



Digitalna prava u praksi

Zaštita osobnih podataka i nova EU pravila za digitalne tehnologije

Praktična brošura za organizacije civilnog društva, aktiviste, lokalne vlasti i zainteresirane zajednice na Zapadnom Balkanu, nastala na temelju online radionice održane 24. lipnja 2026. godine na hrvatskom jeziku.

Sadržaj brošure

- GDPR i osnovni pojmovi zaštite osobnih podataka
- pravne osnove i načela obrade osobnih podataka
- prava ispitanika, sigurnost i povrede osobnih podataka
- Digitalni omnibus i AI omnibus
- odgovorno korištenje digitalnih i AI alata u radu OCD-ova i lokalnih samouprava

Aktivnost/publikacija izrađena je u sklopu projekta „Razvijanje digitalne pismenosti za predstavnike OCD-ova i lokalnih vlasti Zapadnog Balkana”, koji se odvija uz financijsku potporu Grada Zagreba.

Stajališta izražena u ovoj publikaciji isključiva su odgovornost CROSOL-a i ne odražavaju nužno stajališta Grada Zagreba.

1. O ovoj brošuri

Ova brošura prenosi ključne poruke s CROSOL-ove online radionice „Digitalna prava u praksi” u praktičan referentni materijal za organizacije i institucije koje rade s ljudima, zajednicama i digitalnim alatima. Namijenjena je organizacijama civilnog društva, aktivistima, zaposlenicima jedinica lokalne samouprave i zainteresiranim sudionicima iz Crne Gore, Srbije, Bosne i Hercegovine i Hrvatske.

Radionica je spojila dvije povezane teme: osnovne obveze zaštite osobnih podataka u svakodnevnom radu organizacija civilnog društva i lokalnih zajednica te širu raspravu u Europskoj uniji o regulaciji digitalnih tehnologija, uključujući Digitalni omnibus i Digitalni omnibus o umjetnoj inteligenciji.

Kako koristiti brošuru

Brošuru koristite kao polazište za interne rasprave, uvođenje zaposlenika i volontera, planiranje projekata, komunikaciju s korisnicima, te praćenje javnih politika. Ovaj materijal nije pravni savjet i ne može zamijeniti konzultacije s kvalificiranim pravnikom ili nadležnim tijelom za zaštitu podataka u vašoj zemlji.

Zašto je tema važna

Organizacije koje prikupljaju podatke o korisnicima, članovima, volonterima, zaposlenicima, sudionicima događanja ili online publici odgovorne su postupati s tim podacima zakonito, pošteno, transparentno i sigurno. Istodobno, digitalna regulacija utječe na alate koji se koriste u javnim uslugama, zagovaranju, kampanjama, sudjelovanju građana, novinarstvu i radu sa zajednicom.

2. Zaštita podataka ukratko

Zaštita podataka nije samo obveza usklađenosti s propisima. Ona je dio organizacijske kulture koja poštuje dostojanstvo, autonomiju i povjerenje. Na radionici su naglašena tri razloga donošenja GDPR-a: vraćanje kontrole građanima, stvaranje dosljedne zaštite u cijeloj EU i ugrađivanje privatnosti u organizacijsku praksu kroz načelo privacy by design.

Za zemlje Zapadnog Balkana standardi zaštite podataka u EU važni su i zato što se nacionalni zakoni oblikuju kroz usklađivanje s pravnim okvirom EU. To je relevantno za prekograničnu suradnju, partnerstva s organizacijama iz EU, javnim tijelima i donatorima, kao i za buduće rasprave o adekvatnosti.

Osnovni pojam	Praktično pravilo
Osobni podaci: svaka informacija koja se odnosi na identificiranu ili moguće identificiranu osobu.	Pretpostavite da je riječ o osobnom podatku ako se osoba može identificirati izravno ili neizravno.
Obrada: svaka radnja nad osobnim podacima, uključujući prikupljanje, pohranu, korištenje, dijeljenje ili brisanje.	Pseudonimizirani podaci obično i dalje zahtijevaju zaštitu jer je ponovna identifikacija ponekad moguća.
Pseudonimizacija: podatke više nije moguće pripisati osobi bez dodatnih informacija.	Stvarna anonimizacija je zahtjevnija; budite oprezni pri objavi skupova podataka, fotografija ili opisa slučajeva.
Anonimizacija: podaci su obrađeni tako da ponovna identifikacija više nije moguća.	Prije objave procijenite može li se identitet ipak otkriti kombiniranjem različitih informacija.

Korisna navika: prije nego prikupite bilo koji podatak, pitajte se: Zašto nam je potreban? Što ćemo s njime raditi? Tko će mu pristupiti? Koliko dugo ćemo ga čuvati? Kako ćemo ga zaštititi? Kako ćemo to objasniti osobi na koju se podaci odnose?

3. Tipične obrade osobnih podataka u OCD-ima i lokalnim samoupravama

Organizacije civilnog društva i jedinice lokalne samouprave obrađuju osobne podatke u brojnim svakodnevnim aktivnostima. To što je rad usmjeren javnom interesu, neprofitan ili manjeg opsega ne uklanja potrebu za poštovanjem načela zaštite podataka.

Usluge i aktivnosti OCD-a	Zaposlenici, članovi i volonteri
• kontakt obrasci i upiti e-mailom • zahtjevi za besplatnu pravnu pomoć ili savjetovanje • registracije za događanja i edukacije • pretplate na newsletter • kampanje, zagovaračke i medijske aktivnosti • kolačići i analitika na web stranicama • rad na slučajevima s ranjivim korisnicima	• natječaji za posao i zapošljavanje • obračun plaća i druge zakonom propisane evidencije • članovi, skupštine i upravljačka tijela • evidencije i ugovori s volonterima • objava fotografija ili biografija zaposlenika • videonadzor ureda ili javnih prostora

Lokalne samouprave dodatno mogu obrađivati podatke u javnim savjetovanjima, programima za mlade, dodjeli potpora, socijalnim uslugama, lokalnim registrima, javnim događanjima, e-uslugama, pritužbama, peticijama i participativnom budžetiranju. U tim je aktivnostima često riječ o javnoj zadaći ili pravnoj obvezi, ali i dalje vrijede transparentnost, minimizacija podataka i sigurnost.

Nemojte prikupljati podatke „za svaki slučaj”. Registracijski obrazac za radionicu obično ne treba OIB, datum rođenja, punu adresu ili osjetljive podatke. Prikupite samo ono što je nužno za jasno navedenu svrhu.

4. Odabir pravne osnove obrade

Svaka aktivnost obrade treba imati pravnu osnovu. Nijedna pravna osnova nije automatski „bolja” od drugih: odgovarajuća osnova ovisi o svrsi, ulozi organizacije, odnosu s osobom na koju se podaci odnose i primjenjivom nacionalnom pravu. Odabir treba napraviti prije početka obrade i interno ga dokumentirati.

Šest pravnih osnova	Primjeri s radionice
• privola • izvršenje ugovora • pravna obveza • zaštita životno važnih interesa • javna zadaća / javni interes • legitimni interes	• Pravna obveza: evidencije zaposlenika, članova i volontera propisane zakonom. • Ugovor: prijava za članstvo ili odnos pružanja besplatne pravne pomoći/usluge. • Legitimni interes: neki oblici videonadzora, fotografije zaposlenika ili novinarska aktivnost, uz vaganje interesa i zaštitne mjere. • Privola: pretplate na newsletter i nenužni kolačići.

Privola nije prečac. Privola mora biti dobrovoljna, posebna, informirana i nedvosmislena. Povlačenje privole mora biti jednako jednostavno kao i njezino davanje. Izbjegavajte oslanjanje na privolu kada postoji izrazita neravnoteža moći ili kada je primjerenija druga pravna osnova.

Važno: gore navedeni primjeri su ilustrativni. Nacionalna pravila mogu biti stroža, osobito za radne odnose, javna tijela, videonadzor, djecu, zdravstvene podatke ili socijalne usluge.

5. Šest načela za svakodnevnu usklađenost

Zakovitost, poštenost i transparentnost

Imajte pravnu osnovu, obrađujte podatke na način koji osoba razumno može očekivati i pružite jasne informacije o obradi.

Ograničavanje svrhe

Prikupljajte podatke za posebne, izričite i zakonite svrhe. Nemojte ih naknadno koristiti na način koji nije spojiv s tim svrhama.

Smanjenje količine podataka

Obrađujte samo one podatke koji su primjereni, relevantni i nužni za određenu svrhu.

Točnost

Poduzmite razumne korake kako bi podaci bili točni te bez odgode ispravite ili izbrišite netočne podatke.

Ograničenje pohrane

Identificirajuće podatke čuvajte samo onoliko dugo koliko je potrebno za svrhu ili koliko to zahtijeva zakon.

Cjelovitost i povjerljivost

Zaštitite podatke od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja.

6. Posebne kategorije podataka zahtijevaju dodatnu pažnju

Posebne kategorije osobnih podataka uključuju podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu, zdravstvene podatke, genetske i biometrijske podatke te podatke o spolnom životu ili spolnoj orijentaciji. Ove su kategorije osobito relevantne za mnoge OCD-ove jer rad na ljudskim pravima, socijalnoj uključenosti, zdravlju, pravima manjina, rodnoj ravnopravnosti i demokraciji često uključuje osjetljive kontekste.

Prema članku 9. GDPR-a obrada posebnih kategorija podataka načelno je zabranjena, osim ako se primjenjuje određena iznimka. Jedna od iznimki može se odnositi na zaklade, udruge ili druga neprofitna tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljevima, kada je obrada dio njihovih legitimnih aktivnosti, odnosi se na članove, bivše članove ili osobe koje su s organizacijom u redovitom kontaktu, postoje odgovarajuće zaštitne mjere i podaci se bez privole ne otkrivaju izvan organizacije.

Dobra praksa	Primjeri visokog rizika
- prikupljajte osjetljive podatke samo kada su stvarno nužni - odvojite osjetljive evidencije od općih kontakt-lista - ograničite pristup samo na osposobljeno osoblje - koristite šifriranu pohranu za datoteke i uređaje - izbjegavajte objavu identifikacijskih detalja u studijama slučaja - dokumentirajte koja se iznimka iz članka 9. ili nacionalnog prava primjenjuje	- popisi korisnika prema zdravstvenom statusu ili etnicitetu - politička pripadnost izvedena iz prisustva na događaju - evidencije preživjelih nasilja ili diskriminacije - fotografije ili priče koje otkrivaju migrantski, zdravstveni ili manjinski status - AI alati koji profiliraju ranjive skupine

7. Uloge i odgovornost

Posao zaštite podataka lakši je kada su uloge jasne. Organizacije trebaju znati kada same odlučuju o svrhama i sredstvima obrade, kada obrađuju podatke za nekoga drugoga te kada neka druga organizacija djeluje kao izvršitelj obrade za njih.

Glavne uloge	Tipični aranžmani
• Voditelj obrade: odlučuje zašto i kako se osobni podaci obrađuju. • Izvršitelj obrade: obrađuje osobne podatke u ime voditelja obrade. • Nadzorno tijelo: neovisno javno tijelo koje nadzire i provodi pravo zaštite podataka. • Službenik za zaštitu podataka: savjetuje i prati usklađenost kada je DPO obvezan ili imenovan.	• udruga kao voditelj obrade za prijave na događaj • online platforma za newsletter kao izvršitelj obrade • općina ili grad kao voditelj obrade za javno savjetovanje • cloud usluga ili IT tvrtka kao izvršitelj obrade • zajednički rad s partnerima koji zahtijeva jasno razgraničenje uloga

Što radi službenik za zaštitu podataka

Službenik za zaštitu podataka savjetuje organizaciju o pravnim obvezama, prati usklađenost sa zakonom i internim politikama, surađuje s nadzornim tijelom, pomaže pojedincima u ostvarivanju njihovih prava, savjetuje pri procjenama učinka na zaštitu podataka te djeluje neovisno i bez sukoba interesa.

Čak i kada DPO nije zakonski obvezan, korisno je imenovati odgovornu osobu ili tim za pitanja zaštite podataka, povrede i interne procedure.

8. Prava pojedinaca i povrede osobnih podataka

Osobe čije podatke obrađujete imaju određena prava. U praksi, vaša organizacija trebala bi znati kako zaprimiti, evidentirati, provjeriti i odgovoriti na zahtjeve pojedinaca.

Prava pojedinaca	Odgovor na povredu osobnih podataka
• pravo na pristup osobnim podacima • pravo na ispravak netočnih podataka • pravo na prenosivost podataka • pravo na brisanje • pravo na ograničenje obrade • pravo na prigovor na obradu • pravo da se u određenim slučajevima ne podliježe isključivo automatiziranom odlučivanju	• Povreda je sigurnosni incident koji dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima. • Odmah obavijestite odgovornu osobu. • Procijenite rizik za pojedince i dokumentirajte incident. • Kada je potrebno, obavijestite nadzorno tijelo u roku od 72 sata. • Kada je rizik visok, bez nepotrebnog odgađanja obavijestite pogođene osobe.

Pripremite se unaprijed. Imajte kratak postupak za odgovor na povredu: tko zaprima prijave incidenta, tko odlučuje o obavješćavanju nadzornog tijela, tko komunicira s pogođenim osobama i gdje se vodi evidencija povreda.

9. Praktična kontrolna lista zaštite podataka

- Mapirajte glavne aktivnosti obrade: sudionici, članovi, volonteri, zaposlenici, korisnici, posjetitelji weba, partneri i dobavljači.
- Za svaku aktivnost definirajte svrhu i pravnu osnovu.
- Uklonite nepotrebna polja iz obrazaca i baza podataka.
- Pripremite jasne obavijesti o privatnosti za događanja, newslettere, savjetovanja, usluge i web stranice.
- Držite privolu odvojeno od drugih uvjeta i čuvajte dokaz o privoli kada se na nju oslanjate.
- Usvojite rokove čuvanja podataka te brišite ili anonimizirajte podatke kada više nisu potrebni.
- Sklopite ugovore s izvršiteljima obrade za IT, cloud, mailing, anketne ili event-platforme.
- Ograničite pristup osjetljivim evidencijama i redovito provjeravajte ovlasti pristupa.
- Koristite snažne lozinke, višefaktorsku autentifikaciju i sigurnu pohranu za datoteke i uređaje.
- Vodite evidenciju povreda i testirajte svoj postupak odgovora na povrede.
- Osposobite zaposlenike, volontere i projektne partnere koji rukuju osobnim podacima.
- Prije objave pregledajte javne komunikacije, fotografije i studije slučaja.
- AI alate koristite samo uz jasna pravila: ne unosite povjerljive, korisničke ili osjetljive osobne podatke u javne ili nekontrolirane alate.

10. EU regulacija digitalnih tehnologija: šira slika

EU regulacija digitalnih tehnologija nije jedan zakon, nego sve širi okvir pravila o zaštiti podataka, podacima u provedbi zakona, platformama, tržištima, pristupu podacima, kibernetičkoj sigurnosti i umjetnoj inteligenciji. Radionica je smjestila raspravu o Digitalnom omnibusu u taj širi regulatorni kontekst.

Instrument	Glavni fokus	Zašto je relevantan za OCD-ove / lokalne vlasti
GDPR	Zaštita osobnih podataka	Obavijesti o privatnosti, pravne osnove, prava, sigurnost, povrede i odgovornost.
LED	Zaštita podataka u provedbi zakona	Relevantno kada su uključeni policijski, sigurnosni ili pravosudni podaci.
DSA	Online platforme i upravljanje sadržajem	Transparentnost platformi, sistemski rizici, moderiranje sadržaja i online građanski prostor.
DMA	Veliki digitalni „gatekeeperi“	Tržišno natjecanje, pristup tržištu i moć vrlo velikih platformi.
Data Act / o pravila o podacima	Pristup podacima i njihovo korištenje	Dijeljenje podataka, interoperabilnost i podatkovno vođene usluge.
AI Act	Pravila za AI sustave temeljena na riziku	AI pismenost, transparentnost, visokorizični sustavi i korištenje AI-a u javnom sektoru.
NIS2 / kibernetička sigurnost	Kibernetička sigurnost	Kultura sigurnosti, prijava incidenata i otpornost usluga.

Za manje organizacije i jedinice lokalne samouprave izazov često nije jedan propis, nego kumulativni učinak više preklapajućih okvira, platformi, nabavnih odluka, cloud usluga, AI alata i javnih očekivanja.

11. Digitalni omnibus i AI omnibus

Europska komisija predstavila je u studenome 2025. Digitalni paket s ciljem pojednostavljenja dijelova digitalnog pravnog okvira EU. Paket uključuje prijedloge poznate kao Digitalni omnibus ili Data Omnibus te Digitalni omnibus o umjetnoj inteligenciji. Materijali Komisije opisuju cilj kao pojednostavljenje, smanjenje preklapajućih obveza te podršku inovacijama i konkurentnosti.

AI Omnibus počeo se primjenjivati u cijeloj EU 27. srpnja 2026. te uvodi ciljana pojednostavljenja i dulje rokove za dio obveza iz Akta o umjetnoj inteligenciji. Šira rasprava o Digitalnom omnibusu obuhvaća i podatke, kibernetičku sigurnost te elemente regulacije umjetne inteligencije.

Prikaz Komisije	Zabrinutosti civilnog društva istaknute na radionici
• pojednostaviti i konsolidirati digitalni pravni okvir • smanjiti administrativna opterećenja i preklapanja • poduprijeti inovacije i konkurentnost • uskladiti obveze iz područja podataka, kibernetičke sigurnosti i AI-a • olakšati izvještavanje kroz zajedničke ili jedinstvene postupke	• moguće sužavanje prava i zaštitnih mjera • širenje iznimaka ili slučajeva neprimjene pravila • smanjivanje obveza transparentnosti • odgode zakonskih obveza • ograničeno sudjelovanje ombudsmanskih institucija, OCD-ova i sindikata • snažan utjecaj velikih tehnoloških kompanija

Uravnoteženo čitanje: isti se prijedlog može predstavljati kao administrativno pojednostavljenje iz perspektive institucija, a kao deregulacija ili nazadovanje iz perspektive organizacija koje polaze od zaštite prava. Za OCD-ove i lokalne samouprave ključno je pitanje olakšava li pojednostavljenje usklađenost bez slabljenja zaštite ljudi.

12. Zašto bi civilno društvo i lokalne samouprave trebali obratiti pažnju

Digitalna pravila oblikuju okoliš u kojem organizacije komuniciraju, mobiliziraju građane, pružaju usluge, prikupljaju dokaze, sudjeluju u javnoj raspravi i koriste tehnologiju. Ona također utječu na to kako javne usluge mogu uvoditi umjetnu inteligenciju, digitalni identitet, automatizirane sustave i alate vođene podacima.

Rizici na koje treba paziti	Mogućnosti za djelovanje
- slabija transparentnost može otežati razumijevanje automatiziranih ili platformskih odluka - široke iznimke mogu povećati korištenje osobnih ili osjetljivih podataka bez stvarnih zaštitnih mjera - dulji rokovi provedbe mogu odgoditi praktičnu zaštitu - složena pravila mogu dodatno opteretiti manje organizacije i općine - privatni pružatelji tehnologije mogu dobiti veći utjecaj nad infrastrukturama od javnog interesa	- jačati interno znanje o digitalnim pravima - sudjelovati u javnim savjetovanjima i raspravama - tražiti procjene učinka na temeljna prava za AI projekte u javnom sektoru - regionalno surađivati i razmjenjivati primjere odgovornog korištenja tehnologije - uključiti digitalna prava u zagovaranje, lokalne politike i građanski odgoj

Pitanja za praćenje politika

Tko ima korist od predloženog pojednostavljenja? Koje se obveze odgađaju ili uklanjaju? Jesu li pogođene zajednice konzultirane? Postoji li procjena učinka? Jesu li transparentnost, pravna zaštita i nadzor i dalje dovoljno snažni? Što promjena znači za ranjive skupine?

13. Odgovorno korištenje digitalnih i AI alata

Digitalni alati i sustavi umjetne inteligencije mogu pomoći organizacijama da uštede vrijeme, bolje komuniciraju i analiziraju informacije. Istodobno mogu stvarati rizike ako se koriste bez jasnih pravila, posebno kada su u pitanju osobni podaci, ranjive zajednice ili javne odluke.

Prije korištenja alata	Kada koristite AI rezultate
• definirajte svrhu i očekivanu korist • provjerite hoće li se obrađivati osobni ili osjetljivi podaci • pročitajte uvjete privatnosti i korištenja podataka pružatelja usluge • odlučite tko smije koristiti alat i za koje zadatke • izbjegavajte unos povjerljivih spisa, podataka korisnika ili neobjavljenih osjetljivih dokumenata • procijenite rizike pristupačnosti, jezika i pristranosti	• zadržite ljudski nadzor i konačnu odgovornost • provjeravajte rezultate prema pouzdanim izvorima • ne koristite AI kao jedinu osnovu za odluke koje utječu na ljude • budite transparentni kada je AI bitno oblikovao javnu komunikaciju ili analizu • štitite autorska prava, povjerljive informacije i osobne podatke • vodite evidenciju važnih odluka i analiza

Jednostavno interno AI pravilo: nijedan zaposlenik, volonter ili vanjski suradnik ne bi smio unositi osobne podatke korisnika, članova, prijavitelja, zaposlenika ili volontera u javne AI alate ako organizacija prethodno nije procijenila alat, dokumentirala pravnu osnovu i uspostavila odgovarajuće zaštitne mjere.

14. Korisni mini-predlošci

Kostur obavijesti o privatnosti za događanja

- Tko je voditelj obrade? Navedite naziv organizacije i adresu za kontakt.
- Koji se podaci prikupljaju? Primjerice: ime, e-mail, organizacija, država, potrebe pristupačnosti.
- Zašto se podaci prikupljaju? Registracija, komunikacija o događaju, izvještavanje, evidencija sudjelovanja.
- Koja je pravna osnova? Jasno je definirajte.
- Koliko dugo se podaci čuvaju? Odredite rok čuvanja.
- Tko prima podatke? Event platforma, projektni tim, donator samo u agregiranom obliku, osim ako je drukčije opravdano.
- Koja su prava sudionika i kome se mogu obratiti?

Polja evidencije povrede osobnih podataka

- datum i vrijeme kada je incident otkriven
- što se dogodilo i koji su sustavi/datoteke bili pogođeni
- kategorije i približan broj pogođenih osoba
- kategorije uključenih podataka
- početne mjere za zaustavljanje štete
- procjena rizika
- odluka o obavještanju nadzornog tijela / pojedinaca
- naknadne mjere i naučene lekcije

Polja registra korištenja AI alata

- naziv alata i pružatelj usluge
- svrha i korisnici
- vrste unesenih podataka
- rizici i zaštitne mjere
- koraci ljudske provjere
- datum pregleda i odgovorna osoba

15. Izvori i dodatna literatura

Ova brošura temelji se na prezentacijama pripremljenima za CROSOL-ovu online radionicu „Digitalna prava u praksi“, na projektnoj dokumentaciji CROSOL-a te na odabranim službenim i organizacijskim izvorima navedenima u nastavku. Online izvori provjereni su u kolovozu 2026.

1. Materijali s radionice: „Zaštita osobnih podataka“, CROSOL radionica, 24. lipnja 2026.; „Regulacija digitalne tehnologije u EU“, Politiscope radionica, 24. lipnja 2026.
2. Projektna dokumentacija: CROSOL projekt „Razvijanje digitalne pismenosti za predstavnike OCD-ova i lokalnih vlasti Zapadnog Balkana“.
3. Europska komisija, Data protection explained: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en
4. Europska komisija, Application of the GDPR: https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/application-gdpr_en
5. Europska komisija, Legal grounds for processing data: https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/legal-grounds-processing-data_en
6. Europska komisija, What is a data breach and what do we have to do in case of a data breach?: https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-to-do-in-case-data-breach_en
7. European Data Protection Board, Personal data breaches: https://www.edpb.europa.eu/topics/security-data-breaches/personal-data-breaches_en
8. EUR-Lex, Uredba (EU) 2016/679 – Opća uredba o zaštiti podataka: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
9. Europska komisija, Digital Package: <https://digital-strategy.ec.europa.eu/en/faqs/digital-package>
10. Europska komisija, Simpler digital rules to help EU businesses grow: https://commission.europa.eu/news-and-media/news/simpler-digital-rules-help-eu-businesses-grow-2025-11-19_en
11. Europska komisija, An agile Digital Rulebook for the EU: <https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook>
12. EUR-Lex, Digital Omnibus on AI – adopted text: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3APE_30_2026_REV_1
13. BEUC i partneri, Open Joint Letter on the Digital Omnibus on AI, 8. travnja 2026.: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-029_Open_Joint_Letter_on_the_Digital_Omnibus_on_AI.pdf

Pravna napomena

Ova publikacija edukativni je resurs. Pruža opće informacije i praktičnu orijentaciju, ali ne predstavlja pravni savjet. Uvijek provjerite zakonodavstvo i smjernice primjenjive u vašoj jurisdikciji.

16. O projektu i vidljivosti

Ova brošura izrađena je u sklopu CROSOL-ova projekta usmjerenog na jačanje digitalne pismenosti i odgovornog korištenja digitalnih tehnologija među organizacijama civilnog društva i lokalnim vlastima na Zapadnom Balkanu. Aktivnost se nadovezuje na CROSOL-ovu suradnju s organizacijama i mrežama u regiji te na stručnost organizacije Politiscope u području digitalnih prava, EU regulacije tehnologije i odgovornog korištenja suvremenih tehnologija.

Izjava o vidljivosti donatora

Aktivnost/publikacija izrađena je u sklopu projekta „Razvijanje digitalne pismenosti za predstavnike OCD-ova i lokalnih vlasti Zapadnog Balkana”, koji se odvija uz financijsku potporu Grada Zagreba.

Stajališta izražena u ovoj publikaciji isključiva su odgovornost CROSOL-a i ne odražavaju nužno stajališta Grada Zagreba.



CROSOL – Platforma za međunarodnu građansku solidarnost Hrvatske

www.crosol.hr

Kolovoz 2026.