnici** (sadržaj komentara, podaci profila, metapodaci neophodni za moderaciju i bezbednost).

Medij sam odlučuje koje će podatke obrađivati i u koje svrhe. Deo podataka je tehnički nužan da bi sajt funkcionisao, dok se drugi prikupljaju radi unapređenja poslovanja, analitike i monetizacije - pa zato zahtevaju pažljivo obrazloženje, jasna obaveštenja i odgovarajući pravni osnov.

21 Zakon o zaštiti podataka o ličnosti, član 4, stav 1, tačka 5.

22 Pored Zakona o zaštiti podataka o ličnosti, relevantan je i Zakon o elektronskim komunikacijama (član 160).

Obrada podataka može se zasnivati samo na jednom od zakonom propisanih osnova.²³ U domaćem pravu, medij može obradu podataka o korisnicima da vrši samo uz odgovarajući pravni osnov iz ZZPL-a, pri čemu su u praksi najčešći: izvršenje ugovora, legitiman interes i saglasnost.

Kod sistema pretplata i članstava, pravni osnov je najčešće **izvršenje ugovora**.²⁴ U praksi to znači da medij treba da obrađuje samo one podatke koji su stvarno neophodni da bi se ugovorena usluga pružila. Sve dodatno - napredna personalizacija ili marketinško profilisanje - po pravilu zahteva dodatni pravni osnov.

Legitimni interes²⁵ se najčešće koristi za obradu u vezi sa bezbednošću i integritetom sistema, sprečavanjem zloupotreba, osnovnom statistikom i unapređenjem usluge - ali samo u meri u kojoj takva obrada ne „preteže” nad interesima i slobodama korisnika. **Korisnik ima pravo da uloži prigovor na ovakvu obradu**. Ukoliko je reč o obradi u svrhe direktnog oglašavanja, prigovor ima neposredno dejstvo - medij podatke više ne sme da obrađuje u te svrhe.²⁶

Saglasnost²⁷ je tipičan osnov za obradu koja nije nužna za pružanje usluge - *newsletter* (kada nije deo ugovorne usluge), targetirano oglašavanje i korišćenje naprednih kolačića. ZZPL zahteva da saglasnost bude dobrovoljna, određena, informisana i nedvosmislena, i da se može opozvati u svakom trenutku. Posebno je važno da pružanje usluge ne bude uslovljeno saglasnošću koja nije neophodna.²⁸

23 Zakon o zaštiti podataka o ličnosti, član 12.

24 Zakon o zaštiti podataka o ličnosti, član 12, stav 1, tačka 2.

25 Zakon o zaštiti podataka o ličnosti, član 12, stav 1, tačka 6.

26 Zakon o zaštiti podataka o ličnosti, član 37, stav 2 i 3.

27 Zakon o zaštiti podataka o ličnosti, član 12, stav 1, tačka 1.

28 Zakon o zaštiti podataka o ličnosti, član 15.

Kada je reč o kolačićima i sličnim tehnologijama, Zakon o elektronskim komunikacijama²⁹ polazi od toga da se isti ne smeju koristiti bez prethodnog pristanka korisnika, osim onih koji su striktno neophodni za funkcionisanje sajta.³⁰

U kontekstu EU, DSA dodatno postavlja standarde u pogledu dizajna interfejsa i oglašavanja, uključujući zabranu određenih manipulativnih obrazaca, obaveze transparentnosti oglasa i ograničenja oglašavanja zasnovanog na profilisanju, posebno kada su u pitanju maloletnici.³¹ U Srbiji je ova oblast trenutno delimično regulisana sektorskim zakonima, a očekuje se i usvajanje posebnog zakona po ugledu na DSA, koji bi ova pravila dodatno uredio.

Transparentnost i informisanje korisnika

Zakonnost obrade u praksi zavisi i od toga da li je korisnik blagovremeno, jasno i potpuno informisan. Transparentnost podrazumeva da medij saopšti najmanje: ko obrađuje podatke (identitet rukovaoca/medija i kontakt), u koje svrhe, koje vrste podataka se prikupljaju, na kom pravnom osnovu, kome se podaci otkrivaju, koliko dugo se čuvaju, i da li se prenose u inostranstvo.³²

U praksi se transparentnost najčešće ostvaruje kroz **politiku privatnosti**, **politiku kolačića** i prateća **obaveštenja o obradi podataka**. Da bi bila delotvorna, ova dokumenta moraju biti lako dostupna, jasna, napisana razumljivim jezikom i redovno ažurirana, posebno kada se uvode nove tehnologije ili nove svrhe obrade.

Kvalitet politike privatnosti prepoznaje se po tome da li je strukturirana po svrhama obrade (funktionalno, analitika, marketing, komentari), da

29 „Sl. glasnik RS», br. 35/2023.

30 Zakon o elektronskim komunikacijama, član 160, stav 4 i 5.

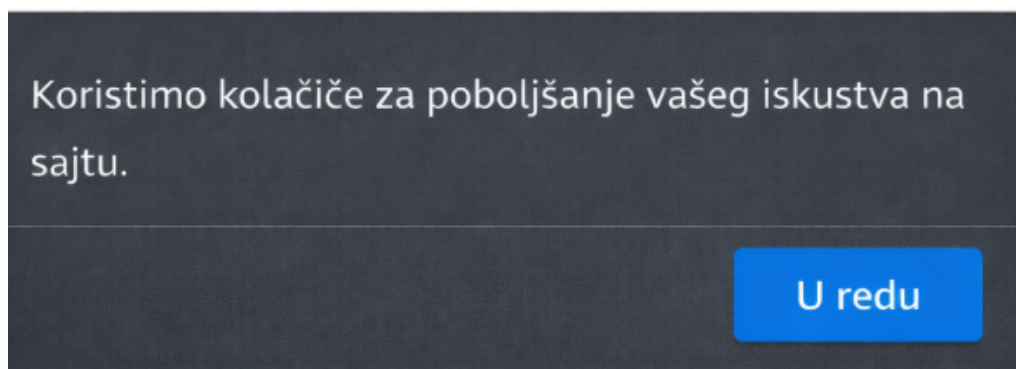
31 Zakon o digitalnim uslugama Evropske unije, član 25, 26 i 28.

32 Zakon o zaštiti podataka o ličnosti, članovi 21, 22, 23.

li jasno navodi pravne osnove, kategorije primalaca podataka, rokove čuvanja podataka i prava korisnika uz konkretna uputstva za njihovo ostvarivanje.

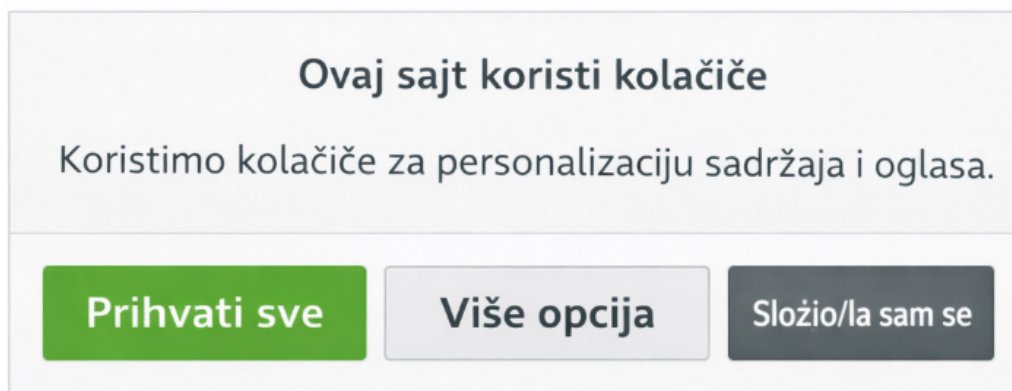
Kod politike kolačića i mehanizama upravljanja saglasnostima, **ključno je da korisnik dobije stvarnu kontrolu nad tehnologijama praćenja**. Mehanizam upravljanja saglasnošću treba jasno da razlikuje nužne od analitičkih i marketinških kolačića, i da obezbedi jasne, razgraničene i trajno dostupne opcije prihvatanja i odbijanja, kao i mogućnost naknadne promene izbora.³³

Najčešći problem u praksi je razlika između formalne i stvarne transparentnosti - dokumenti postoje, ali su napisani tako da korisnik ne može da razume aspekte obrade, ili su kontrole saglasnosti dizajnirane tako da podstiču „prihvati sve“, dok je odbijanje teže dostupno. U takvim slučajevima korisnik može biti formalno obavešten, ali suštinski nema informisan izbor niti realnu kontrolu.



Ilustracija 1 Primer nedovoljno informativnog banera

33 U skladu sa pravilima izloženim u odeljku „Pravni osnov obrade podataka korisnika“.



Ilustracija 2 Primer nedovoljno informativnog banera



Ilustracija 3 Primer banera koji korisnika informiše i daje mogućnost kontrole nad obradom podataka

Upravljanje podacima i interne prakse medija

Pravni okvir zaštite podataka ne svodi se na objavljivanje politike privatnosti, već podrazumeva i unutrašnju organizaciju rada: jasna pravila o tome ko sme da pristupa podacima, u koje svrhe, kako se postupak obrade dokumentuje i kako se obezbeđuje usklađenost i zaštita. ZZPL polazi od obaveze da rukovalac preduzme odgovarajuće tehničke, organizacione i kadrovske

mere i da to može da predoči.³⁴ Pri tome, zakon ne definiše unapred šta se smatra „odgovarajućim”, već se to procenjuje od slučaja do slučaja, u zavisnosti od prirode podataka koji se obrađuju, obima obrade, mogućih rizika po prava korisnika i raspoloživih resursa rukovaoca. Zakon propisuje i obavezu dokazivanja da ove mere postoje - u slučaju nadzora, pri tužbe ili drugog postupka pred nadležnim organom, rukovalac mora biti u mogućnosti da dokumentuje i obrazloži preuzete mere.

Ključni deo interne prakse su **interne procedure i jasno definisane uloge**, pravila za uvođenje i korišćenje alata trećih strana, kao i standardi bezbednosti - upravljanje lozinkama, dvofaktorska autentifikacija za administraciju sajta i naloge na platformama, procedure za pristup bazama pretplatnika i *newsletter* alatima. Ove mere se u ZZPL-u nadovezuju na zahtev da se zaštita podataka obezbeđuje i kroz organizaciju procesa, posebno kada se uvode nove tehnologije ili modeli obrade.³⁵

ZZPL predviđa i obavezu vođenja **evidencija radnji obrade**, koje u praksi predstavljaju osnovni alat kontrole - sistematično se beleži koje se radnje obrade sprovode, u koje svrhe, koje kategorije podataka su obuhvaćene, kome se podaci otkrivaju, koliko se čuvaju i koje su mere zaštite primenjene.³⁶

Posebno je važno **upravljanje pristupom podacima u redakcijama**. Pristup bi trebalo ograničiti na princip nužnosti, uz jasna pravila o tome ko ima administratorska prava i ko može da izvozi baze podataka.³⁷

Kod **čuvanja podataka i rokova brisanja**, polazno pravilo je da se podaci ne čuvaju duže nego što je potrebno za svrhu zbog koje su prikupljeni - što zahteva unapred definisane rokove za brisanje, posebno za logove, analitiku, marketinške liste i podatke o aktivnostima korisnika.³⁸

34 Zakon o zaštiti podataka o ličnosti, član 41.

35 Zakon o zaštiti podataka o ličnosti, član 42.

36 Zakon o zaštiti podataka o ličnosti, član 47.

37 Zakon o zaštiti podataka o ličnosti, član 50.

38 Zakon o zaštiti podataka o ličnosti, član 5.

Na kraju, **upravljanje incidentima i povredama podataka** mora biti operativno - medij treba da ima internu podelu uloga članova tima, interne procedure upravljanja i zaštite podacima, da dokumentuje incident i sprovede procenu rizika. Interna podela uloga znači da svaki član tima unapred zna ko prvi reaguje, ko obaveštava nadređene i ko komunicira sa spoljnim stranama. Interne procedure treba da predvide konkretne korake za moguće scenarije (poput hakerskog napada ili gubitka uređaja sa podacima publike) i da se redovno ažuriraju. Dokumentovanje incidenta obuhvata pisano beleženje okolnosti povrede, pogođenih kategorija podataka i preduzetih mera, što u slučaju nadzora služi kao dokaz odgovornog postupanja. Sprovođenje procene rizika podrazumeva utvrđivanje da li povreda može proizvesti rizik po prava korisnika, što određuje da li nastaje obaveza obaveštavanja Poverenika i samih lica čiji su podaci povređeni.



ZZPL propisuje obavezu **obaveštavanja Poverenika o povredi podataka** koja može da proizvede rizik po prava fizičkih lica (po pravilu u roku od 72 časa od saznanja), kao i obaveštavanje lica na koja se podaci odnose kada povreda može da proizvede visok rizik.³⁹ U kontekstu rada onlajn medija, obaveza obaveštavanja Poverenika nastaje u situacijama kao što su: neovlašćeni pristup bazi pretplatnika ili registrovanih korisnika, cure-nje podataka o korisnicima usled bezbednosnog propusta na sajtu ili kod eksternog pružaoca usluga, gubitak ili krađu uređaja na kojima se nalaze lični podaci publike, kao i slučajeve kada su podaci korisnika slučajno pro-sledeni pogrešnom primaocu.

Prava korisnika medijskih sadržaja (publike) i njihova ostvarivost u praksi

ZZPL garantuje korisnicima niz prava u odnosu na rukovaoce. Korisnici ova prava ostvaruju podnošenjem **zahteva** mediju, a medij je dužan da po njima postupi u roku od 30 dana (ili 90 dana za složene zahteve). Meha-nizmi za ostvarivanje ovih prava moraju biti jednostavni i lako dostupni.⁴⁰ Kada medij ne postupi po zahtevu, ZZPL predviđa pravo na pritužbu Pove-reniku i mogućnost sudske zaštite.⁴¹

Pravo na pristup obuhvata potvrdu da li se podaci obrađuju, uvid u podatke i dobijanje kopije, uz informacije o svrsi, primaocima, rokovima čuvanja i drugim pravima lica.⁴²

Pravo na brisanje omogućava korisniku da od medija zatraži da obriše podatke koje o njemu čuva. Na primer, da ukloni njegove kontakt podatke sa *newsletter* liste, da obriše nalog koji je kreirao na sajtu, ili da izbriše komentare koje je ostavio uz identifikacione podatke profila. Pravo na

39 Zakon o zaštiti podataka o ličnosti, članovi 52 i 53.

40 Zakon o zaštiti podataka o ličnosti, član 21, stav 3.

41 Zakon o zaštiti podataka o ličnosti, član 82.

42 Zakon o zaštiti podataka o ličnosti, član 26.

brisanje može se ostvariti kada podaci više nisu potrebni za svrhu zbog koje su prikupljeni, kada je korisnik povukao saglasnost na osnovu koje se obrada vršila, ili kada su podaci nezakonito obrađivani.⁴³

Pravo na prenosivost omogućava dobijanje podataka u strukturisanom i mašinski čitljivom formatu, kao i neposredan prenos drugom rukovaocu - ali samo kada je obrada zasnovana na saglasnosti ili ugovoru i vrši se automatizovano.⁴⁴ Na primer, kada korisnik želi da dobije svoje podatke sa *newsletter* platforme jednog medija u formatu koji može direktno da uveze u drugu platformu ili servis koji koristi.

Pravo na prigovor je posebno važno kada medij obrađuje podatke na osnovu legitimnog interesa (npr. određene vrste analitike, unapređenje usluge). Korisnik može u svakom trenutku uložiti prigovor, a medij je dužan da prekine obradu, osim ako dokaže da postoji pretežniji legitimni interes.⁴⁵ U kontekstu onlajn medija, pravo na prigovor najčešće će biti relevantno kada medij obrađuje podatke korisnika u svrhe direktnog oglašavanja ili analitičkog profilisanja. Na primer, kada portal prati ponašanje korisnika kako bi mu prikazivao targetirane oglase, ili kada na osnovu istorije čitanja gradi profil interesovanja i koristi ga u marketinške svrhe. Korisnik može uložiti prigovor i zahtevati da medij prestane sa takvom obradom.

Za medije je posebno važno pravilo koje se odnosi na **obradu u svrhe direktnog oglašavanja**. Kada se podaci obrađuju radi direktnog marketinga, uključujući profilisanje povezano sa takvim oglašavanjem (na primer - slanje *newsletter*-a ili targetiranih oglasa), prigovor korisnika ima neposredno dejstvo - medij od tog trenutka više ne sme da obrađuje podatke u te svrhe. Zato je u praksi ključno da mediji obezbede jasnu i jednostavnu mogućnost podnošenja prigovora (npr. link za odjavu, podešavanja privatnosti, kontakt), kao i interni mehanizam koji garantuje da se prigovor odmah

43 Zakon o zaštiti podataka o ličnosti, član 30.

44 Zakon o zaštiti podataka o ličnosti, član 36.

45 Zakon o zaštiti podataka o ličnosti, član 37, stav 1.

sprovodi u svim relevantnim sistemima i kod trećih strana uključenih u marketing.⁴⁶

U praksi je korisno da medij odredi jednu jasnu kontakt tačku (posebnu imejl adresu ili formular) i jasno podeli interne uloge - ko prima zahtev, ko proverava baze i alate, ko priprema odgovor. Kod medija koji imaju veći obim obrade ili redovno koriste alate praćenja, preporučljivo je imenovanje **lica za zaštitu podataka o ličnosti**,⁴⁷ koje koordiniše usklađenost, prati rizike, učestvuje u proceni novih tehnologija i služi kao kontakt za korisnike i Poverenika.

Bezbednost podataka

Bezbednost podataka u digitalnom mediju nije samo tehničko pitanje, **to treba da bude ključni deo uredničke i menadžerske odgovornosti**. Kako su podaci postali „nova valuta“, tako su i rizici od njihovog gubitka ili zloupotrebe postali direktna pretnja kredibilitetu medija. Iako mediji nisu primarno IT kompanije i moraju se oslanjati na eksterne partnere, od njih se očekuje da pokažu određeni nivo profesionalne odgovornosti u digitalnom dobu, jer je odgovorno upravljanje podacima produžetak novinarske etike.

ZZPL zahteva da rukovalac primeni odgovarajuće **tehničke i organizacione mere** kako bi obezbedio nivo bezbednosti primeren riziku.⁴⁸ To u praksi uključuje: kontrolu pristupa podacima, enkripciju gde je primerno, vođenje i nadzor logova pristupa, redovno ažuriranje sistema, rezervne kopije i procedure za povratak sistema, kao i obuku zaposlenih i jasna interna pravila postupanja.

Rizici su često izraženiji kod malih i lokalnih medija koji imaju ograničene resurse, i u situacijama kada su IT usluge poverene eksternim subjektima.

46 Zakon o zaštiti podataka o ličnosti, član 37, stav 2 i 3.

47 Zakon o zaštiti podataka o ličnosti, član 56.

48 Zakon o zaštiti podataka o ličnosti, član 50.

Čak i kada eksterni provajder (u ulozi obrađivača) obrađuje podatke u ime medija, medij kao rukovalac i dalje snosi odgovornost za zakonitost i bezbednost obrade.⁴⁹

Interna pravila i bezbednosna kultura

Redakcije moraju razviti bezbednosnu kulturu kroz uspostavljanje različitih nivoa pristupa podacima, naročito ličnim podacima, podacima izvora ili posebno osetljivim podacima. Nivoi pristupa mogu se ograničiti na osnovu opisa posla - na primer, samo marketing tim vidi podatke o pretplatnicima, a istraživački tim samo svoje izvore.

„Digitalna higijena“ podrazumeva i obaveznu upotrebu sigurnih aplikacija, enkripcije, dvostruke autentifikacije i drugih dostupnih tehničkih rešenja. Preporučuju se i povremena revizija internih pravila i redovne edukacije zaposlenih.

Tehničke mere i testiranje novih alata

Pre nego što se novi alat (naročito AI alat) uvede u svakodnevni rad, on mora proći kroz tzv. „*sandbox*“ testiranje - izolovanu sredinu gde se proverava kako alat tretira podatke pre nego što mu se dopusti pristup glavnim sistemima redakcije. U ovoj fazi potrebna je saradnja IT stručnjaka, novinara i pravnika kako bi se procenili tehnički, etički i pravni rizici.

Preporučuje se i redovni monitoring podataka koji odlaze sa sajta ili na njega dolaze, kao i praćenje netipičnih ponašanja na nalogima društvenih mreža, kako bi se na vreme reagovalo u slučajevima digitalnih napada.

49 Zakon o zaštiti podataka o ličnosti, član 45.

Revizija ugovornih obaveza i dobavljača

Brojni mediji u Srbiji koriste eksterne pružaoce usluga za *hosting*, *newsletter* servise ili održavanje sajta. Preporučena mera zaštite je redovna revizija ugovora i provera u kojoj meri pružaoci usluga i dalje ispunjavaju bezbednosne standarde. Potrebno je ograničiti broj pružalaca usluga (što je manje posrednika, manji je prostor za napad), kao i propisati strožije ugovorne klauzule koje garantuju da se podaci publike neće deliti sa trećim licima bez izričite dozvole.

Upravljanje povredama podataka

U slučaju **povrede podataka** (curenje, neovlašćeni pristup, gubitak uređaja), ZZPL propisuje obavezu procene rizika i, kada su ispunjeni uslovi, obaveštavanja Poverenika i/ili lica na koja se podaci odnose, kao i dokumentovanja povrede i preduzetih mera.⁵⁰ Odgovornost se ne završava reagovanjem na incident, već uključuje transparentno postupanje, ograničavanje štete i uvođenje mera kako bi se povreda sprečila u budućnosti.

Nadzor i regulatorni okvir

U oblasti zaštite privatnosti korisnika onlajn medija, centralnu ulogu ima **Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti**, kao nadzorni organ za primenu ZZPL-a. Poverenik postupa po pritužbama građana i sprovodi nadzor nad rukovaocima i obrađivačima, uz inspeksijska ovlašćenja i ovlašćenje da izriče korektivne mere radi unapređenja zaštite podataka prilikom obrade.⁵¹ Za povrede ZZPL-a propisane su novčane kazne za pravna lica u rasponu od 50.000 do 2.000.000 dinara.⁵²

50 Zakon o zaštiti podataka o ličnosti, članovi 52 i 53.

51 Zakon o zaštiti podataka o ličnosti, članovi 78–79 i 82–84.

52 Zakon o zaštiti podataka o ličnosti, član 95.

Paralelno, za rad medija u onlajn okruženju i zaštitu privatnosti publike onlajn medija koji se odnosi na elektronsku privatnost (kolačići i slične tehnologije), relevantan je Zakon o elektronskim komunikacijama. **Regulatorno telo za elektronske komunikacije (RATEL)** obavlja stručni nadzor, dok inspekcijski nadzor vrši nadležno ministarstvo preko **Inspektora elektronskih komunikacija**.⁵³

Pored formalnih mehanizama, relevantan je i **Savet za štampu** kao samoregulatorno telo. Savet postupi po žalbama povodom kršenja profesionalnih i etičkih standarda, uključujući i povrede privatnosti u sadržaju, poput neopravdanog zadiranja u privatni život, objavljivanja privatnih informacija bez pristanka ili identifikovanja lica koja imaju pravo na zaštitu. Ovaj mehanizam ne zamenjuje postupanje pred Poverenikom kada je reč o obradi podataka, ali može biti važan kanal za utvrđivanje profesionalne odgovornosti.

Nalazi analize prakse

Uporedna iskustva i primeri dobre prakse

Uporedne prakse upravljanja podacima korisnika od strane medija razlikuju se u zavisnosti od regulatornog okvira, ali i etičkih standarda i poslovnih pristupa redakcija. Mediji koji posluju na teritoriji EU primenjuju standarde predviđene GDPR-om i ePrivacy direktivom. Međutim, neki mediji, uključujući i one van EU tržišta, primenjuju i striktnije standarde od zakonskih minimuma, u nameri da zadrže ili izgrade poverenje publike - radi se uglavnom o medijima sa uže definisanom, vrednosno orijentisanom publikom, koja ceni etičnost u poslovanju i često je spremna da za nju plati ili donira. U nastavku je nekoliko primera dobrih uporednih praksi medija u pogledu upravljanja podataka korisnicima.

53 Zakon o elektronskim komunikacijama, članovi 161 i 163.

Britanski *The Guardian*⁵⁴ praktikuje transparentno informisanje čitalaca o upravljanju njihovim podacima, kao i primenu pristupa „privatnost po dizajnu“ (*Privacy by Design*). Umesto komplikovanih politika privatnosti, razvili su video sadržaje⁵⁵ i infografike kako bi što jednostavnije objasnili čitaocima svoje prakse.

Američki *The New York Times*⁵⁶ postepeno je ukinuo oslanjanje na kolačiće trećih strana i prešao na kontekstualno oglašavanje,⁵⁷ što znači da oglase plasiraju na osnovu sadržaja koji čitate, a ne na osnovu vašeg ličnog profila i istorije pretraživanja.

Financial Times primenjuje pristup zasnovan na privatnosti u oglašavanju, u nameri da pomiri prednosti ciljanog oglašavanja, sa zahtevima zaštite privatnosti korisnika. Tako, umesto praćenja šta čitalac radi na internetu, Financial Times primenjuje tzv. kontekstualno oglašavanje, koje usklađuje oglase sa sadržajem članka koji se čita - bez potrebe za ličnim podacima. Ovakvo oglašavanje može biti korisna alternativa koja se fokusira na prikazivanje oglasa na osnovu sadržaja veb stranice, a ne ponašanja korisnika. Takođe, rizici korišćenja alata za praćenje, uključujući i kolačiće trećih strana na portalu, umanjeni su primenom niza zaštitnih mera. One uključuju protokole o bezbednosti podataka, poput primene enkripcije, „firewalls“ zaštitnih sistema, kao i striktnu kontrolu pristupa podacima. Takođe, prema dostupnim informacijama,⁵⁸ vrše se redovne revizije bezbednosnih procedura, obuka zaposlenih, kao i primena minimizacije podataka i sigurnih sistema čuvanja i prenosa. Dostupne politike privatnosti i kolačića na jasan i detaljan način informišu korisnike o vrstama podataka koji se prikupljaju, njihovim izvorima, rokovima čuvanja. Posebna

54 The Guardian, <https://www.theguardian.com/europe>

55 The Guardian's privacy policy – video, <https://www.theguardian.com/info/video/2019/sep/12/the-guardians-privacy-policy-video>

56 The New York Times, <https://www.nytimes.com/>

57 Exclusive: New York Times phasing out all 3rd-party advertising data, Axios, 2020.

58 Understanding Financial Times Delivery: [Where and How to Get Your Daily News - Hedge Think](#)

pažnja obraća se na bezbednost finansijskih informacija pretplatnika, i primenu sigurnih sistema plaćanja.

Javni servisi u skandinavskim zemljama (poput norveškog **NRK**⁵⁹) i Švajcarskoj (**SRG SSR**⁶⁰) predvode pokret „Public Service Data“ - podatke građana tretiraju kao javno dobro. NRK je razvio stroge protokole po kojima se podaci prikupljeni putem njihovih aplikacija ne smeju koristiti za komercijalno profilisanje, već isključivo za personalizaciju javnog sadržaja. Ovi javni servisi koriste minimalan broj treкера, odnosno alata za praćenje ponašanja publike, u poređenju sa komercijalnim portalima.⁶¹

Prakse i iskustva u Srbiji

Postupanje medija u Srbiji u pogledu upravljanja podacima korisnika retko je u fokusu debate o stanju medijskog ekosistema, pre svega zbog niza problema sa kojima se mediji danas suočavaju. **Indeks privatnosti u medijima (IPM)**, koji SHARE fondacija sprovodi od 2021. godine, jedan je od retkih istraživačkih instrumenata na osnovu koga se mogu pratiti prakse i trendovi u ovoj oblasti.

Nalazi indeksa za 2021, 2022. i 2024. godinu⁶² ukazuju na trend koji je označen kao „spor i neravnomeran napredak“. Dok se tehnička usklađenost popravljja, suštinska zaštita čitalaca na najposećenijim portalima ostaje na veoma niskom nivou. I pored činjenice da većina analiziranih stranica⁶³ ima objavljene politike privatnosti, ti dokumenti su često generički, preobimni i ne odražavaju stvarne procese obrade podataka. Dalje, većina

59 About NRK, <https://www.nrk.no/about/>

60 SRG SSR, <https://www.srgssr.ch/en/home>

61 EBU Annual Report 2024–2025, <https://annual-report-2025.ebu.ai/>

62 Nalazi Indeksa privatnosti medija dostupni su na: <https://indeks.onlajnmediji.rs/>

63 U okviru IPM za 2021. godinu analizirano je 50 medija, za 2022. godinu 49, a za 2024. godinu 50 medija.

medija i dalje koristi „zidove kolačića“⁶⁴ koji primoravaju korisnike da prihvate praćenje kako bi pristupili sadržaju - što je suprotno načelu slobodnog pristanka.

U IPM za 2024. godinu uočen je obrazac diskriminatornog postupanja prema korisnicima van teritorije EU. Portali poput Blica i Kurira nude bolju zaštitu i jasnije opcije upravljanja kolačićima posetiocima iz EU nego onima iz Srbije - što govori da je motivacija za usklađenost pre regulatorna pretnja nego stvarna briga za privatnost korisnika.

Paradoksalno, manji, uglavnom lokalni i neprofitni mediji sa ograničenim dosegom imaju transparentnije politike i minimalno koriste invazivne alate za praćenje publike. U 2024. godini najbolje rangirani bili su Moj Bečej, Kruševac press, Magločistač, 021, Kolubarske i Kragujevačke. Na začelju su kontinuirano najposećeniji komercijalni portali: Politika, Blic, Alo, Informer i Republika.

Ovakvo stanje može se delom obrazložiti i finansijskim aspektima, i ranjivostima medija u Srbiji. Manji mediji koji se finansiraju iz projekata ili donacija često nemaju imperativ masovnog prikupljanja podataka za reklame, što im omogućava da budu etičniji u pogledu privatnosti. Treba, doduše, naglasiti da se ovakav nalaz odnosi na stanje pre 2025. godine, tj. pre značajnog smanjenja donatorskih sredstava namenjenih (između ostalog i) medijima u Srbiji. Sa druge strane, veliki portali koji su izgubili prihode od tradicionalnog oglašavanja, upravljanje podacima posmatraju kao resurs za preživljavanje na tržištu, a ne kao pravno i etičko pitanje.

Nalazi Indeksa ukazuju i na sistemske probleme u sektoru: mediji u Srbiji duboko su integrisani u globalni sistem *AdTech*-a (reklamnih tehnologija). Njihov poslovni model oslanja se na maksimalno prikupljanje podataka

64 „Cookie wall“ (ili „zid kolačića“) je iskaćući prozor ili baner na sajtu koji onemogućava pristup sadržaju dok korisnik ne prihvati sve kolačiće za praćenje i prikupljanje podataka. Za razliku od banera „saglasnosti“ koji omogućavaju i odbijanje kolačića, ovaj pristup „uzmi ili ostavi“ uslovljava korišćenje sajta davanjem potpune saglasnosti..

radi prodaje oglasnog prostora, što je u direktnom konfliktu sa privatnošću. Dodatno, većina podataka čitalaca iz Srbije odlazi u inostranstvo (najviše u Nemačku, gde se hostuje 17 od 50 analiziranih sajtova), što komplikuje pravnu zaštitu i nadzor.

Analiza odgovora na upitnik⁶⁵ koji je upućen medijima za potrebe izrade ove analize pokazuje zabrinjavajući nivo neznanja o sopstvenim praksama. Gotovo četvrtina učesnika ne zna koje podatke prikuplja od svoje onlajn publike, a trećina ne zna koje vrste kolačića se koriste na sajtu. Oko 35% ispitanih ne zna koje treće strane imaju pristup podacima njihove publike. Samo petina redakcija ima razvijene procedure u slučajevima povrede podataka, a gotovo 62% nema interne politike o unosu podataka u komercijalne AI sisteme. Kao prioritetnu potrebu, više od 60% učesnika navodi jačanje kapaciteta u oblasti pravnih obaveza i informacione bezbednosti.

Obrade podataka o ličnosti prilikom izveštavanja - Balans između prava na privatnost i javnog interesa

U medijskom izveštavanju u Srbiji uočljivo je kršenje prava na privatnost na dnevnom nivou. Monitoring izveštaji BIRN-a i Partnera Srbija pokazuju da se pravo na privatnost u redovnom medijskom izveštavanju krši oko dva puta dnevno,⁶⁶ dok u periodima društvenih nestabilnosti, političkih kriza ili traumatičnih događaja broj prekršaja značajno raste.⁶⁷

65 Upitnik je popunilo 34 predstavnika medija koji imaju različite uloge unutar redakcija (urednici, novinari, i drugi), najveći deo su činili lokalni i regionalni mediji. Više o upitniku u delu „Metodologija“.

66 Partneri Srbija, BIRN Srbija, Share Fondacija: „Invazija na privatnost“ (Beograd, 2025), strana 13.

67 Ibid, strana 23.

Izveštaji Saveta za štampu⁶⁸ pokazuju da je poglavlje o poštovanju privatnosti Kodeksa novinara i novinarki Srbije drugo po broju prekršaja, odmah iza poglavlja o „istinitosti izveštavanja“. Najčešće se krše prava na privatnost žrtava krivičnih dela i osumnjičenih u krivičnim postupcima, kao i pojedinaca koji su predmet kampanja targetiranja, poput aktivista ili učesnika protesta.⁶⁹ Najčešće objavljivani lični ili osetljivi podaci uključuju: puno ime i prezime, privatne fotografije, adresu ili mesto boravka, informacije o prethodnim krivičnim postupcima, zdravstveno stanje, podatke o socijalnoj pomoći, seksualnu orijentaciju i etničku ili nacionalnu pripadnost.⁷⁰

Regulatorni okvir i etičke norme

Mediji u Srbiji imaju pravo da obrađuju i objavljuju podatke o ličnosti kada je to u **javnom interesu**. Zakon o zaštiti podataka o ličnosti⁷¹ u članu 88 jasno definiše da se odredbe ovog zakona o obavezama u rukovanju i objavljivanju podataka **ne odnose** na obradu „koja se vrši u svrhe novinarskog istraživanja i objavljivanja informacija u medijima“ i u „cilju zaštite slobode izražavanja i informisanja“.

Zakon o javnom informisanju i medijima navodi da mediji ne smeju da objavljuju informacije iz privatnog života ili lične zapise bez pristanka osobe na čiji se privatni život odnose.⁷² Ipak, predviđen je niz izuzetaka: ove informacije mogu se objaviti bez pristanka ako se odnose „na ličnost, pojavu ili događaj od **interesa za javnost**, posebno ako se odnosi na nosioca javne ili političke funkcije“.⁷³

68 Savet za štampu: Izveštaj o monitoringu poštovanja Kodeksa novinara i novinarki Srbije u dnevnim novinama u periodu od 1. jula 2025. do 31. decembra 2025. godine (Beograd, 2026), strana 4.

69 Invazija na privatnost, strana 17.

70 Ibid, strana 20.

71 Zakon o zaštiti podataka o ličnosti „Sl. glasnik RS“, br. 87/2018

72 Zakon o javnom informisanju i medijima, član 91.

73 Zakon o javnom informisanju i medijima, član 93.

Kodeks novinara i novinarki Srbije⁷⁴ daje najprecizniji okvir kada je u pitanju balans između zaštite privatnosti i javnog interesa⁷⁵ i predviđa mogućnost objavljivanja privatnih podataka kada za tim „postoji **javni interes koji preteže nad pravom na privatnost**“.⁷⁶ **Javni interes** se definiše kao „objavljivanje svih važnih informacija koje su građanima od pomoći pri formiranju suda/mišljenja o pojavama i događajima“.⁷⁷

Pravo na brisanje podataka i pravo na zaborav

Razvoj interneta i objavljivanje podataka u digitalnom prostoru otvorili su niz pitanja u vezi sa dugoročnom dostupnošću informacija i podataka očnosti. Podaci objavljeni u onlajn medijima potencijalno ostaju dostupni zauvek, pa i onda kada njihovo postojanje ne doprinosi više javnom interesu.

U Srbiji, Zakon o javnom informisanju i medijima predviđa mogućnost da osobe kojima je povređeno pravo na privatnost zahtevaju **uklanjanje** ili uništenje informacija ili zapisa.⁷⁸ Ovi sudski postupci se pokreću tužbom, u proseku traju nešto manje od dve godine, a najčešće dosuđivan iznos naknade štete iznosi oko 100.000 dinara.^{79 80}

U Evropskoj uniji, odlukom Suda pravde iz 2014. godine⁸¹ uspostavljen je princip „**prava na zaborav**“, koji omogućava pojedincima da zahtevaju uklanjanje rezultata pretrage koji sadrže lične podatke, čak i kada su

74 Kodeks novinara i novinarki Srbije <https://savetzastampu.rs/wp-content/uploads/2024/12/KODEKS-novinara-i-novinarki-2025-korekcija.pdf>

75 Kodeks novinara i novinarki Srbije, poglavlje VI.

76 Ibidem.

77 Kodeks novinara i novinarki Srbije, Preambula.

78 Zakon o javnom informisanju i medijima, član 112.

79 Partneri Srbija, BIRN Srbija, Share Fondacija: „Povrede privatnosti u medijima“ (Beograd, 2024), strana 8.

80 Podaci se odnose na presude donete 2023. godine.

81 Presuda Suda pravde Evropske unije u sporu Google Spain SL, Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Mario Costeja González (2014).

objavljene informacije tačne, ali više nisu relevantne. Ovi zahtevi ne upućuju se medijima, već internet pretraživačima - ukoliko se zahtevi utvrde kao osnovani, sami podaci se ne brišu, već se smanjuje njihova dostupnost uklanjanjem iz internet pretraga. Ovo se odnosi i na istinite, ali irelevantne, stare, intruzivne informacije ili informacije objavljene bez pristanka.

U slučaju koji je Sud pravde razmatrao 2014. godine, građanin Španije tražio je da se ukloni njegovo ime iz pretraga, jer su na pretraživaču kompanije Gugl izlazili tekstovi iz 1998. godine o prodaji njegove imovine na licitaciji, zbog dugova. Sud je naredio da se linkovi uklone iz pretraga jer objavljene informacije, iako tačne, nisu više i relevantne, između ostalog.

U Velikoj Britaniji, osoba osuđena na šest meseci zatvora, tražila je da kompanija Gugl ukloni linkove ka vestima o postupku koji je protiv nje vođen, što je sud 2018. godine i naložio. U obrazloženju suda se navodi da se okrivljeni pokajao i odslužio kaznu, da je u pitanju blaže krivično delo, da su tekstovi zastareli, nerelevantni i da ne postoji legitimni interes da i dalje budu dostupni, uzimajući u obzir da se okrivljeni bavi potpuno drugim delatnostima i da tekstovi o krivičnom postupku nisu značajni za donošenje odluka o tome da li će neko ubuduće sa njim sarađivati⁸².

U Srbiji je Kodeksom novinara i novinarki Srbije⁸³ predviđeno da mediji mogu ukloniti ime i podatke o ličnosti na zahtev osobe čija su prava povređena, pod uslovom da objavljivanje tih podataka nije u javnom interesu. Urednici pri odlučivanju uzimaju u obzir prirodu i aktuelnost teme, društveni položaj osobe o kojoj se pisalo, kao i aktuelnost i naučni ili istorijski značaj podataka. Mediji mogu odlučiti da uklone samo lične podatke ili celokupan sadržaj.

82 Portal Pravosuđa Velike Britanije, presuda u predmetu NT1 i NT2 protiv Google LLC (2018).

83 Kodeks novinara i novinarki Srbije, poglavlje VI.

Zloupotreba prava

U praksi postoji i rizik od zloupotrebe pravnih postupaka protiv novinara i medija. Takozvane SLAPP tužbe (strateške tužbe protiv učešća javnosti) koriste se za zastrašivanje novinara i medija, često uz pretnju velikim finansijskim kaznama ili zahtevima za otkrivanje izvora.

U Evropskoj uniji godinama se upozorava na mogućnost zloupotrebe GDPR-a i prava na zaborav.⁸⁴ Medijske organizacije i organizacije za zaštitu ljudskih prava prepoznale su brojne slučajeve pokušaja da se mediji primoraju da uklone informacije od javnog interesa,⁸⁵ kao i da se pokrenu postupci kontrole medija radi uvida u novinarske izvore.⁸⁶ Zbog toga je važno razlikovati legitimne zahteve za zaštitu privatnosti i pokušaje ograničavanja slobode medija.

U Rumuniji je institucija nadležna za zaštitu podataka o ličnosti tražila od istraživačkog medija RISE 2018. godine uvid u celokupnu dokumentaciju koju su koristili za istraživanje o zloupotrebi EU sredstava, kao i izvore informacija, uz pretnju kaznom od 20 miliona evra⁸⁷.

Kancelarija za zaštitu ličnih podataka Slovačke zahtevala je od Češkog centra za istraživačko novinarstvo da otkrije izvor koji im je dostavio video na kom se vide slovački oligrah Marian Kočner i tadašnji generalni tužilac Dobroslav Trnka, pozivajući se na zaštitu podataka i preteći kaznom od 10 miliona evra⁸⁸. Kasnije je otkriveno da je direktorka kancelarije bila godinama u komunikaciji sa Kočnerom⁸⁹, a sam Kočner je osuđen na 19 godina

84 Article 19: „The 'Right to be Forgotten': Remembering Freedom of Expression" (London, 2016).

85 International Press Institute: „Court orders recall of Forbes Hungary following GDPR complaint" (2020).

86 European Journalism Observatory: „How GDPR can be used to threaten investigative journalists?" (London, 2018).

87 OCCRP: „English Translation of the Letter from the Romanian Data Protection Authority to RISE Project" (2018).

88 Aktuality: „Šéfka Úradu na ochranu osobných údajov písala Kočnerovi. Jej úrad hrozil novinárom likvidačnou pokutou" (2020).

89 Aktuality: „Šéfka Úradu na ochranu osobných údajov písala Kočnerovi. Jej úrad hrozil novinárom likvidačnou pokutou" (2020).

zatvora zbog falsifikovanja menica⁹⁰. Suđeno mu je i za ubistvo slovačkog novinara Jana Kucijaka i njegove verenice Martine Kusnirove, ali je oslobođen optužbi⁹¹.

Test javnog interesa

U cilju zaštite prava na privatnost i unapređenja profesionalnih standarda, mediji bi pre objavljivanja ličnih podataka trebalo da procene: da li informacija doprinosi javnoj debati, da li je identitet osobe relevantan za javnost i da li je objavljivanje proporcionalno cilju informisanja.

Svaki zahtev za uklanjanjem privatnih podataka treba razmatrati posebno, uzimajući u obzir sve specifičnosti slučaja - **društveni položaj osobe** (javna ličnost, javni funkcioner, žrtva krivičnog dela), **prirodu i aktuelnost teme** i da li su podaci od **javnog, naučnog ili istorijskog značaja**. Osobe čije podatke mediji objavljuju nisu u obavezi da poznaju odredbe zakona ili kodeksa.

Ukoliko odluče da ispune zahtev, mediji nisu u obavezi da uklone sadržaj u onom obimu u kom je navedeno u zahtevu - trebalo bi da, u skladu sa javnim interesom i proporcionalnošću, donesu samostalnu odluku o tome da li će ukloniti samo lične podatke ili celokupan sadržaj.

90 Aktuality: „Kauza zmenky: súd definitívne odsúdil Kočnera a Ruska na 19 rokov väzenia" (2021).

91 Guardian: „Slovakia: court acquits tycoon in retrial over 2018 killing of journalist and fiancée" (2023).

Zaključak

Upravljanje podacima korisnika nije samo pravna obaveza - ono je strateška kompetencija koja određuje dugoročnu održivost i kredibilitet medija. Ovaj dokument pokazuje da su zaštita privatnosti i ekonomska održivost kompatibilni ciljevi: medij koji transparentno postupi sa podacima, gradi poverenje publike koje je osnova svakog modela monetizacije, od pretplate do donacija.

Nalazi istraživanja i analize prakse u Srbiji ukazuju na paradoks: manji, lokalni i neprofitni mediji često bolje štite privatnost korisnika od velikih komercijalnih portala, ne zbog većih resursa, već zbog manje zavisnosti od agresivnog *AdTech* modela. To pokazuje da odgovornost u upravljanju podacima nije pitanje veličine, već poslovnog modela i vrednosnog opredeljivanja.

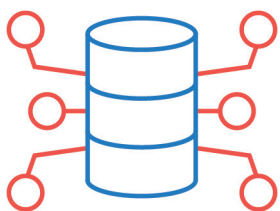
Regulatorni okviri Srbije i EU postavljaju minimalne standarde, ali pravo pitanje za redakcije nije kako ispuniti zakonski minimum, već kako izgraditi kulturu u kojoj se podacima korisnika postupi sa istom pažnjom sa kojom se postupi sa novinarskim izvorima. U tom smislu, zaštita podataka je produžetak novinarske etike, a ne njen suparnik.

U godinama koje dolaze, uvođenje veštačke inteligencije u redakcije ubrzaće i produbiti izazove opisane u ovom dokumentu. Mediji koji sada izgrade jasne procedure za upravljanje podacima biće bolje pripremljeni za AI okruženje u kome personalizacija sadržaja i zaštita privatnosti moraju da idu ruku pod ruku. Mediji koji to ne učine izlažu se ne samo pravnim posledicama, već i gubitku poverenja publike koje je, jednom izgubljeno, teško povratiti.

Konkretni koraci za usklađivanje poslovanja nalaze se u narednom poglavlju.

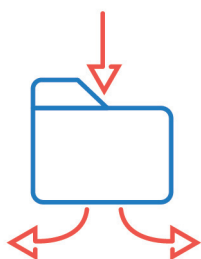
Deo III – Set koraka za usklađivanje poslovanja medija

1. Sprovesti interni popis podataka i alata koje medij koristi.



Prvi korak je da redakcija, menadžment, marketing i IT zajedno utvrde koje podatke medij prikuplja, gde se oni nalaze, kroz koje sisteme prolaze i ko im pristupa. Popis treba da obuhvati sajt, CMS, analitiku, *newsletter* alate, CRM, komentare, društvene mreže, oglasne servise i sve druge spoljne servise. Bez ovog koraka medij ne može pouzdano da proceni ni svoje obaveze, ni rizike, ni stvarni obim obrade.

2. Razdvojite vrste obrada i ograničite prikupljanje na ono što je stvarno potrebno.



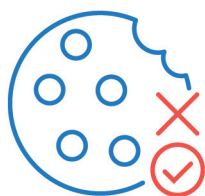
Medij treba jasno da razlikuje funkcionalnu obradu, koja je nužna za rad sajta i pružanje usluge, od analitičke, marketinške i profilisane obrade, koja ide dalje od tehničke nužnosti. Posebno je važno da se obrada publike razdvoji od obrade podataka u novinarskom radu i uređivačkom procesu. U svakom slučaju treba poći od načela minimizacije: ne prikupljati više podataka nego što je opravdano svrhom.

3. Za svaku svrhu obrade odredite pravni osnov i dokumentujte ga.



Medij ne sme obrađivati podatke „zato što mu mogu zatrebati“, već za svaku obradu mora unapred znati po kom pravnom osnovu se ona vrši. Za pretplate i članstva osnov će najčešće biti izvršenje ugovora; za određene bezbednosne i ograničene analitičke svrhe - legitiman interes; za *newsletter* (koji nije deo ugovorne usluge), targetirano oglašavanje i napredne kolačiće - najčešće saglasnost. Dodatne svrhe, poput napredne personalizacije ili marketinškog profilisanja, ne treba prikrivati pod osnovnim pružanjem usluge.

4. Uredite kolačiće i druge tehnologije praćenja tako da korisnik ima stvaran izbor.



Medij treba da ukloni praksu „prihvati sve ili nema pristupa“, da jasno odvoji nužne kolačiće od analitičkih i marketinških i da korisniku omogući jednako vidljivu opciju prihvatanja i odbijanja. Saglasnost mora biti dobrovoljna, određena, informisana i opoziva. Posebno treba izbegavati obrasce koji korisnika guraju ka prihvatanju praćenja, jer formalna saglasnost bez stvarne kontrole ne znači zakonitu obradu.

5. Ažurirajte politiku privatnosti i politiku kolačića tako da odražavaju stvarne procese.



Politike privatnosti ne smeju biti generički, prepisani dokumenti. One treba jasno da objasne ko obrađuje podatke, koje vrste podataka se prikupljaju, u koje svrhe, na kom osnovu, kome se podaci otkrivaju, koliko dugo se čuvaju, da li se prenose u inostranstvo i kako korisnik ostvaruje svoja prava. Dobra politika privatnosti prati stvarne tokove obrade podataka po svrhama i povezana je sa stvarnim internim praksama medija.

6. Uspostavite evidenciju radnji obrade, rokove čuvanja i pravila pristupa.



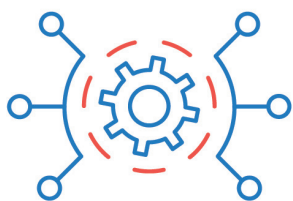
Medij treba da vodi internu evidenciju o tome koje podatke obrađuje, u koje svrhe, kojim sistemima, ko im pristupa, kome se podaci otkrivaju i koliko dugo se čuvaju. Istovremeno, potrebno je unapred odrediti rokove brisanja za logove, analitiku, marketinške liste, naloge korisnika i druge baze. Pristup podacima mora biti ograničen po principu nužnosti, uz jasna pravila ko ima administratorska prava i ko može izvoziti baze podataka.

7. Odredite jasnu internu odgovornost za zahteve korisnika i prigovore.



Korisnik mora lako da pronade gde može da se obrati mediju radi pristupa, brisanja, prigovora, odjave sa *newsletter*-a ili drugih zahteva. Zato je važno odrediti jednu jasnu kontaktnu tačku i podeliti interne uloge: ko prima zahtev, ko proverava baze i alate, a ko priprema odgovor. Posebno treba obezbediti da se prigovor na direktni marketing ili profilisanje odmah sprovede u svim sistemima, uključujući i sisteme trećih strana.

8. Smanjite oslanjanje na treće strane i revidirajte sve dobavljače i ugovore.



Svaki eksterni servis koji medij koristi povećava pravni, bezbednosni i reputacioni rizik. Zato je potrebno proveriti koje treće strane zaista moraju da budu uključene, kakvu ulogu imaju, koje podatke dobijaju, gde se ti podaci šalju i pod kojim uslovima. Ugovori sa hosting kompanijama, *newsletter* platformama, održavaocima sajta i drugim dobavljačima treba da sadrže jasna ograničenja obrade, bezbednosne obaveze i zabranu neovlašćenog deljenja podataka publike.

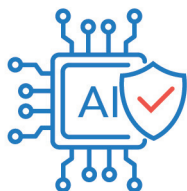
Kada god je moguće, medij treba da daje prednost modelima koji se više oslanjaju na podatke prve strane, a manje na invazivni *AdTech* ekosistem.

9. Uvedite osnovne bezbednosne mere i plan za reagovanje na povredu podataka.



Minimum bezbednosne kulture obuhvata kontrolu pristupa, jake lozinke, dvostruku autentifikaciju, ažuriranje sistema, rezervne kopije, nadzor pristupa i redovne interne obuke. Pored toga, medij treba da ima unapred pripremljenu proceduru za incidente: ko prvi reaguje, ko procenjuje rizik, ko dokumentuje događaj i ko odlučuje o obaveštavanju Poverenika i pogođenih lica. Kod povreda koje mogu proizvesti rizik po prava fizičkih lica, postoji obaveza obaveštavanja Poverenika, po pravilu u roku od 72 časa od saznanja.

10. Uvedite posebna pravila za AI alate i testirajte ih pre puštanja u rad.



AI alat ne treba uvoditi kao još jedan „koristan dodatak“, već kao novi tok obrade podataka koji može otvoriti ozbiljne pravne i etičke rizike. Pre upotrebe treba sprovesti procenu rizika, proveriti poreklo podataka na kojima je alat obučen, testirati alat u kontrolisanom okruženju i zabraniti unos neobjavljenih, poverljivih ili urednički osetljivih sadržaja bez jasnog odobrenja. Eksterni partneri ne smeju imati pristup izvorima, internim komunikacijama redakcije ili nacrtima tekstova. Odgovornost za tačnost i zakonitost obrade i dalje ostaje na ljudima, a ne na alatu.

11. Usklađenost merite kroz praksu, a ne kroz postojanje dokumenata.



Analiza pokazuje da su u Srbiji česti slučajevi formalne, ali ne i stvarne usklađenosti: politike privatnosti i druga interna akta postoje, ali ne odgovaraju realnim procesima; korisnici formalno dobijaju oba-

veštenja, ali nemaju stvarnu kontrolu; redakcije koriste alate čiji rad ne poznaju dovoljno. Zato medij treba periodično da proverava da li se interna pravila zaista primenjuju, da li zaposleni znaju koje podatke obrađuju, da li znaju koje treće strane imaju pristup tim podacima i da li postoji realna spremnost za incident, zahtev korisnika ili proveru nadzornog organa.

12. Zaštitu podataka tretirajte kao deo poverenja publike i dugoročne održivosti medija.



Medij koji transparentno i srazmerno postupa sa podacima publike ne ispunjava samo pravnu obavezu, već gradi reputaciju i poverenje koje postaje ključna poslovna vrednost. U okruženju u kome su korisnici sve svesniji svojih prava, a regulatorna očekivanja sve stroža, zakonito postupanje sa podacima više nije sporedno administrativno pitanje, već deo uredničke i menadžerske odgovornosti.

Kontrolna lista za redakcije

Bezbednost i zaštita podataka publike

(Za urednike, novinare i menadžment)

1. Razumevanje i mapiranje podataka

- ☐ Znamo koje vrste podataka prikupljamo od publike (analitika, komentari, *newsletter*, kontakti, donacije)
- ☐ Imamo spisak svih alata i platformi koje koristimo (analitika, oglašavanje, embedovi, *newsletter* alati)
- ☐ Znamo koje treće strane imaju pristup podacima naše publike
- ☐ Razlikujemo:
 - podatke publike
 - podatke izvora i sagovornika
 - interne podatke redakcije

2. Transparentnost prema publici

- ☐ Imamo javno dostupnu i razumljivu politiku privatnosti (ne samo pravni tekst)
- ☐ Jasno objašnjavamo:
 - koje podatke prikupljamo
 - zašto
 - koliko dugo ih čuvamo
- ☐ Publika ima način da nas kontaktira u vezi sa podacima (mejl, forma, kontakt osoba)
- ☐ Ne skrivamo obradu podataka iza „obaveznih kolačića“

3. Kontrola trećih strana i tehnologija

- ☐ Znamo koje skripte se učitavaju na sajtu
- ☐ Embedovani sadržaj koristimo samo kada je urednički opravdan
- ☐ Razmatramo alternative embedovima (*screenshot*, link)
- ☐ Oglašivačke mreže ne rade bez ikakvog uredničkog nadzora
- ☐ Razumemo osnovne posledice programatskog oglašavanja

4. Minimizacija podataka (manje je više)

- ☐ Ne prikupljamo podatke koji nam nisu neophodni
- ☐ *Newsletter* ne traži više podataka nego što je potrebno
- ☐ Komentari ne zahtevaju nepotrebne lične podatke
- ☐ Imamo praksu brisanja starih i neaktivnih podataka

5. Bezbednost sistema i komunikacije

- ☐ Baze podataka su zaštićene i pristup je ograničen
- ☐ Samo ovlašćene osobe imaju pristup osetljivim podacima
- ☐ Postoje posebne mere za:
 - kontakt forme
 - prijave građana
 - uzbunjivače
- ☐ Redakcija koristi sigurne kanale komunikacije (za izvore i interne teme)

6. Urednička odgovornost i etika

- ☐ Urednici razumeju kako analitika i AI alati utiču na odluke
- ☐ AI alati se koriste uz ljudski nadzor
- ☐ Personalizacija sadržaja ne menja činjenice ili kontekst
- ☐ Postoji svest o riziku profilisanja publike

7. Organizacija i interna pravila

- ☐ Postoji osoba ili tim odgovoran za pitanja podataka (ne mora biti formalni DPO)
- ☐ Urednici, novinari i tehnički tim komuniciraju o alatima
- ☐ Novi alati se uvode uz procenu rizika
- ☐ Postoje osnovna interna pravila o zaštiti podataka

8. Krizne situacije i incidenti

- ☐ Znamo šta radimo ako dođe do curenja podataka
- ☐ Znamo koga obaveštavamo (interno i eksterno)
- ☐ Postoji plan za minimizaciju štete
- ☐ Incidenti se dokumentuju i analiziraju

9. Realnost za male i lokalne medije

- ☐ Svesni smo da ne možemo sve - ali znamo šta možemo
- ☐ Prioritet dajemo:
 - osetljivim temama
 - ranjivoj publici
 - istraživačkom radu
- ☐ Biramo manje alata, ali sa više kontrole

Prilog 1- Onlajn anketa za medijske radnike

I. OSNOVNE INFORMACIJE O REDAKCIJI

1. Veličina redakcije (broj zaposlenih)

Odaberite jedan od ponuđenih odgovora

- 1–5
- 6–10
- 11–20
- 21–50
- više od 50

2. Tip medija

- Lokalni
- Regionalni
- Nacionalni

2 (A). Vaš mediji ima online prisustvo

- Da
- Ne

II. RAZUMEVANJE I MAPIRANJE PODATAKA

3. Da li znate koje vrste podataka prikupljate od publike online?

- Da, u potpunosti

- Delimično
- Ne
- Nisam siguran/na

4. Koje vrste podataka prikupljate?

(moguće više odgovora)

- Analitika poseta
- Komentari korisnika
- Newsletter prijave
- Kontakt forme
- Donacije / pretplate
- Korisnički nalozi
- Drugo: _____

5. Da li znate koje vrste kolačića su postavljene na vašem sajtu?

- Da
- Delimično
- Ne

6. Koje vrste kolačića koristite?

- Neophodni (osnovni)
- Funkcionalni
- Analitički
- Marketinški
- Nisam siguran/na

7. Da li imate spisak svih digitalnih alata i platformi koje koristite, a koji obrađuju podatke o ličnosti (npr. analitika, oglašavanje, embedovi, newsletter alati i dr)?

- Da
- Delimično
- Ne

8. Da li znate koje treće strane imaju pristup podacima vaše onlajn publike?

- Da
- Delimično
- Ne
- Nisam siguran/na

III. TRANSPARENTNOST PREMA PUBLICI

9. Da li imate javno dostupnu i razumljivu politiku privatnosti?

- Da, napisana jednostavnim jezikom
- Da, ali je pravno/formalno napisana
- Ne
- Nisam siguran/na

10. Da li imate jednostavan mehanizam za odjavu sa newsletter-a?

- Da
- Ne
- Nemamo newsletter

IV. ORGANIZACIJA I INTERNA PRAKSA

11. Da li su baze podataka zaštićene lozinkom ili enkripcijom?

- Da
- Delimično
- Ne
- Nisam siguran/na

12. Da li imate procedure i rokove za brisanje podataka o ličnosti koje više ne koristite?

- Da
- U pripremi

- Ne
- Nisam siguran/na

13. Da li postoji osoba ili tim odgovoran za upravljanje i zaštitu podataka o ličnosti?

- Da, formalno imenovana osoba ili tim
- Da, neformalno određena osoba
- Ne
- Nisam siguran/na

14. Da li imate internu politiku o unosu podataka u komercijalne AI sisteme (npr. ChatGPT, alati za transkripciju, analitiku)?

- Da
- U pripremi
- Ne
- Nisam siguran/na

15. Da li vaša redakcija ima razvijenu praksu usavršavanja zaposlenih u oblasti zaštite podataka o ličnosti i privatnosti?

- Da, redovno organizujemo ili pohađamo obuke
- Povremeno
- Ne, ali planiramo
- Ne

16. Da li imate procedure za slučaj gubitka ili curenja podataka ili opreme?

- Da
- Delimično
- Ne
- Nisam siguran/na

17. Ako novinar izgubi ili mu bude ukraden službeni uređaj (laptop, telefon), koje mere preduzimate?

V. POTREBE I PODRŠKA

18. U kojim oblastima vam je potrebna dodatna podrška ili obuka?

- Pravne obaveze i regulative za zaštitu privatnosti korisnika online medijskih sadržaja
- Upravljanje kolačićima i analitikom
- Bezbednost podataka
- Privatnost u novinarskom izveštavanju
- Upravljanje newsletter bazama
- AI alati i zaštita podataka
- Drugo: _____

19. Dodatni komentari ili izazovi sa kojima se suočavate
