REPUBLIKA HRVATSKA
AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA

PREDMET: Obrada osobnih podataka putem kolačića i pružanje informacija ispitanicima vezano za obradu osobnih podataka

- preporuka, daje se

Agencija za zaštitu osobnih podataka (dalje u tekstu: Agencija), nadzorno tijelo u smislu odredbe članka 51. UREDBE (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) SL EU L119 i članka 4. Zakona o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, 42/18, dalje u tekstu: Zakon), odgovorna je za praćenje primjene Opće uredbe o zaštiti podataka. Navedena Opća uredba o zaštiti podataka je od 25. svibnja 2018., u obvezujućoj primjeni u svim državama članicama, pa tako i u Republici Hrvatskoj. Vodeći računa o tome da Agencija, između ostalog, prati i provodi primjenu Opće uredbe o zaštiti podataka, te promiče osviještenost voditelja obrade i izvršitelja obrade o njihovim obvezama iz Opće uredbe o zaštiti podataka, u nastavku navodimo kako slijedi:

Obrada osobnih podataka putem kolačića u zakonodavnom okviru Europske unije propisana je Direktivom 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) te Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektroničke komunikacijske mreže i usluge (Direktiva o univerzalnim uslugama), a navedene direktive su u Republici Hrvatskoj implementirane u Zakon o elektroničkim komunikacijama (NN 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17).

Vezano za korištenje tzv. kolačića kao poseban zakon primjenjuje se Zakon o elektroničkim komunikacijama („Narodne novine“ broj 73/08, 90/11, 132/12, 80/13, 71/14). Tako je člankom 100. stavkom 4. citiranog Zakona propisano kako je korištenje elektroničkih komunikacijskih mreža za pohranu podataka ili za pristup već pohranjenim podacima u terminalnoj opremi pretplatnika ili korisnika usluga dopušteno samo u slučaju kada je taj pretplatnik ili korisnik usluga **dao svoju privolu, nakon što je dobio jasnu i potpunu obavijest u skladu s posebnim propisima o zaštiti osobnih podataka, i to osobito o svrhama obrade podataka**. Time se ne može spriječiti tehnička pohrana podataka ili pristup podacima isključivo u svrhu obavljanja

prijenosa komunikacija putem elektroničke komunikacijske mreže, ili, ako je to nužno, radi pružanja usluga informacijskog društva na izričit zahtjev pretplatnika ili korisnika usluga.

Sukladno navedenom, pravna osnova za prikupljanje osobnih podataka korištenjem kolačića (pohranjenih na računalo/terminalnu opremu krajnjeg korisnika), osim u točno navedenim iznimnim slučajevima, je privola krajnjeg korisnika koja treba biti usklađena sa odredbama Opće uredbe o zaštiti podataka, točnije člankom 4. stavkom 1. točkom 11 koja definira privolu kao svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

U tom smislu pod elementom „**dobrovoljna**" podrazumijeva se istinski izbor korisnika web mjesta. U pravilu, Općom uredbom o zaštiti podataka propisuje se da ako ispitanik nema istinski izbor i ako smatra da je obvezan pristati ili će u protivnom trpjeti negativne posljedice, privola neće biti valjana tj. dobrovoljno dana. **Ako je privola uključena u druge uvjete kao njihov neprenosivi dio, pretpostavlja se da nije dana dobrovoljno. Stoga se privola neće smatrati dobrovoljnom ako ispitanik ne može odbiti ili povući svoju privolu bez štetnih posljedica.**

Usluga može uključivati višestruke postupke obrade u više svrha. U takvim slučajevima ispitanici bi trebali imati slobodu izbora svrhe koju prihvaćaju umjesto da moraju dati privolu za cijeli skup svrha obrade. U određenom slučaju može se dopustiti nekoliko privola za početak pružanja usluge, u skladu s Općom uredbom o zaštiti podataka. U uvodnoj izjavi 43. objašnjava se da se privola ne smatra dobrovoljnom ako proces/postupak dobivanja privole ne omogućuje ispitanicima davanje zasebne privole za pojedine postupke obrade osobnih podataka (npr. samo za neke postupke obrade, a ne za druge) unatoč tome što je primjerena pojedinačnom slučaju. U navedenom smislu potrebno je naglasiti kako bi to značilo kako za preglednike tako i za voditelje obrade, da bi bilo nevaljano kada bi nudili jedino opciju „Prihvati sve kolačiće" jer tako ne bi omogućili korisnicima davanje potrebe precizno definirane privole. Međutim, preglednici bi trebali omogućiti korisnicima/ispitanicima donošenje informirane i svjesne odluke o prihvaćanju svih kolačića kako bi spriječili sve buduće zahtjeve za davanje privole za web mjesta koja budu posjećivali. O navedenom osobito govori i Radni dokument 02/2013 WP29 koji sadrži smjernice za dobivanje pristanka/privole za kolačiće kako slijedi:

„*Iako je Direktivom o e-privatnosti propisana potreba za pristankom za pohranu ili pristup kolačićima praktična primjena zakonskih zahtjeva razlikuje se od operatora web stranica u državama članicama EU. Trenutno promatrane implementacije temelje se na jednoj ili više sljedećih praksi, iako je važno napomenuti da svaka može biti korisna komponenta mehanizma pristanka, korištenje pojedinačne prakse izolirano malo je vjerojatno da bi moglo dati valjanu suglasnost jer moraju biti prisutni svi elementi valjanog pristanka (npr. učinkovit mehanizam izbora također zahtijeva obavijest i informacije):*

- *odmah vidljiva obavijest da web mjesto koriste razne vrste kolačića, pružaju informacije slojevitog pristupa, obično nude vezu ili seriju veza, gdje korisnik može saznati više o vrstama kolačića koji se koriste,*
- *odmah vidljiva obavijest da korisnik upotrebom web stranice pristaje na kolačiće koje web stranice postavljaju,*

- *informacije o tome kako korisnici mogu označiti i kasnije povući svoje želje u vezi s kolačićima, uključujući podatke o radnji potrebnoj za izražavanje takve sklonosti,*
- *mehanizam kojim korisnik može odlučiti prihvatiti sve ili neke ili odbiti kolačiće,*
- *mogućnost da korisnik naknadno promijeni prethodnu prednost u vezi s kolačićima.*

Navedeno je svakako primjenjivo kada govorimo, između ostalog, i o tzv. granularnosti/slojevitosti privole. Naime, člankom 6. stavkom 1. točkom (a) Opće uredbe o zaštiti podataka potvrđuje se da ispitanik mora dati privolu u jednu posebnu svrhu ili više njih i da u pogledu svake od njih ima mogućnost izbora. Zahtjevom da privola mora biti **„posebna"** nastoji se osigurati stupanj korisnikova nadzora i transparentnost za ispitanika. Taj zahtjev nije izmijenjen Općom uredbom o zaštiti podataka i ostaje usko povezan sa zahtjevom informirane privole. Ukratko, kako bi ispunio uvjet posebnosti privole, voditelj obrade mora osobito primijeniti specifikaciju svrhe kao zaštitnu mjeru od širenja namjene, granularnost u zahtjevima za privolu i jasno razdvajanje informacija koje se odnose na dobivanje privole za aktivnosti obrade podataka od informacija o drugim pitanjima.

Tu je svakako nužno spomenuti da su pravne osnove za obradu podataka pa tako i privolu usko i neodvojivo povezane sa **svrhom obrade osobnih podataka**, osobito uzimajući u obzir obvezu poštivanje načela obrade osobnih podataka iz članka 5. Opće uredbe o zaštiti podataka. Dakle, sukladno načelo „ograničenja obrade" za zakonitu i poštenu obradu podataka moraju se ispuniti tri zahtjeva, odnosno osobni podaci se moraju prikupljati u posebne (određene/specificirane), izričite i zakonite svrhe. Stoga voditelj obrade mora pažljivo razmotriti u koju će svrhu ili svrhe biti obrađivani osobni podaci i ne smije prikupljati osobne podatke koji nisu potrebni, primjereni ili relevantni za svrhu ili svrhe kojima se namjerava služiti. Da bi se utvrdilo je li obrada podataka u skladu sa zakonom i utvrdi koje se zaštitne mjere zaštite podataka trebaju primijeniti preduvjet je da se utvrde konkretne svrhe za koje je potrebno prikupljanje i obrada osobnih podataka. Stoga se može zaključiti da se svrhe moraju navesti prije samog prikupljanja i obrade osobnih podataka. Svrha obrade mora biti jasno i posebno identificirana tj. ona mora biti dovoljno detaljna da se utvrdi kakva je vrsta obrade i je li uključena u određenu svrhu te da se omogući da se može procijeniti poštivanje zakona i primijeniti zaštitne mjere zaštite podataka.

Međutim, potrebno je napomenuti kako se osobni podaci mogu prikupljati u više svrha. U nekim su slučajevima svrhe, iako različite, ipak mogu biti povezane u određenoj mjeri ili pak mogu biti nepovezane. Ovdje se postavlja pitanje u kojoj mjeri voditelj obrade treba specificirati svaku od tih zasebnih svrha i koliko dodatnih detalja treba navesti. Za „povezane" procese obrade može biti koristan koncept sveukupne svrhe, pod čijim se kišobranom odvija niz zasebnih operacija obrade. Voditelji obrade bi trebali izbjegavati identificirati samo jednu široku svrhu kako bi opravdali različite daljnje aktivnosti obrade koje su zapravo samo na daljinu povezane sa stvarnom početnom svrhom. U konačnici, kako bi se osigurala sukladnost s člankom 5. stavkom 1. točkom (b), svaka zasebna svrha trebala bi biti navedena dovoljno detaljno da se može procijeniti je li prikupljanje osobnih podataka u tu svrhu zakonito, pošteno i transparentno.

Nadalje, da bi privola bila valjana ispitanik mora biti u dovoljnoj mjeri **informiran** na temelju članka 5. Opće uredbe o zaštiti podataka, odnosno zahtjev transparentnosti jedno je od temeljnih načela, koje je usko povezano s načelima poštenosti i zakonitosti. Pružanje informacija ispitanicima prije dobivanja njihove privole ključno je kako bi im se omogućilo donošenje utemeljene odluke, razumijevanje onoga na što pristaju te ostvarivanje prava na povlačenje privole. Ako voditelj obrade ne pruži dostupne informacije, korisnik ne može ostvariti nadzor te će privola biti nevažeća osnova za obradu.

Stoga je obveza svakog voditelja obrade zadovoljiti minimalne zahtjeve u pogledu sadržaja kako bi privola bila „informirana" uzimajući u obzir članak 13. Opće uredbe o zaštiti podataka.

Naime, kako bi privola bila informirana potrebno je obavijestiti ispitanika o određenim elementima koji su ključni za izbor. **Stoga, Agencija za zaštitu osobnih podataka uzimajući u obzir Smjernice o privoli u skladu s Uredbom 2016/679, WP29 i Odluku Suda Europske unije (ECLI:EU:C:2019:801) u predmetu C-673/17, smatra da je za dobivanje valjane privole prilikom obrade osobnih podataka putem kolačića (cookies) potrebno navesti najmanje sljedeće informacije iz članka 13. Opće uredbe o zaštiti podataka:**

- identitet i kontakt podatke voditelja obrade,
- svrhu svakog pojedinog postupka obrade za koju se traži privola (specificirana i posebna svrha za svaki postupak obrade),
- vrste osobnih podataka koji će se prikupljati i obrađivati,
- postojanje prava na povlačenje privole (koje mora biti jednostavno kao i njezino davanje, obratiti pozornost na članak 7. stavak 3.),
- primatelje ili kategorije primatelja (ako se zna koji su to primatelji primjerice ako se koriste tzv. kolačići treće strane)
- razdoblje pohrane osobnih podataka ili bar kriterije kojima bi se utvrdilo to razdoblje (primjerice trajanje određenog kolačića ili skupine kolačića)
- prema potrebi informacije o korištenju podataka za automatizirano donošenje odluka u skladu s člankom 22. stavkom 2. točkom (c);
- moguće rizike ako dolazi do eventualnih prijenosa podataka zbog nepostojanja odluke o prikladnosti i odgovarajućih zaštitnih mjera (kako je opisano u članku 46.)

Navedene informacije ispitanicima će najčešće biti pružene u dokumentu pod nazivom „Politika privatnosti", a isti mora biti napisan na jednostavan i razumljiv način te lako dostupan posjetiteljima web stranica.

Međutim, potrebno je napomenuti kako za određene vrste obrade podataka pa tako osobnih podataka putem kolačića postoji izuzetak kada govorimo o zakonitosti obrade za koji je voditeljima obrade potreba privola ispitanika/korisnika. Tako članak 100. stavak 4. Zakona o elektroničkim komunikacijama uzimajući u obzir članak 5.3. Direktive o e-privatnosti omogućuje da se kolačići izuzmu iz zahtjeva informirane privole, ako ispunjavaju jedan od sljedećih kriterija:

- ako se kolačić se upotrebljava „isključivo u svrhu obavljanja prijenosa komunikacije preko elektroničke komunikacijske mreže“,
- ako je kolačić "strogo neophodan/nužan kako bi pružatelj usluge informacijskog društva izričito tražio od pretplatnika ili korisnika da pruži uslugu".

Vezano uz navedene kriterije potrebno je napomenuti kako WP29 u Mišljenju 04/2012 o **izuzeću kolačića navodi da se najmanje 3 elementa mogu smatrati strogo potrebnim da bi se komunikacija odvijala preko mreže dviju strana: sposobnost usmjeravanja podataka preko mreže (osobito prepoznavanjem krajnjih točaka komunikacije), mogućnost razmjene podataka u njihovom predviđenom redoslijedu (posebno numeriranjem paketa podataka) te sposobnost otkrivanja pogrešaka u prijenosu ili gubitka podataka.**
Nadalje, u drugom navedenom kriteriju sugerira se da europski zakonodavac želi osigurati da test za osposobljenost za takvo izuzeće mora ostati visok, odnosno kolačić mora istodobno proći dva sljedeća ispitivanja: je li korisnik izričito zatražio uslugu informacijskog društva; je li korisnik (ili pretplatnik) učinio pozitivnu akciju odnosno zatražio uslugu s jasno definiranim perimetrom i je li kolačić strogo potreban za omogućavanje usluge informacijskog društva (ako su kolačići onemogućeni, usluga neće raditi).

Uzimajući u obzir analizu koja je provedena u navedenom Mišljenju o izuzeću kolačića, ista je pokazala da **sljedeći kolačići mogu biti izuzeti iz informiranog pristanka pod određenim uvjetima, samo ako se ne koriste u dodatne svrhe:**

1) kolačići za unos korisnika (id-sesije), za vrijeme trajanja sesije ili trajni kolačići u nekim slučajevima ograničeni na nekoliko sati,
2) kolačići za provjeru autentičnosti, koji se koriste za provjeru autentičnosti usluga, tijekom trajanja sesije,
3) sigurnosni kolačići usmjereni na korisnika, koji se koriste za otkrivanje zloupotrebe autentičnosti, ograničeno uporno trajanje,
4) kolačići sesije multimedijskog sadržaja (kao što su flash player-i) tijekom trajanja sesije,
5) kolačići sesije za uravnoteženije učitavanje, za vrijeme trajanja sesije,
6) kolačići za prilagođavanje korisničkog sučelja u trajanju sesije (ili nešto više),
7) kolačići za dijeljenje sadržaja društvenih mreža/treće strane za prijavu njihovih članova.

Uzimajući u obzir društvene mreže, WP29 primjećuje da je za **upotrebu kolačića društvenih mreža u druge svrhe, osim za pružanje funkcionalnosti koje su njihovi članovi izričito zatražili, potrebna privola osobito ako te svrhe uključuju praćenje korisnika na web stranicama.** Također, WP29 podsjeća da se marketinški kolačići trećih strana ne mogu izuzeti od pristanka te dalje pojašnjava da bi privola bila potrebna i za operativne svrhe povezane s oglašavanjem trećih strana, kao što su ograničenje učestalosti, financijska evidencija, pridruživanje oglasa, otkrivanje prijevara klikova, istraživanje i tržište analiza, poboljšanje proizvoda i uklanjanje pogrešaka.

Sukladno navedenom Agencija za zaštitu osobnih podataka navodi kako je važno ispitati što je nužno i potrebno s gledišta korisnika/ispitanika, a ne davatelja usluga/voditelja obrade tj. za odlučivanje je li pojedini kolačić moguće izuzeti od načela davanja informirane privole važno

je pažljivo provjeriti ispunjava li jedan od dva kriterija za izuzeće iz članka 100. stavka 4. Zakona o elektroničkim komunikacijama. Nakon pažljivog ispitivanja, ako se zadržavaju značajne sumnje u primjenu kriterija za izuzeće ili ne, operatori web stranica trebali bi pomno ispitati postoji li u praksi prilika za privlačenje korisnika na jednostavan, nenametljiv način, izbjegavajući na taj način bilo kakvu pravnu nesigurnost.

Također, podsjećamo na odredbe članaka 25. i 32. Opće uredbe o zaštiti podataka **kojima je propisano provođenje odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka.** Svaki voditelj obrade dužan je poduzimati i provoditi odgovarajuće tehničke i organizacijske mjere zaštite koje imaju za cilj osigurati **sigurnost i povjerljivost obrade osobnih podataka**, odnosno sprječavanje neovlaštenog pristupa ili neovlaštenog raspolaganja osobnim podacima kao i tehničkoj opremi kojom se koristi (npr. smanjenje količine podataka, pristup osobnim podacima uporabom korisničkog imena i lozinke, podizanje sigurnosti web stranice-SSL certifikat/HTTPS protokol, pseudonimizacija, izrada sigurnosnih kopija, bilježenje pristupa podacima, potpisivanje izjava o povjerljivosti osoba koje su u obradi osobnih podataka, i sl.).

Nastavno na prethodno navedene zakonske odredbe Opće uredbe o zaštiti podataka, Zakona i Zakona o elektroničkim komunikacijama, **Agencija preporučuje voditeljima obrade koji prikupljaju osobne podatke ispitanika na Internet stranicama putem kolačića, da obavijest o obradi osobnih podataka putem kolačića i privolu za obradu osobnih podataka putem kolačića i informiranje ispitanika o obradi osobnih podataka usklade s prethodno navedenim. Također, Agencija preporučuje da voditelji obrade koji obrađuju osobne podatke putem Internet stranica implementiraju i navedene tehničke mjere zaštite na iste.**