

Vodič za usklađivanje poslovanja medija

Upravljanje podacima publike u digitalnim medijima

Autorke:
Milica Tošić
Tanja Maksić



Vodič pred Vama nastao je na osnovu analize „**Od čitalaca do profita: Upravljanje podacima korisnika u digitalnim medijima**“ i predstavlja praktičan skup preporuka za usklađivanje poslovanja medija sa standardima zaštite privatnosti. Namenjen je urednicima, menadžerima i drugim donosiocima odluka u medijima koji upravljaju digitalnim alatima, monetizacijom i odnosom sa publikom.

Za bolje razumevanje ovog vodiča preporučujemo da se prvo pročitava analiza „**Od čitalaca do profita: Upravljanje podacima korisnika u digitalnim medijima**“, koja je dostupna na sajtu organizacije Partneri Srbija <https://www.partners-serbia.org/>.

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.

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 početi od načela minimizacije: ne prikupljati više podataka nego što je opravdano svrhom.

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.

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 omogućiti 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.

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.

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.

Odredite jasnu internu odgovornost za zahteve korisnika i prigovore.

Korisnik mora lako da pronađe gde može da se obrati mediju radi pristupa, brisanja, prigovora, objave 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.

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 kadege 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.

Uvedite osnovne bezbednosne mere i plan za reagovanje na povrede podataka.

Minimum bezbednosne kulture obuhvata kontrolu pristupa, jake lozinke, dvostruku autentifikaciju, ažuriranje sistema, rezervne kopije, nadzor pristupa i redovne interne buke. 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.

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.

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 obaveštenja, 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.

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

Medij koji transparentno i srazmerno postupi 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.

Maj 2026.

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.