Zaštita podataka posjetitelja mrežnih stranica obrazovnih institucija - Cookiebot

Tihomir Katulić | 7 travnja, 2026

Kad se govori o novim informacijskim uslugama, velikim platformama i *Big Data* projektima, često se kaže kako su podaci nova valuta, digitalno zlato ili digitalna nafta, resurs koji se treba crpiti, obrađivati i monetizirati. No podatke, osobito osobne podatke, ne prikupljaju i obrađuju samo privatne organizacije, trgovačka društva i međunarodne korporacije, nego i razna tijela javne vlasti pa tako i javne ustanove poput onih u sustavu odgoja, obrazovanja i znanosti. Te se organizacije susreću s izazovima usklađivanja s modernim europskim digitalnim zakonodavstvom, ponajviše zbog manjka ljudskih i financijskih resursa. Obrazovne i znanstvene institucije imaju važnu društvenu zadaću, one nisu samo formativne, odgojne i pedagoške institucije, čuvari vještina i znanosti, već imaju i zadaću biti predvodnici u neprestanom društvenom napretku, u čemu se trebaju čvrsto držati pravnih i etičkih pravila i standarda. Pomalo je ironično da se u predavaonicama, laboratorijima i učionicama raspravlja o visokim moralnim načelima, znanstvenoj čestitosti i etičkim dilemama znanstvenih i obrazovnih aktivnosti, a da istovremeno u praksi tih institucija dominira nerazumijevanje i nepoznavanje pravnog okvira u kojem djeluju, čak i kad je riječ o skromnim naporima koje bi takve organizacije mogle poduzeti kako bi svoje poslovanje dovele u sklad s pravnim obvezama.

Pitanje usklađenosti obrazovnih i znanstvenih institucija s propisima kao što je Opća uredba o zaštiti podataka (u daljnjem tekstu OUZP) mnogo je šire od teme ovog prikaza, no treba naglasiti da osam godina nakon početka primjene OUZP-a, mnoge škole, fakulteti, sveučilišta i visoke škole i dalje nisu adekvatno uskladile svoje poslovanje sa zahtjevima Uredbe. Budući da ta kategorija voditelja obrade nije prema odredbama hrvatskog Zakona o provedbi OUZP isključena od mogućnosti izricanja upravne novčane kazne, baš kao ni druge slične javne ustanove poput bolnica i domova zdravlja, takvo nemarno ponašanje može dovesti do visokih kazni.

Jedan relativno vidljiv i potencijalno lako „popravljiv“ aspekt usklađivanja takvih organizacija s OUZP-om i drugim primjenjivim propisima svakako je pitanje upotrebe tzv. *cookieja* odnosno kolačića, malih tekstualnih datoteka koje služe za praćenje korisnika, posjetitelja mrežnih stranica koje ih upotrebljavaju pa tako i posjetitelja mrežnih stranica obrazovnih institucija. Zamislimo sljedeću situaciju: znanstveni institut provodi sociološko istraživanje, primjerice o eroziji privatnosti i zaštiti podataka u kontekstu novih digitalnih usluga, a posjetitelje mrežne stranice tog istog projekta dočekuje nepotpuna ili nepostojeća obavijest o kolačićima, dok u pozadini Google Analytics i desetine skripti trećih strana bez pitanja prikupljaju podatke o ponašanju korisnika.

Službenici za zaštitu podataka (DPO = *data protection officers*), ako odgovorno rade svoj posao, pod velikim su pritiskom identificirati nove obrade osobnih podataka i odgovarajuće ih unijeti u dokumentaciju kao što su politike, odnosno informacije o obradi podataka, evidencije aktivnosti obrade i tako dalje. Dinamičnost razvoja i uporabe kolačića u velikom je nesrazmjeru s kapacitetima službenika da, uz druge poslove koje redovito obavljaju, prate deklaracije kolačića i ažuriraju ih u pratećoj dokumentaciji.

Zbog toga alati poput Cookiebota i sličnih rješenja (o kojima više u pratećem okviru) mogu pomoći kroz dinamičke deklaracije kolačića. Budući da skeneri ovih alata redovito (npr. mjesečno) prolaze kroz cijelu mrežnu stranicu, oni automatski ažuriraju tablicu kolačića. Ako skener pronađe novi kolačić, on ga automatski dodaje na popis, kategorizira ga kao neku od ponuđenih kategorija, navodi njegovu svrhu, trajanje i davatelja usluge, što olakšava posao mrežnom uredništvu i drugim djelatnicima čiji je zadatak održavati institucionalni sustav zaštite osobnih podataka. Automatizacija ovih zadaća osigurava da ono što piše u informacijama o obradi i drugoj dokumentaciji bude identično onome što se tehnički događa na stranici. To je razina transparentnosti koju je ručno

gotovo nemoguće održavati.

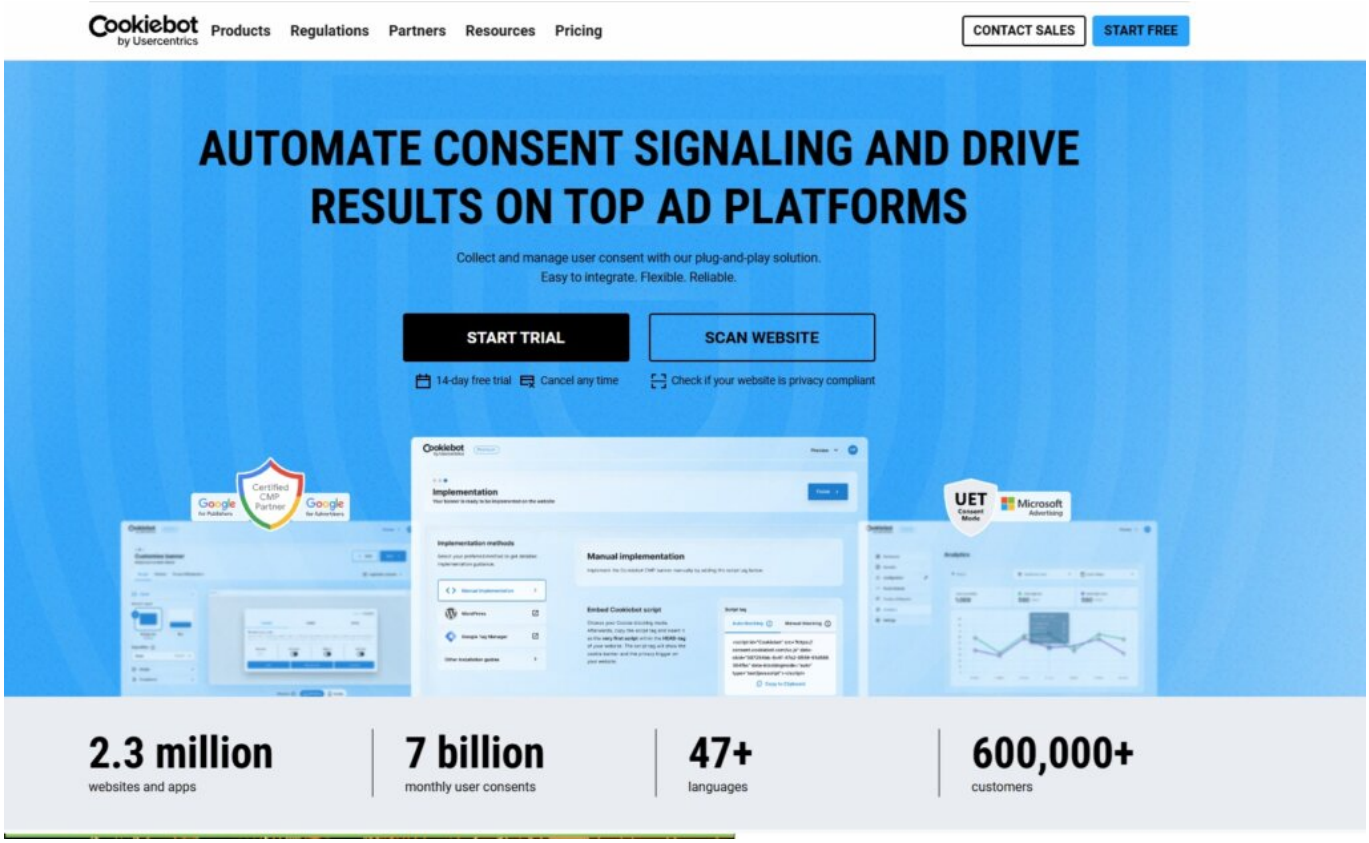
Što je CookieBot?

Cookiebot je sustav za upravljanje privolama (*consent management system*), koji je razvila tvrtka Usercentrics. Njegova osnovna svrha je automatizirati složeni proces postizanja i održavanja usklađenosti mrežne stranice s glavnim globalnim zakonima o privatnosti podataka, poput europskog GDPR-a i Direktive ePrivacy odnosno nacionalnih transponirajućih propisa za tu direktivu (U RH – Zakon o elektroničkim komunikacijama).

Ova kategorija alata obavlja brojne funkcije u pogledu osiguranja zakonitog i transparentnog korištenja kolačića na mrežnim stranicama tako što omogućuju redovito skeniranje i identifikaciju korištenih kolačića otkrivajući sve kolačiće, *trackere* i druge tehnologije praćenja koje se koriste na nekoj mrežnoj stranici. Istovremeno, alat će po otkrivanju kolačića u izvještaju klasificirati otkrivene kolačiće prema njihovoj svrsi (npr. nužni, statistički, marketinški) koristeći vlastitu opsežnu bazu podataka.

U pogledu upravljanja privolama, ova kategorija alata omogućuje postavljanje i prilagođavanje *bannera* za privolu, omogućujući korisnicima da daju granularnu, odnosno za svrhu obrade posebnu, jasnu, afirmativnu privolu. Istovremeno, tehnički se osigurava da se marketinške i statističke skripte ne učitaju i ne aktiviraju prije nego što korisnik zaista da privolu. Konačno, ovakvi alati, pa tako i Cookiebot bilježe i čuvaju digitalne dokaze o danim ili uskraćenim privolama, stvarajući revizijski trag (*audit trail*) organizaciji – voditelju obrade, ključan za dokazivanje odgovornog postupanja.

S alatima kao što je Cookiebot, službenici za zaštitu podataka i stručnjaci za kibernetičku sigurnost, koji po prirodi posla često surađuju s mrežnim uredništvom u predmetnim organizacijama, koje su zbog financijskih razloga često ograničenih ljudskih resursa u navedenim ulogama, dobivaju moćan alat za reviziju odnosno audit svoje poslovne prakse. U slučaju prigovora korisnika ili upita nadzornog tijela, što je kod nas u pogledu zaštite osobnih podataka Agencija za zaštitu osobnih podataka (AZOP), službenik može putem alata izvući točne podatke o tome koji se kolačići koriste, kada je ispitanik odnosno posjetitelj stranice dao privolu za kolačiće koji nisu nužni za samo funkcioniranje stranice, što mu je bilo komunicirano oko svrhe i trajanja obrade i ostale podatke koje je dužan evidentirati i na zahtjev korisnika ili nadzornog tijela predočiti. Teret dokazivanja sukladnosti prebacuje se tako s preopterećenih stručnjaka na automatizirani sustav.

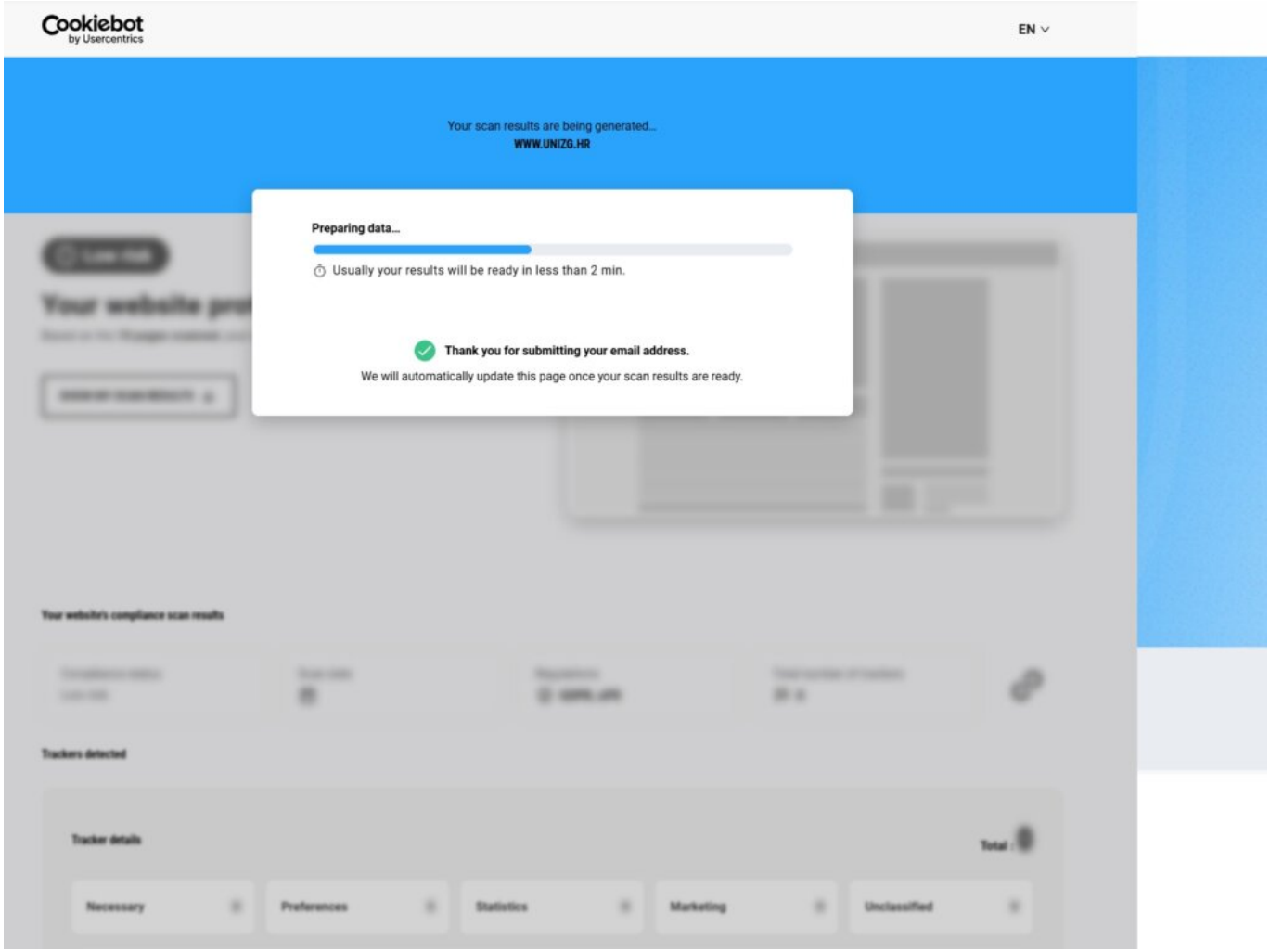


Slika 1.

Samopregledom do informacije o usklađenosti

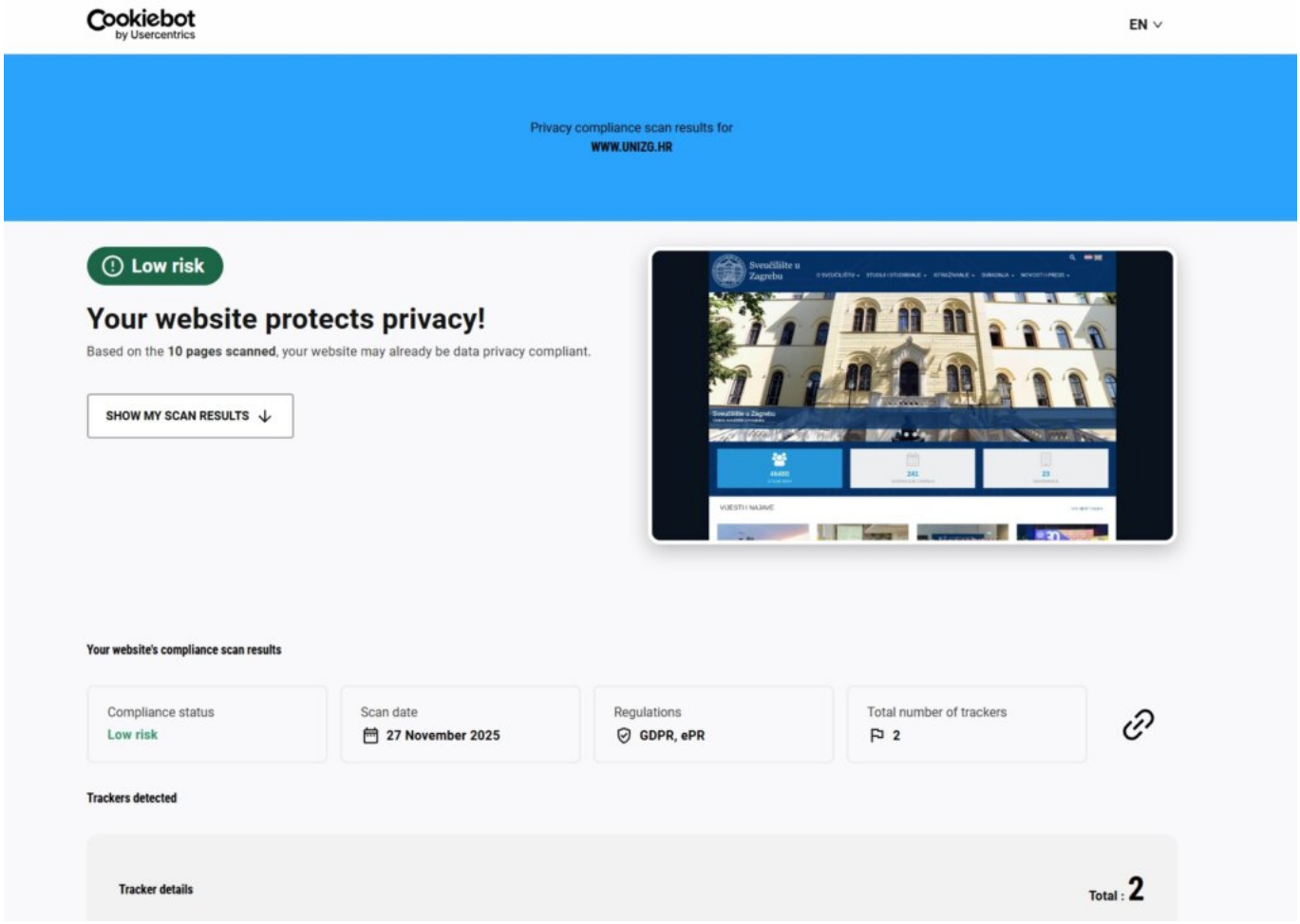
Najvažnija funkcionalnost Cookiebota, osobito za mrežne administratore u javnim ustanovama, jest njegov automatski mehanizam za skeniranje i otkrivanje kolačića. To je ključan element koji CMP alat izdvaja od pasivnog *pop-up bannera* kakav se nalazi integriran u većinu popularnih platformi za standardiziranu i brzu izradu mrežnih stranica, kao što su Joomla ili Wordpress. Alat može pomoći oko:

Kako skeniranje funkcionira? Cookiebot koristi robotski pretraživač (*crawler*) koji simulira stvarnog posjetitelja mrežne stranice. Postupak skeniranja uključuje nekoliko faza poput otkrivanja svih postojećih podstranica na domeni, bilježenja aktivnosti koje se događaju na otkrivenim stranicama, praćenje skripti koje se pokušavaju pokrenuti te usporedbe pronađenih kolačića sa stalno ažuriranom bazom podataka opisa kolačića, na temelju čega se automatski određuje je li kolačić nužan, funkcionalan, statistički ili marketinški, njegovo trajanje (koliko dugo ostaje aktivan) i slično.



Slika 2.

Konačni rezultat postupka skeniranja je detaljan izvještaj koji kod naplatnih inačica alata može biti izravno integriran u administrativno sučelje (*dashboard*) organizacije čime administratori dobivaju pregled svih kolačića i potrebne informacije koje se onda mogu koristiti za automatsko generiranje i ažuriranje Politike kolačića na mrežnoj stranici te za ispravno konfiguriranje *auto-blocking* mehanizma, čime se administrativni posao svodi na nadzor i upravljanje umjesto na detektivski rad.



Slika 3.

Za obrazovne institucije, usklađenost s Općom uredbom i drugim propisima nije samo zakonska obveza, već i etički zahtjev. Sveučilišta barataju podacima specifičnih skupina korisnika, studenata, a ponekad i maloljetnika (primjerice, u kontekstu promotivnih kampanja za upise, suradnje s nižim obrazovnim razinama u okviru raznih nastavnih i projektnih aktivnosti i slično). Ako akademska zajednica, koja bi trebala educirati društvo o digitalnoj pismenosti, ne poštuje obveze tehničke i integrirane zaštite osobnih podataka (*privacy by design and by default*), kakvu poruku šalje društvu i novim generacijama građana koje odgaja i obrazuje.

Sindrom projektnih stranica

IT podrška velikih obrazovnih institucija najviše pažnje posvećuje stranicama na krovnim domenama svojih institucija. Platforme poput WordPressa sadrže određene mogućnosti upravljanja privolama, a organizacije objavljuju i obavijesti o obradi podataka različite razine sadržajnosti. Često previđeni rizik leži u stranicama i poddomenama skrivenima daleko od matične, kao posljedica projektnog karaktera znanstvenih organizacija.

S obzirom da gotovo svaki EU projekt, svaka konferencija ili istraživačka grupa treba svoju mrežnu stranicu te stranice često ne izrađuje središnji IT odjel, već vanjski suradnici, studenti ili sami istraživači koristeći WordPress predloške, što rezultira visokim brojem poddomena koje su digitalno „nevidljive“ središnjoj upravi, a koje su krcate neusklađenim kolačićima, neispravnim ili zastarjelim podacima u obavijestima o obradi podataka i neažuriranim *cookie bannerima* koji ne blokiraju skripte prije traženja privole od posjetitelja.

Ima li alternative Cookiebotu?

Usercentricsov Cookiebot u praksi je vrlo raširen i mnogi stručnjaci za zaštitu osobnih podataka koriste njegove usluge te je čest izbor za velik broj mrežnih stranica čiji nakladnici su podvrgnuti europskom pravnom režimu, ponajviše zbog brojnih integriranih usluga ili barem korištenja besplatne ograničene pretplate za korisnike manjeg opsega nadziranih stranica. Razlog za to je kombinacija automatiziranog skeniranja mrežnih stranica, automatskog blokiranja kolačića, podrške za Google Consent Mode v2, brojnih integracija s popularnim CMS-ovima te podrške za više desetaka jezika. Zbog takve razine raširenosti druge se platforme gotovo uvijek percipiraju u odnosu na njega ili kao „lakša“ verzija istog koncepta ili kao dio šireg ekosustava zaštite osobnih podataka. Besplatan je za bazično skeniranje, a za više funkcionalnosti potrebno je platiti pretplatu.

Što čini druge alate zanimljivima? Neki će korisnici preferirati jednostavniji *onboarding* za timove koji nisu nužno tehnički, bolji korisnički doživljaj *bannera* i veće ostvarene stope korisničke privole (oprezno s privolom, uvijek u skladu sa standardima čl. 7 Opće uredbe o zaštiti podataka i primjenjivim smjernicama nadzornih tijela) te mogućnost da se obveze oko dokumentacije privole za kolačiće funkcionalno povežu s drugim obvezama iz područja zaštite podataka, poput upravljanja zahtjevima ispitanika ili vođenja evidencija aktivnosti obrade.

Jedna od češće spominjanih alternativa je CookieYes, koji se često promatra kao izravna zamjena za Cookiebot. Funkcionalno pokriva poznati paket: prikaz *bannera*, skeniranje kolačića i generiranje politika. Ipak, naglasak stavlja na intuitivnije sučelje i ugodniji rad za marketing i sadržajne timove, koji često nisu pretjerano tehnički potkovani. U recenzijama se često ističe jednostavan *dashboard* odnosno kontrolno sučelje, dobra dokumentacija i podrška te relativno transparentna i fleksibilna struktura cijena. Zbog toga se CookieYes pozicionira kao rješenje koje nudi sličnu razinu usklađenosti, ali u nešto cjenovno pristupačnijem paketu, osobito za manje i srednje organizacije gdje se svaka dodatna kompleksnost osjeti kao nepotreban administrativni teret.

Na drugom kraju spektra nalazi se sofisticiran i skup proizvod tvrtke OneTrust, koju često nazivaju Microsoftom *data protection softvera*. OneTrust nije samo *consent management* rješenje nego predstavlja potpuno *data protection management* rješenje. *Cookie banner* i upravljanje kolačićima tek su jedan od modula, uz DSAR, RoPA, *vendor management*, *data mapping*, DPIA i brojne druge procese koje veće organizacije imaju obvezu sustavno pokrivati i dokumentirati. Za razliku od Cookiebota, koji je primarno usmjeren na automatizirano skeniranje kolačića, OneTrust pokušava obuhvatiti cijeli životni ciklus osobnih podataka u organizaciji. To ga čini vrlo privlačnim za banke, telekome, velike javne sustave i druge subjekte s razvijenom *governance* strukturom, ali istovremeno znači da je za mali ili jednostavan mrežni sustav takav alat često pretjerano složen, skup i operativno zahtjevan. U kontekstu obrazovnih institucija, takav bi alat bio primjeren velikim sveučilištima, pod uvjetom da organizacije posjeduju adekvatne ljudske resurse za njegovu odgovarajuću integraciju i upotrebu.

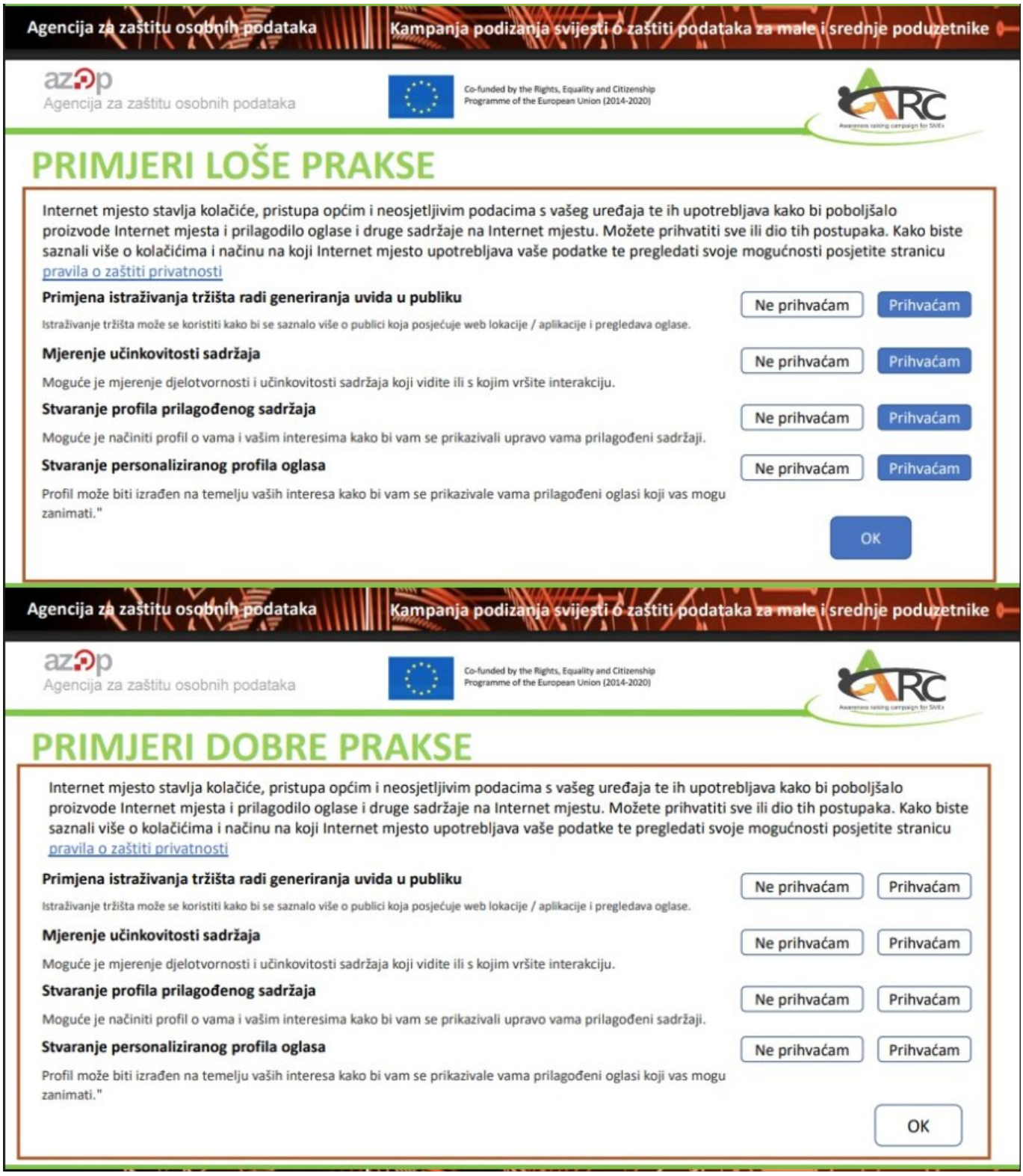
AZOP-ov vodič za kolačiće

Agencija za zaštitu osobnih podataka (AZOP) je kroz edukativne materijale EU projekta ARC (*Awareness Raising Campaign*) navela primjer kako prozor za privolu smije, a kako nikako ne smije izgledati, održavajući važeće pravne standarde za privolu.

Slika 4.

Tako primjerice *cookie* obavijest ne smije sadržavati unaprijed označene kućice za privolu (potrebno je da korisnik davanje privole poprati aktivnim odabirom, ne prihvaćanjem unaprijed ispunjenog obrasca). Zatim, opcije prihvaćanja i odbijanja trebaju biti jednake težine i vizualno ravnopravne, skrolanje po stranici nije zamjena za aktivni odabir opcije i slično. Ispravno dizajnirana obavijest ne bi trebala funkcionirati kao prepreka ili iritantna barijera koju korisnik želi što prije ukloniti, već kao transparentan alat za informiranje. U tzv. „prvom sloju“, odnosno onom dijelu obavijesti koji je odmah vidljiv posjetitelju, moraju biti zadovoljeni strogi kriteriji vizualne i funkcionalne ravnopravnosti. Temelj tog pristupa leži u jasnoj opciji odbijanja; korisniku treba biti omogućeno da

kaže „ne“ jednako lako i brzo kao što može reći „da“. U praksi to znači da gumbi za prihvaćanje svih kolačića i odbijanje svih (ili prihvaćanje samo nužnih) trebaju biti vizualno istaknuti na isti način i postavljeni jedan pored drugog, kako bi se izbjeglo bilo kakvo sugestivno navođenje korisnika prema opciji koju preferira vlasnik stranice.



Slika 5.

Odabir „sve ili ništa“ nije adekvatan jer sustav upravljanja privolama treba nuditi granularnost, omogućujući korisniku da, ukoliko to želi, uđe u postavke i selektivno odabere kategorije kolačića na koje pristaje, poput statistike, marketinga ili preferencija sadržaja, odvojeno jedne od drugih. Sve te

opcije trebaju biti opisane razumljivim jezikom, bez kompliciranog pravnog žargona, kako bi prosječan posjetitelj točno znao tko prikuplja njegove podatke i u koju svrhu. Također, poveznica na detaljnu obavijest o obradi podataka treba biti jasno dostupna unutar samog *bannera*, prije nego što korisnik uopće donese odluku o privoli.

Važno je naglasiti i često zanemaren aspekt povlačivosti privole. Pristanak korisnika nije jednokratan čin koji je zauvijek uklesan u kamen i nepromjenjiv, upravo suprotno. Na mrežnoj stranici treba postojati lako dostupna opcija, obično smještena u podnožju stranice ili u obliku diskretne ikone, koja posjetitelju omogućuje da u bilo kojem trenutku promijeni mišljenje ili povuče privolu jednako lagano kao što ju je i dao. Za više primjera i informacija konzultirajte AZOP-ov vodič (na adresi: https://arc-rec-project.eu/wp-content/uploads/2022/01/Obavijesti-o-kolacicima-primjeri.pdf).

Umjesto zaključka

Možda najpragmatičniji razlog zašto znanstvene organizacije moraju hitno uvesti red u svoje kolačiće leži u novcu. Europska komisija, kroz programe poput Horizon Europe, sve više postavlja etičko upravljanje podacima kao uvjet za financiranje. Evaluatori projekata više ne gledaju samo znanstvenu izvrsnost. Gleda se i tzv. *open science* pristup i etika podataka. Ako institucija ne može demonstrirati kontrolu nad time tko i kako prikuplja podatke posjetitelja na njihovim diseminacijskim kanalima, dovodi se u pitanje i njihova sposobnost rukovanja osjetljivim istraživačkim podacima. Neusklađen *cookie banner* na stranici projekta može biti onaj „crveni karton“ koji ukazuje na nemar u upravljanju podacima. Za znanstvene i obrazovne organizacije, implementacija ili barem sustavno korištenje osnovnih funkcija takvih sustava znači prelazak s deklarativne brige o privatnosti na stvarnu, tehnički provedivu zaštitu. To je korak kojim se vraća povjerenje javnosti u funkcioniranje javnih ustanova i zaštitu temeljnih prava građana u digitalnom prostoru.