



**POLOŽAJ ORGANIZACIJA CIVILNOG DRUŠTVA U
KONTEKSTU NOVE REGULATIVE ZAŠTITE LIČNIH
PODATAKA U BOSNI I HERCEGOVINI**

/Analiza normativno – pravnog okvira i praktični priručnik/

Sarajevo, februar 2026. godine

POLOŽAJ ORGANIZACIJA CIVILNOG DRUŠTVA U KONTEKSTU NOVE REGULATIVE ZAŠTITE LIČNIH PODATAKA U BOSNI I HERCEGOVINI: Analiza normativno – pravnog okvira i praktični priručnik

Autori/ca: Miloš Davidović, Tarik Velić, Amila Šišić

Publikacija “Položaj organizacija civilnog društva u kontesktu nove regulative zaštite ličnih podataka u Bosni i Hercegovini je izrađen/a uz podršku regionalnog projekta SMART Balkan – Civilno društvo za povezan Zapadni Balkan kojeg implementira Centar za promociju civilnog društva (CPCD), Center for Research and Policy Making (CRPM) i Institute for Democracy and Mediation (IDM), a finansijski podržava Ministarstvo vanjskih poslova Kraljevine Norveške.

Sadržaj publikacije je isključiva odgovornost autora i ne odražava nužno stavove Centra za promociju civilnog društva, Center for Research and Policy Making (CRPM), Institute for Democracy and Mediation i Ministarsvta vanjskih poslova Kraljevine Norveške.

SADRŽAJ

<u>1. UVOD I POSTUPAK USVAJANJA NORMATIVNO – PRAVNOG OKVIRA.....</u>	5
<u>2. OSNOVNE KATEGORIJE U POSTUPKU ZAŠTITE LIČNIH PODATAKA.....</u>	8
<u>3. OSNOVNI PRINCIPI ZAŠTITE LIČNIH PODATAKA</u>	10
<u>4. TEMELJNI USLOVI ZAKONITE OBRADE LIČNIH PODATAKA.....</u>	11
<u>5. PRAVA NOSILACA PODATAKA PREMA NOVOJ REGULATIVNI ZAŠTITE LIČNIH PODATAKA.....</u>	12
5.1. PRAVO NA ADEKVATAN UVID U SISTEM ZAŠTITE LIČNIH PODATAKA, KAO I NAČINE OSTVARIVANJA PREDVIĐENIH PRAVA NOSIOCA PODATKA (<i>PRAVO IZVEDENO IZ PRINCIPA TRANSPARENTNOSTI</i>).....	12
5.2. PRAVO NA PRISTUP LIČNOM PODATKU:	13
5.3. PRAVO NA ISPRAVKU	13
5.4. PRAVO NA BRISANJE	13
5.5. PRAVO NA OGRANIČENJE OBRADE	14
5.6. PRAVO NA PRENOSIVOST LIČNOG PODATKA	14
5.7. PRAVO NA PRIGOVOR.....	14
<u>6. OGRANIČENJA PRAVA ZAŠTITE LIČNIH PODATAKA</u>	16
<u>7. OBAVEZE KONTROLORA PODATAKA I OBRADIVAČA U POSTUPKU ZAŠTITE LIČNIH PODATAKA.....</u>	17
7.1. OBAVEZE OPERATIVNO – TEHNIČKOG I SIGURNOSNOG KARAKTERA	17
7.2. PROCESNE OBAVEZE.....	18
7.3. OBAVEZE USVAJANJA ODREĐENIH DOKUMENATA I AKATA	21
7.4. OBAVEZA IMENOVANJA SLUŽBENIKA ZA ZAŠTITU LIČNIH PODATAKA	22
<u>8. INSTITUCIJE ZA PROVOĐENJE ZAKONA O ZAŠTITI LIČNIH PODATAKA</u>	24
8.1. STATUS AGENCIJE ZA ZAŠTITU LIČNIH PODATAKA BIH	24
8.2. NADLEŽNOSTI AGENCIJE ZA ZAŠTITU LIČNIH PODATAKA BIH	24
8.3. INSPEKCIJSKI NADZOR.....	25
8.4. STATUS ODLUKA AGENCIJE	25
8.5. SANKCIJE ZA POVREDE ZAKONA.....	26
INTERNI KAPACITETI AGENCIJE	26
<u>9. KLJUČNI IZAZOVI ZA ORGANIZACIJE CIVILNOG DRUŠTVA U POSTUPKU ZAŠTITE LIČNIH PODATAKA</u>	27

9.1. ORGANIZACIJE CIVILNOG DRUŠTVA KAO POSLODAVACI.....	27
9.2. SLOBODA IZRAŽAVANJA	29
<u>10. PRAKTIČNI PRIRUČNIK.....</u>	<u>32</u>
PRILOG 1.	34
PRILOG 2	40
PRILOG 3	43
PRILOG 4.....	45
PRILOG 5	46
PRILOG 6	47
PRILOG 7.....	47

1. UVOD I POSTUPAK USVAJANJA NORMATIVNO – PRAVNOG OKVIRA

Zaštita ličnih podataka jedna je od osnovnih vrijednosti u svakom demokratskom društvu, a pravo na zaštitu ličnih podataka jedan je od segmenata prava na privatnost, kao fundamentalnog ljudskog prava. Ustavom BiH garantuje se osiguranje najvišeg nivoa međunarodno priznatih ljudskih prava i osnovnih sloboda, a prava i slobode predviđeni u Evropskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda i u njenim protokolima direktno se primjenjuju u BiH i imaju prioritet nad svim ostalim zakonima.

U sklopu procesa usklađivanja zakonodavstva Bosne i Hercegovine sa pravnom stečevinom Evropske unije, a kao jedan od ključnih uslova za članstvo BiH u EU, Parlamentarna skupština BiH usvojila je novi Zakon o zaštiti ličnih podataka BiH. Naime, BiH je potpisivanjem Sporazuma o stabilizaciji i pridruživanju,¹ preuzela i obaveze usklađivanja zakonodavstva koje se odnosi na zaštitu ličnih podataka sa pravom EU. Na nivou EU, ova materija sistemski je regulisana Opštom uredbom o zaštiti ličnih podataka (GDPR) iz 2016. godine, a koja se primarno odnosi zaštita pojedinaca u vezi s obradom ličnih podataka unutar EU, slobodno kretanje takvih podataka u okviru EU, kao i iznošenje podataka u treće države. Kao glavni ciljevi GDPR-a navode se vraćanje građanima nadzora nad njihovim ličnim podacima i pojednostavljivanje regulatornog okruženja za međunarodne kompanije ujednačavanjem propisa u cijeloj EU.² U samom obrazloženju Prijedloga novog Zakona o zaštiti ličnih podataka, koje je Parlamentarnoj skupštini podnijelo Vijeće ministara kao predlagač Zakona, navodi se da će BiH usvajanjem ovog Zakona domaće zakonodavstvo iz ove oblasti djelimično uskladiti sa naprijed navedenom Uredbom EU i Direktivom (EU) 2016/680 Evropskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom ličnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona krivičnih djela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka (tzv. Policijska direktiva). Kako stoji u spomenutom Obrazloženju, Zakon je usklađen sa odredbama Uredbe i Direktive na način da je istovjetan odredbama istih, izuzev onih koje se isključivo mogu primijeniti na države koje su države članice EU (npr. odredbe o slobodnom kretanju podataka unutar EU).³ Nadalje, BiH se članom 79. Sporazuma također obavezala da će uspostaviti nezavisna nadzorna tijela s dostatnim finansijskim i ljudskim potencijalima radi učinkovitog praćenja i jamčenja provedbe nacionalnog zakonodavstva o zaštiti ličnih podataka.

Osim obaveze usklađivanja sa pravom EU, BiH je usvajanjem novog Zakona započela sa ispunjavanjem i drugih obaveza koje za nju proizlaze iz međunarodnih ugovora. Naime, BiH je ratificirala Konvenciju Vijeća Evrope za zaštitu osoba s obzirom na automatsku obradu ličnih podataka i Protokol kojim se mijenja i dopunjuje Konvencija. Ova Konvencija je od ključnog značaja za osiguranje prava na privatnost, a time i zaštitu ličnih podataka svakog fizičkog lica. Naime, prema stavu Evropskog suda za ljudska prava, dio prava na privatnost garantovanog

1 „Službeni glasnik BiH – Međunarodni ugovori”, br. 10/08, 1/17 i 8/17

2 Preuzeto sa: https://azlp.ba/GDPR_Menu/Opsta_uredba/default.aspx?id=2366&langTag=bs-BA&template_id=149&pageIndex=1

3 Preuzeto sa: https://static.parlament.ba/doc/172651_B%20Obrazlo%20c5%20beenje%20Prijedloga%20Zakona.pdf

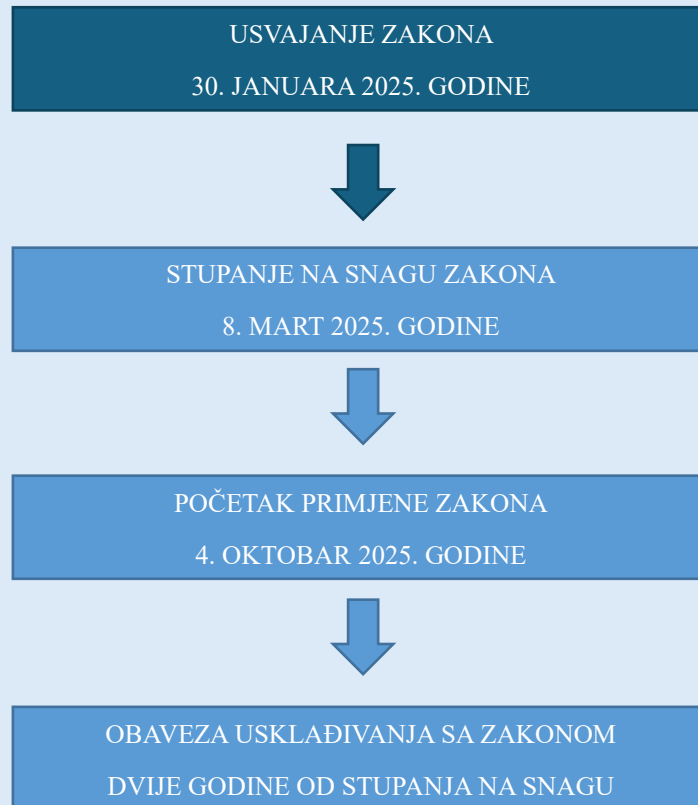
članom 8. Evropske konvencije o zaštiti ljudskih prava, predstavlja i zaštita ličnosti u vezi sa obradom podataka.

Osnovni propis koji je do početka primjene novog Zakona uređivao materiju zaštite ličnih podataka bio je stari Zakon o zaštiti ličnih podataka, usvojen još 2006. godine, sa nekoliko izmjena iz 2006. i 2011. godine. Stari zakon bio je usklađen sa Direktivom EU 95/46/EC, koja je prethodila GDPR-u i koja je, stupanjem na snagu GDPR-a stavljena van snage. Stari zakon je, stoga, imao niz neusklađenosti sa GDPR-om, te se javila potreba za donošenjem novog zakona kojim bi ova materija bila regulisana u skladu sa aktuelnim propisima u EU.⁴

Tako je na 16. hitnoj sjednici Predstavničkog doma, održanoj 23. januara 2025. godine i na 8. hitnoj sjednici Doma naroda, održanoj 30. januara 2025. godine, Parlamentarna skupština BiH usvojila novi Zakon o zaštiti ličnih podataka BiH. Zakon je stupio na snagu 08.03.2025. godine, a datum početka njegove primjene je 04.10.2025. godine. S tim u vezi, a za bolje razumijevanje, na samom početku, važno je napraviti razliku između četiri ključna momenta u pogledu pravne važnosti ovog Zakona. To su: *usvajanje, stupanje na snagu, početak primjene i obaveza usklađivanja sa Zakonom*. Naime, određeni zakon smatra se donesenim kada ga u istovjetnom tekstu usvoje oba doma Parlamentarne skupštine BiH, a zatim se isti objavljuje u Službenom glasniku BiH. Shodno navedenom, kao datum usvajanja ovog Zakona uzima se 30. januar 2025. godine. Time je zakonodavni postupak okončan, zakon je formalno donesen i objavljen, međutim, usvojeni zakon u pravilu ne stupa na snagu odmah po objavljivanju, nego protekom određenog roka nakon objavljivanja u Službenom glasniku (tzv. „*vacatio legis*“). Drugim riječima, isti, momentom donošenja, još uvijek nije pravno obavezujući. U konkretnom slučaju, u završnim odredbama novog Zakona o zaštiti ličnih podataka, određeno je da isti stupa na snagu osmog dana od dana objavljivanja. S obzirom na to da je Zakon objavljen 25.02.2025. godine, isti je stupio na snagu 08.03.2025. godine. Stupanjem na snagu zakona, smatra se da je isti postao pravno obavezujući i da proizvodi pravne učinke. Iako, u pravilu, sa danom stupanja na snagu počinje i primjena određenog zakona, moguće je odgoditi njegovu primjenu, a sve kako bi se pravni subjekti koji su adresati zakona, kao i institucije nadležne za njegovu provedbu mogli pripremiti za ispunjavanje obaveza koje za njih proističu iz tog zakona. Nameće se pitanje zbog čega nije odloženo stupanje na snagu zakona, a ne početak njegove primjene? Naime, zakon mora stupiti na snagu kako bi se donijeli podzakonski propisi i ostali provedbeni akti. U konkretnom slučaju, da je bio odložen početak stupanja na snagu ovog Zakona, ne bi se mogli donositi provedbeni akti niti vršiti usklađivanje. Zbog toga poseže za pravnom konstrukcijom „stupanja na pravnu snagu“, ali sa „odloženom primjenom“. U skladu sa članom 210. novog Zakona o zaštiti ličnih podataka, primjena ovog Zakona odgođena je za 210 dana od dana stupanja na snagu, odnosno, isti se počeo primjenjivati tek od 4.10.2025. godine, kada je ujedno i prestala primjena starog Zakona. Pored ovoga, Zakonom je pravnim subjektima definisana još jedna vremenska odrednica. Naime, odredbom člana 116. stav 2. predviđeno je da su kontrolori i obrađivači podataka koji su već započeli obrade podataka, dužni iste obrade uskladiti u roku od dvije godine od dana stupanja na snagu ovog Zakona. Također, u ovom prelaznom periodu, sve odredbe drugih zakona koje se odnose na obradu ličnih podataka moraju

⁴ Nasir Muftić, Analiza zakonske regulative i institucionalnog okvira za zaštitu podataka u Bosni i Hercegovini, 2024.

biti usklađene sa ovim Zakonom. U nastavku će kroz šemu biti vremenski prikazani ovi momenti.



Zakonom o zaštiti ličnih podataka propisana su pravila zaštite fizičkih lica u vezi sa obradom ličnih podataka i pravila povezana sa slobodnim kretanjem ličnih podataka, kao i nadležnosti Agencije za zaštitu ličnih podataka u BiH, njena organizacija i upravljanje, te druga pitanja značajna za njen rad i zakonito funkcionisanje. Zakonom je također regulisana zaštita fizičkih lica u vezi s obradom ličnih podataka od nadležnih organa u svrhe sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinitelaca krivičnih djela, izvršavanje krivičnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje.⁵

Novi Zakon o zaštiti ličnih podataka BiH donio je značajan napredak u usklađivanju sa modernim evropskim standardima, kroz proširivanje prava nosilaca podataka, preciznije definisanje obaveza onih koji obrađuju podatke i uvođenje strožijih sankcija. Međutim, za organizacije civilnog društva, primjena ovog Zakona predstavlja značajan izazov. Stoga je neophodno ispitati mogućnosti postizanja ciljeva nevladinih organizacija u novom regulatornom okviru, kao i kapacitete Agencije za zaštitu ličnih podataka za sprovođenje novog regulatornog okvira.

⁵ Član 1. Zakona.

2. OSNOVNE KATEGORIJE U POSTUPKU ZAŠTITE LIČNIH PODATAKA

Odredba člana 4. Zakona sadrži definicije kojima se utvrđuju **temeljne kategorije u postupku zaštite ličnih podataka**, a koje su istovjetne onima iz GDPR-a. Stoga će u nastavku, za pojašnjenje određenih pojmova, biti izneseni stavovi dati u mišljenjima ekspertne Radne grupe iz člana 29.⁶

S obzirom na to da se ovaj Zakon primjenjuje na obradu ličnog podatka, najprije se postavlja pitanje šta se to uopšte podrazumijeva pod ličnim podacima i pod obradom, kao osnovnim elementima koji određuju materijalnu primjenjivost Zakona.

Lični podatak, koji je predmet zaštite ovog Zakona, predstavlja svaki podatak koji se odnosi na fizičko lice, kako ono čiji je identitet utvrđen, tako i ono čiji se identitet može utvrditi. Dakle, radi se o svim vrstama izjava o jednoj osobi, a što obuhvata kako objektivne informacije, poput utvrđenih činjenica, tako i one subjektivne prirode, kao što su mišljenja i procjene.

Nadalje, **obrada** u smislu Zakona predstavlja svaki postupak ili skup postupaka koji se obavlja na ličnim podacima ili skupovima ličnih podataka. Da li se radi o obradi podataka, nije od značaja da li se ista obavlja automatiziranim ili neautomatiziranim sredstvima. U zakonu se samo primjera radi navode određeni načini obrade, poput prikupljanja, evidentiranja, organizacije, strukturiranja, čuvanja, prilagođavanja ili izmjene, pronalaženja, ostvarivanja uvida, upotrebe, otkrivanja prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanja ili kombiniranja, ograničenja, brisanja ili uništavanja.

Osnovni subjekti u postupku zaštite ličnih podataka su: nosilac, kontrolor i obrađivač podataka.

Prvo, **nosilac podataka** može biti samo fizičko lice, kako ono čiji je identitet utvrđen, tako i ono čiji se identitet može utvrditi, bilo posredno ili neposredno. U Zakonu se navode posebni identifikatori pomoću kojih se utvrđuje identitet fizičkog lica, kao što su: ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili pomoću jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet tog lica.

Zatim, prema Zakonu, **kontrolor podataka** može biti fizičko i pravno lice, javni ili nadležni organ. Da bi se određeno fizičko ili pravno lice ili javni ili nadležni organ mogli smatrati kontrolorom podataka u smislu ovog Zakona, uslov je da to lice, odnosno, organ određuju svrhu i sredstva obrade ličnih podataka, pri čemu nije bitno da li tu svrhu i sredstvo određuju samostalno ili s drugim licem, odnosno, organom. U slučaju da su svrha i sredstvo obrade utvrđeni zakonom, onda se kontrolor ili posebni kriteriji za njegovo imenovanje propisuju zakonom. Na ovom mjestu, važno je razjasniti pitanje statusa fizičkih lica koje određeno preduzeće ili tijelo javne vlasti imenuju kao ovlašteno lice odgovorno za obradu ili zaštitu podataka. U tom slučaju, kontrolorom podataka neće se smatrati imenovano fizičko lice, nego pravno lice ili tijelo javne vlasti, izuzev ako bi to fizičko lice iskoristilo podatke u sopstvene

⁶ Radna grupa osnovana je na temelju člana 29. Direktive 95/46/EZ. Ona je nezavisno evropsko savjetodavno tijelo za zaštitu podataka i privatnost.

svrhe i izvan tog preduzeća ili javnog organa, kada bi se ono smatralo kontrolorom u smislu ovog Zakona.

Što se tiče treće kategorije, **obrađivača podataka**, Zakonom je određeno da je to fizičko ili pravno lice ili javni organ koji obrađuje podatke, sa naglaskom na to da tu obradu vrši u ime kontrolora. Dakle, obrađivač podataka ne obrađuje podatke u svoje ime i on nije nužni, već samo mogući učesnik u obradi ličnih podataka, jer određeno lice/organ može imati status i kontrolora i obrađivača podataka. Važno je napomenuti da ukoliko obrađivač prekorači svoju ulogu, preuzimajući ulogu odlučivanja o svrsi i sredstvima obrade podataka, on gubi status obrađivača. U tom slučaju, radi se o zajedničkim kontrolorima podataka. S tim u vezi, zajedničkim kontrolorima smatraju se dva ili više kontrolora podataka pod uslovom da zajednički odrede svrhe i načine obrade.

Navedene kategorije objasniti ćemo kroz praktične primjere. Npr. određena nevladina organizacija „X“ organizuje neki seminar, pozivajući zainteresovane da se za učešće prijave putem online obrasca navođenjem podataka poput imena, prezimena, mjesta stanovanja, kontakt podataka i slično. Za tehnički dio organizacije seminara nevladina organizacija „X“ angažuje nevladinu organizaciju „Y“. Građani koji popune obrazac i daju svoje lične podatke kako bi učestvovali na seminaru smatraju se nosiocima ličnih podataka. Nevladina organizacija „X“ koja organizuje taj seminar ima status kontrolora podataka, budući da prikuplja podatke, određuje svrhu obrade (organizacija seminara), te odlučuje o sredstvima obrade (online obrazac) i o roku čuvanja podataka. **Obrađivač** je, u ovom slučaju, nevladina organizacija „Y“, jer ista neposredno samo tehnički obrađuje podatke, ali ne samostalno, već po uputi NVO „X“ kao kontrolora podataka i u skladu sa svrhom obrade koju NVO „X“ odredi. Zatim, NVO kao poslodavac također može imati status kontrolora podataka. U tom slučaju, radnici zaposleni u toj NVO imaju status nosioca podataka, a određena knjigovodstvena agencija koju ta NVO angažuje radi vođenja knjigovodstvenog poslovanja status obrađivača.

U lancu obrade ličnih podataka, pored nabrojana tri, pojavljuje se još jedno lice. To je tzv. **primalac**, odnosno fizičko ili pravno lice ili javni organ kojem se otkrivaju lični podaci. Pri tome, nije od značaja da li je u pitanju treća strana, odnosno, ona koja nije niti nosilac, niti kontrolor, niti obrađivač podataka niti lice ovlašteno za obradu ličnih podataka pod neposrednom nadležnošću kontrolora ili obrađivača podataka. Primaocima se ne smatraju javni organi koji mogu primiti lične podatke u okviru određene istrage u skladu sa zakonom, ali to ni u kojem slučaju ne znači da obrada tih podataka ne mora biti u skladu sa važećim pravilima o zaštiti podataka prema svrhama obrade.

Odredba člana 11. Zakona sadrži relativnu zabranu obrade određenih, tzv. **posebnih kategorija ličnih podataka**. U tu grupu ličnih podataka spadaju podaci koji otkrivaju rasno ili etničko porijeklo, politička mišljenja, vjerska ili filozofska uvjerenja ili pripadnost sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije lica, podataka o zdravlju ili podataka o spolnom životu ili seksualnoj orijentaciji lica.

3. OSNOVNI PRINCIPI ZAŠTITE LIČNIH PODATAKA

Cjelokupan sistem zaštite ličnih podataka u BiH zasnovan je na poštovanju sljedećih fundamentalnih principa, iz kojih se izvode konkretna prava i dužnosti subjekata u ovom procesu.⁷

Princip **zakovitosti** koji se manifestuje kroz poštovanje jasno definisanih procedura, prava i dužnosti u procesu obrade. Suština **principa transparentnosti** je u tome da nosioci podataka imaju uvid i budu upoznati sa svim odgovornostima koje kontrolor i obrađivač podataka imaju u vezi sa obradom njihovih ličnih podataka. Svrha ovog principa jeste da pojedincu omogući efektivno vršenje kontrole nad svojim podacima. Naime, jedan od bitnih zahtjeva principa transparentnosti je da pojedinac može unaprijed utvrditi obim i posljedice obrade, odnosno, da bude upoznat sa načinima korištenja njegovih podataka. Ovaj zahtjev predstavlja važan aspekt **principa pravičnosti**.⁸

Princip ograničenja svrhe znači da se lični podaci smiju prikupljati isključivo u tačno određenu, jasno definisanu i zakonitu svrhu. Ova svrha mora biti poznata već u trenutku prikupljanja podataka, a nosilac podataka mora biti informisan o istoj. Ovaj princip također podrazumijeva da se prikupljeni podaci kasnije ne mogu koristiti u svrhe koje nisu u skladu sa konkretnom, prvobitno određenom svrhom. Tako svaka dalja (nova) obrada mora biti usklađena sa prvobitnom. Dakle, suština ovog principa je da je sama obrada podataka vezana za svrhu obrade, odnosno, da ista mora biti vezana za unaprijed utvrđeni cilj, štiteći na taj način nosioce podataka od proizvoljnog, naknadnog proširivanja svrhe. Međutim, izuzetak od ovog pravila predstavljaju slučajevi kada se podaci dalje obrađuju u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe, jer se takva obrada ne smatra neusklađenom s prvobitnim svrhama.

Princip smanjenja obima podataka znači da podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u odnosu na svrhe za koje se obrađuju. Kod ovog principa, postavlja se pitanje da li je obrada podataka pogodna za postizanje nekog legitimnog cilja (svrhe) i da li bi se ta svrha mogla postići drugim sredstvima, odnosno, obradom manje količine podataka.

Prema **principu tačnosti**, podaci moraju biti tačni i prema potrebi ažurirani. Ovaj princip podrazumijeva i to da se moraju preduzeti sve razumne mjere kako bi se osiguralo da lični podaci, koji nisu tačni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljeni.

Sljedeći princip je **princip ograničenja čuvanja podataka**. Prema ovom principu, podaci moraju biti čuvani u formi koja omogućava identifikaciju nosioca podataka, i to ne duže nego što je potrebno u svrhe u koje se lični podaci obrađuju. Dakle, ako podaci više nisu potrebni, isti treba da budu obrisani, a ukoliko postoje zakonski rokovi za čuvanje podataka, iste treba

⁷ Član 7. Zakona

⁸ Diligenski, Andrej, Dragan Prlja, Dražen Cerović. *Pravo zaštite podataka-GDPR*. Institut za uporedno pravo, 2018.

čuvati u zakonom predviđenom roku. U Zakonu je predviđen jedan izuzetak od navedenog pravila. Naime, lični podaci se mogu čuvati na duži period ako će se obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe. Međutim, navedeno je uslovljeno i provođenjem primjerenih tehničkih i organizacionih mjera, radi zaštite prava i sloboda nosioca podataka.

Pod **principom cjelovitosti i povjerljivosti** pretpostavlja se da podaci moraju biti obrađivani tako da se osigurava odgovarajuća sigurnost ličnih podataka. To uključuje i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacionih mjera.

Princip pouzdanosti znači da je kontrolor podataka odgovoran za usklađenost obrade ličnog podatka sa svim naprijed navedenim principima. U tom smislu, teret dokazivanja usklađenosti je na njemu.

4. TEMELJNI USLOVI ZAKONITE OBRADJE LIČNIH PODATAKA

Nadalje, odredbom člana 8. stav 1. propisani su **temeljni uslovi** koje je potrebno ispuniti da bi obrada ličnih podataka bila zakonita. Na prvom mjestu, važno je naglasiti da Zakon ne zahtijeva kumulativno ispunjenje ovih uslova za zakonitost obrade. Dakle, da bi obrada podataka bila zakonita, dovoljno je da bude ispunjen najmanje jedan od temeljnih uslova nabrojanih u navedenoj odredbi. Radi se o sljedećim uslovima.

- Prvi temeljni uslov odnosi se na to da je nosilac podataka dao saglasnost za obradu svojih ličnih podataka u jednu ili više posebnih svrha. Ali šta uopšte znači dati saglasnost? Prije svega, pod saglasnošću se podrazumijeva izražavanje volje nosioca podataka, odnosno, davanje pristanka za obradu ličnih podataka koji se odnose na njega izjavom ili jasnom potvrdnom radnjom. To izražavanje volje mora biti dobrovoljno, posebno, informisano i nedvosmisleno. Nadalje, u vezi sa saglasnošću, važno je istaknuti da je teret dokazivanja postojanja saglasnosti nosioca podataka za obradu njegovih ličnih podataka na kontroloru podataka, onda kada je obrada zasnovana na saglasnosti. Na ovom mjestu, napominjemo da nosilac podataka ima pravo u bilo kojem trenutku povući svoju saglasnost. Međutim, postavlja se pitanje da li je u tom slučaju obrada podataka na osnovu saglasnosti, a prije njenog povlačenja zakonita ili ne. Odgovor je da povlačenje saglasnosti ne utiče na zakonitost obrade podataka na osnovu saglasnosti prije njenog povlačenja. Povlačenje saglasnosti mora biti jednako jednostavno kao i njeno davanje.
- Drugi uslov se vezuje za ugovorne odnose. Naime, da bi obrada bila zakonita, ista mora biti neophodna radi izvršenja ugovora u kojem je nosilac podataka ugovorna strana ili radi preduzimanja radnji na zahtjev nosioca podataka prije zaključenja ugovora.
- Zatim, jedan od temeljnih uslova za zakonitost obrade jeste i da je obrada neophodna radi poštovanja pravnih obaveza kontrolora podataka.
- Kao četvrti uslov u Zakonu se navodi neophodnost obrade radi zaštite ključnih interesa nosioca podataka ili drugog fizičkog lica.
- Obrada je zakonita i ako je neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja kontrolora podataka.

- Posljednji alternativno postavljeni uslov jeste da je obrada neophodna zbog legitimnih interesa⁹ kontrolora podataka ili treće strane. Međutim, u tom smislu, nije dovoljno da postoje legitimni interesi kontrolora ili treće strane koji opravdavaju obradu kako bi ista bila zakonita, već je neophodan element i da ti interesi pretežu nad interesima ili osnovnim pravima i slobodama nosioca podataka, a koji zahtijevaju zaštitu ličnih podataka. Jedino u tom slučaju, obrada se može smatrati zakonitom. Navedeno je posebno naglašeno u situacijama u kojima je nosilac podataka dijete. Dakle, kada postoje suprotstavljeni legitimni interesi, vrši se vaganje interesa, pri čemu se procjenjuje da li legitimni interesi kontrolora podataka ili treće strane pretežu nad interesima, osnovnim pravima i slobodama nosioca podataka (npr. s jedne strane sloboda izražavanja, a sa druge zaštita ličnih podataka). Ova procjena mora biti konkretna i zasnovana na okolnostima svakog konkretnog slučaja, uzimajući u obzir prirodu ličnih podataka, svrhu obrade, itd.

Osim kod saglasnosti, kao prvog mogućeg osnova zakonite obrade podataka, svi ostali osnovi zahtijevaju prethodnu procjenu primjenjivosti. Naime, kriterij **neophodnosti** podrazumijeva provođenje testa u kojem se ispituje da li se ista svrha ili cilj može postići drugim mjerama, odnosno, mjerama koje bi manje zadirale u prava pojedinaca.¹⁰

5. PRAVA NOSILACA PODATAKA PREMA NOVOJ REGULATIVNI ZAŠTITE LIČNIH PODATAKA¹¹

Cjelokupna regulativa zaštite ličnih podataka, u duhu GDPR Uredbe, postavljena je na način da nosilac podatka zauzima centralnu poziciju unutar zaštitnih mehanizama, normirajući čitav niz prava koja mu pripadaju, a koja se ostvaruju u skladu sa prethodno navedenim principima obrade, i to:

5.1. Pravo na adekvatan uvid u sistem zaštite ličnih podataka, kao i načine ostvarivanja predviđenih prava nosioca podatka (*pravo izvedeno iz principa transparentnosti*)

Cilj ovog prava jeste upoznavanje nosioca podatka sa cjelokupnim sistemom zaštite ličnih podataka osiguranim ovim Zakonom, te interno od strane konkretnog kontrolora podataka, a što mora biti učinjeno u sažetoj, transparentnoj, razumljivoj i lako dostupnoj formi, uz upotrebu

⁹ „Pojam „interesi“ stoji neposredno u vezi sa svrhom obrade podataka. Dok sa jedne strane svrha obrade podataka predstavlja razlog, namjeru obrade, interesi sa druge strane se odnose na korist koju kontrolor može izvući iz obrade podataka.“ (Diligenski, Andrej, Dragan Prlja, Dražen Cerović. *Pravo zaštite podataka-GDPR*. Institut za uporedno pravo, 2018.)

¹⁰ Diligenski, Andrej, Dragan Prlja, Dražen Cerović. *Pravo zaštite podataka-GDPR*. Institut za uporedno pravo, 2018.

¹¹ Vidjeti: Članovi 14 – 24. Zakona

jasnog i razumljivog jezika (*detaljnije objašnjenje ovog prava biće učinjeno u dijelu obaveza kontrolora podataka koje su u direktnoj korelaciji sa ovim pravom*).

5.2. Pravo na pristup ličnom podatku

Nosilac podataka ima pravo da od kontrolora podataka dobije potvrdu o tome da li on vrši obradu njegovog podatka, te u slučaju pozitivnog odgovora, ostvaruje pravo na pristup podatku, a što uključuje: informacije o svrsi obrade, kategoriji ličnog podatka, subjektima kojima je podatak učinjen dostupnim, naročito ako je podatak otkriven primaocu u drugoj državi ili međunarodnoj organizaciji, a ukoliko se podatak ne prikuplja od nosioca podatka, sve dostupne informacije o njegovom izvoru. U svakom slučaju, nosiocu podatka pripada pravo da zahtijeva ispravku ili brisanje podatka ili ograničenje obrade, te pravo na podnošenje prigovora Agenciji, odnosno tužbe nadležnom sudu.

5.3. Pravo na ispravku

Navedeno pravo se ostvaruje kada kontrolor podatka vrši obradu netačnog ili nepotpunog ličnog podatka, te nosilac podatka ima pravo da mu kontrolor omogući ispravku, odnosno dopunu, bez nepotrebnog odgađanja.

5.4. Pravo na brisanje

Pravo na brisanje ili riječnikom ESLJP „*pravo na zaborav*“, predstavlja izuzetno delikatno subjektivno pravo nosioca podatka, a njegov smisao se ogleda u uskraćivanju daljeg raspolaganja ličnim podatkom nosiocu podatka, ukoliko je za to prestao egzistirati valjani pravni ili stvarni osnov. Međutim, sama priroda ovog prava je takva da se ono primarno aktivira u odnosu na lične podatke dostupne širem spektru javnosti, te korištenje ovog prava predstavlja formu „pretvaranja“ javnih informacija u privatne, kroz zabranu trećim osobama da istima pristupe.¹²

Da bi se nosilac podatka koristio ovim pravom, dovoljno je da je ispunjen **jedan od sljedećih uslova**:

- konkretni podatak više nije neophodan za svrhe u koje je prikupljen ili na drugi način obrađen, što je odraz načela svrshodnosti obrade podataka;
- nosilac podatka je povukao saglasnost za obradu podatka, te ne egzistira drugi pravni osnov iz Zakona temeljem kojeg bi se vršila obrada;
- ulaganje prigovora na obradu podatka;
- ukoliko je lični podatak nezakonito obrađen;
- kada je to potrebno radi postupanja u skladu sa zakonskom obavezom kojoj podliježe kontrolor podataka;

¹² Maja Čolaković, Lana Bubalo, Pravo na zaborav kao instrument prava ličnosti u Evropskoj Uniji, *Zbornik radova Pravnog fakulteta u Tuzli*, str. 20.

- lični podatak je prikupljen u vezi sa ponudom usluga informacionog društva.

Kompleksnost prava na zaborav posebno je izražena na planu njegove praktične implementacije i postizanja potpunog efekta zaštite. Zakonodavac je obavezao kontrolora koji je javno objavio podatak koji ispunjava uslove za brisanje, da preduzme sve razumne mjere, uključujući i tehničke, a kako bi obavijestio druge kontrolore podataka koji obrađuju konkretni lični podatak da je nosilac podatka zatražio od njih da brišu sve poveznice do podatka ili kopiju ili rekonstrukciju. Dakle, u pitanju je širok informaciono – tehnološki poduhvat, koji prethodno pretpostavlja identifikaciju svih kontrolora podataka koji tim podatkom raspolazu.

Istovremeno, zakon je isključio primjenu ovog prava u različitim situacijama, a u pogledu položaja organizacija civilnog društva, dva pravna osnova zaslužuju naročitu pažnju:

- isključenje primjene radi ostvarivanja prava na slobodu izražavanja i informisanja;
- isključenje primjene radi poštovanja zakonske obaveze kontrolora podataka ili radi izvršenja zadatka koji se obavlja u **javnom interesu** ili u okviru izvršenja službenih ovlaštenja dodijeljenih kontroloru podataka;

5.5. Pravo na ograničenje obrade

Kao titular ovog prava, nosilac može zahtijevati ograničenje obrade ličnog podatka, ako je ispunjen samo jedan od uslova: i. osporavanje tačnosti ličnog podatka; ii. obrada podatka je nezakonita; iii. kontroloru podatka ovaj podatak više nije potreban; iv. nosilac podatka je uložio prigovor na obradu i očekuje odluku da li njegovi razlozi prevladavaju nad legitimnim interesima kontrolora podataka.

Ako je usvojeno ograničenje obrade, dalja obrada se može vršiti samo uz saglasnost nosioca podatka, uz nekoliko izuzetaka, a jedan od njih je upravo „*važan javni interes*“.

5.6. Pravo na prenosivost ličnog podatka

Definiše uslove pod kojima nosilac podatka može preuzeti lični podatak koji se odnosi na njega, a koji je dao kontroloru, te ga prenijeti drugom kontroloru podataka, bez ometanja prvobitnog kontrolora.

5.7. Pravo na prigovor

S obzirom na specifične okolnosti svake pojedine situacije, nosilac podatka ima pravo da *u svakom trenutku*, podnese prigovor na obradu podataka, ali samo kada se obrada zasniva na jednom od sljedeća dva pravna osnova:

- ako je obrada podatka neophodna radi izvršenja zadataka koji se obavljaju u javnom interesu ili u okviru izvršavanja službenih ovlaštenja kontrolora podataka;

- ako je obrada neophodna zbog legitimnih interesa kontrolora podataka ili treće strane, a ti legitimni interesi uzimaju prevagu u odnosu na prava i slobode nosioca podataka.

Dakle, pravo na prigovor je isključeno onda kada je nosilac podatka dao saglasnost na obradu.

Kada nosilac podatka podnese predmetni prigovor, kontrolor podataka je dužan suzdržati se od svake dalje obrade podatka, osim u slučaju kada dokaže da postoje uvjerljivi legitimni interesi za obradu koji prevladavaju nad interesima, pravima i slobodama nosioca podataka ili kada je obrada neophodna radi postavljanja, ostvarivanja ili odbrane određenih pravnih zahtjeva kontrolora.

Kontrolor je dužan upoznati nosioca podatka najkasnije u **trenutku njihove prve komunikacije sa predviđenim pravima, što mora biti učinjeno jasno i odvojeno od bilo koje druge informacije.**

6. OGRANIČENJA PRAVA ZAŠTITE LIČNIH PODATAKA

Suština prava zaštite ličnih podataka jeste ta da ovo pravo ima tzv. **relativni karakter**, odnosno dozvoljava ograničenje njegovog obima pod uslovom nastupanja određenih okolnosti. U tim slučajevima, predmetna ograničenja neće dovesti do povrede ovog ljudskog prava. Važno je napomenuti da se radi o ograničenju **obima** prava, a ne ograničenju samog prava.¹³ Dakle, prava kao takva i dalje egzistiraju, ali ne u punom obimu. Tako je zakonodavac propisao sljedeće uslove, u formi svojevrsnog testa, koji moraju biti kumulativno ispunjeni, kako bi se ograničenje obima navedenih prava smatralo zakonitim:

1. ograničenja obima prava moraju biti propisana odredbama **posebnog zakona**, jednog od nivoa vlasti u Bosni i Hercegovini;
2. ako ograničenja poštuju suštinu osnovnih prava i sloboda;
3. ako ograničenja predstavljaju **neophodnu i proporcionalnu mjeru u demokratskom društvu**, za postizanje nekog od sljedećih legitimnih interesa: državna sigurnost, odbrana, sprečavanje, istraga, otkrivanje i gonjenje učinilaca krivičnih djela, drugih važnih ciljeva od opšteg javnog interesa u Bosni i Hercegovini, a posebno važnog privrednog ili finansijskog interesa, što uključuje monetarna, budžetska i poreska pitanja, javno zdravstvo i socijalnu zaštitu; nezavisnosti pravosuđa i sudskih postupaka; sprečavanja, istrage, otkrivanja i gonjenja povrede etike u zakonski regulisanim profesijama, nadzorne, inspeksijske ili regulatorne funkcije; zaštita nosioca podataka ili prava i sloboda drugih osoba; ostvarivanja potraživanja u građanskim sporovima.

Navedeno propisivanje ograničenja slijedi metodologiju koju je Evropski sud za ljudska prava razvio prilikom ispitivanja navoda o potencijalnim povredama ljudskih prava i sloboda. U tom smislu, pretpostavka ograničenja prethodno definisanih prava, jeste postojanje zakona kojim su ta ograničenja definisana. Posebno je predviđeno da predmetni zakon po potrebi, treba da obuhvati sljedeća pitanja: svrhu ili kategoriju obrade, kategoriju ličnog podatka, **obim uvedenih ograničenja**, mjere zaštite za sprečavanje zloupotrebe ili nezakonitog pristupa ili prenošenja, određivanje kontrolora podataka, rok čuvanja, rizik za prava i slobode nosioca podataka, te pravo nosioca podataka da bude obaviješten o ograničenju, osim ako to može biti štetno za svrhu tog ograničenja. Prema ovim rješenjima, u pitanju su posebni zakoni, koji regulišu najrazličitije oblasti, a koje kao takve podrazumijevaju obradu određenih ličnih podataka – npr. Zakon o udruženjima i fondacijama BiH, Zakon o slobodi pristupa informacijama, Zakon o radu. Shodno prethodnom navedenom, odredbe ovih zakona, u roku od 2 godine, moraju biti usklađene sa odredbama Zakona o zaštiti ličnih podataka, i u dijelu predviđanja osnova za ograničenja zaštite ličnih podataka.

Međutim, sama činjenica postojanja zakona nije dovoljna da se ograničenje u uživanju prava na zaštitu ličnog podatka smatra zakonitim, te je neophodno da sam zakon slijedi jedan od

¹³ Član 25 Zakona

prethodno navedenih legitimnih interesa. Legitimni interes se posmatra kao određeno dobro, odnosno viši cilj, a sama ograničenja se ustanovljavaju kako bi se predmetni viši cilj postigao.

U konačnici, najkompleksniji segment ovog ispitivanja jeste utvrđivanje da li ograničenje koje je definisano zakonom, koje teži postizanju određenog legitimnog cilja, predstavlja neophodnu mjeru u demokratskom društvu. Neophodnost se ispituje sa dva aspekta – **adekvatnost**, odnosno da li se putem utvrđenog ograničenja može postići legitimni cilj i – **proporcionalnost**, da li se navedeni legitimni cilj mogao postići primjenom nekih drugih, blažih ograničenja, odnosno da li primijenjeno sredstvo ograničenja predstavlja jedinu i krajnju mjeru za ostvarivanje postavljenog cilja.¹⁴

Identifikovani rizik:

- **(ne)ažurnost zakonodavnih organa na svim nivoima sa izvršavanjem obaveze usklađivanja odredbi posebnih zakona, kojim će se omogućiti ograničenja prava na zaštitu ličnih podataka, na način koji je prethodno opisan;**
- **način na koji će zakonodavac regulisati konkretna pitanja, a posebno definisanje obima ograničenja i kategorija ličnih podataka;**
- **zakonitost ograničenje se na kraju svodi na faktičko pitanje, posebno u odnosu na kriterij proporcionalnosti, na koje krajnji odgovor mogu ponuditi isključivo sudovi, prilikom rješavanja konkretnih pravnih sporova povodom primjene ovog Zakona.**

7. OBAVEZE KONTROLORA PODATAKA I OBRAĐIVAČA U POSTUPKU ZAŠTITE LIČNIH PODATAKA

Zakonom su definisane izuzetno stroge obaveze za kontrolore i obrađivače podataka, a koje dominantno slijede strukturu definisanih prava, te se za potrebe ove analize mogu podijeliti u nekoliko kategorija:¹⁵

7.1. Obaveze operativno – tehničkog i sigurnosnog karaktera

Obaveza primjene odgovarajućih tehničkih i organizacionih mjera, kako bi se osigurala obrada podataka u skladu sa ovim normativnim okvirom, a koje mjere se prema potrebi preispituju i ažuriraju. Dodatno, kontrolori podataka su u obavezi prilikom procesa obrade primjenjivati

¹⁴ Nedim Ademović, Joseph Marko, Goran Marković, *Ustavno pravo Bosne i Hercegovine* (Sarajevo: Konrad Adenauer Stiftung, 2012): 237 – 241.

¹⁵ Članovi 26 – 45. Zakona

zaštitne mjere, poput pseudonimizacije i smanjenja količine podataka koji se obrađuju. Uz to, ova obaveza podrazumijeva i mjere kojima se osigurava da na integrisani način budu obrađeni samo oni podaci koji su neophodni za postizanje svake posebne svrhe zbog koje su prikupljeni, što je naročito izraženo u kontekstu obima njihove obrade, roka čuvanja i dostupnosti.

7.2. Procesne obaveze

- Upoznavanje sa pravima koja nosiocu podataka pripadaju i dostavljanje informacija o različitim aspektima obrade

Imajući u vidu da sistem zaštite ličnih podataka počiva na **principu transparentnosti**, dužnost kontrolora podataka jeste da upozna nosioca podatka sa cjelokupnim sistemom zaštite ličnih podataka osiguranim ovim Zakonom, te interno od strane konkretnog kontrolora podataka. Dakle, u pitanju su svojevrsne pouke o njegovim pravima, a što mora biti učinjeno u sažetoj, transparentnoj, razumljivoj i lako dostupnoj formi, uz upotrebu jasnog i razumljivog jezika. Ove informacije mogu biti učinjene dostupnim u pisanom i elektronskom formatu, ukoliko je ista primjenjiva, a praktična implementacija ovog prava najčešće se ostvaruje putem internih akata nosioca podataka – Pravilnika o zaštiti ličnih podataka i Politike privatnosti.¹⁶ Iako ovi akti nisu izričito predviđeni odredbama Zakona, potreba za njihovim usvajanjem proizlazi upravo iz principa *transparentnosti obrade podataka*.

Pored pouke o pravima koja mu pripadaju, kontrolor podataka je dužan dostaviti nosiocu podataka čitav *set informacija o obradi*. U odnosu na **sadržaj informacija**, zakonodavac ne pravi razliku između toga da li se podatak prikupio neposredno od nosioca ili ne, te one obuhvataju: i. identitet i kontaktne podatke kontrolora podataka; ii. kontaktne podatke službenika za zaštitu podataka; iii. pravni osnov i svrhu obrade ličnog podataka; iv. ukoliko se obrada provodi radi postizanja nekog legitimnog interesa kontrolora ili trećeg lica (obrada bez saglasnosti nosioca), dužan je uputiti ga na konkretni legitimni interes; v. informacije o primaocu ili kategoriji primaoca; vi. namjeru prenosa ličnog podatka u drugu državu ili međunarodnu organizaciju. Ukoliko je to neophodno iz razloga pravičnosti i transparentnosti, kontrolor je dužan dostaviti i druge podatke utvrđene ovim zakonom.

Dvije važne napomene:

- a. Ako kontrolor namjerava dodatno obrađivati lične podatke izvan prvobitno definisane svrhe zbog koje su podaci prikupljeni, on mora prije dodatne obrade informisati nosioca o toj drugoj svrsi;
- b. Ukoliko nosilac podatka već raspolaže svim ovim informacijama koje su prethodno navedene, kontrolor nije dužan pružati te informacije.

Ključne razlike u slučajevima **kada podaci nisu prikupljeni od nosioca**:

¹⁶ Osnovni elementi ovih akata prikazani su u okviru Priručnika.

- a. Predmetne informacije dostavljaju se nosiocu u razumnom roku nakon dobijanja ličnih podataka, a najkasnije u roku od 30 dana; ako se lični podatak koristi za komunikaciju sa nosiocem, najkasnije prilikom prve komunikacije; ako je predviđeno otkrivanje podataka drugom primaocu, najkasnije u trenutku kada je lični podatak prvi put otkriven.
- b. Predviđene su dodatne okolnosti usljed kojih kontrolor neće biti u obavezi dostavljati prethodno navedene informacije nosiocu, i to: i. pružanje takvih informacija je nemoguće ili bi zahtijevalo neproporcionalne napore; ii. dobivanje ili otkrivanje podataka je izričito propisano posebnim zakonom koji se primjenjuje na nosioca podataka; iii. lični podatak mora ostati povjerljiv u skladu s obavezom čuvanja profesionalne tajne, ali i druge zakonske obaveze čuvanja tajne.

- Saradnja sa agencijom i izvještavanje Agencije o povredi

U slučaju povrede ličnog podatka, kontrolor podatka je dužan bez nepotrebnog odgađanja i ako je to moguće, a najkasnije u roku od 72 sata nakon saznanja za tu povredu, obavijestiti o povredi ličnog podatka. Isključenje ove obaveze postoji samo ako je vjerovatno da ta povreda neće ugroziti prava i slobode fizičkog lica. Međutim, navedeno predstavlja faktičko pitanje, uslovljeno specifičnim okolnostima svakog konkretnog slučaja, što neminovno iziskuje potrebu za usvajanjem određenih smjernica od strane regulatora, kojima bi se utvrdili precizniji kriteriji na ovom planu, a kako bi se zadovoljili zahtjevi pravne sigurnosti.

S druge strane, ukoliko je povredu ličnog podatka izvršio obrađivač, on je o tome dužan obavijestiti kontrolora podataka, bez nepotrebnog odgađanja.

Definisan je i obavezan sadržaj ovog izvještaja, a koji čine: opis prirode učinjene povrede ličnog podataka, sa što je moguće preciznijim informacijama o istom; podaci o službeniku za zaštitu podataka ili od druge osobe od koje se mogu dobiti potrebne informacije; opis moguće posljedice povrede ljudskog prava; opis mjera koje je kontrolor preduzeo ili predložio radi rješavanja problema nastalih povredom ličnog podataka.

- Obavještavanje nosioca podataka o povredi

Povreda ličnog podataka stvara obavezu kontroloru podataka da o istoj obavijesti i konkretnog nosioca podataka. Iako je kod ove obaveze primijenjena drugačija nomotehnička konstrukcija u odnosu na obavezu obavještavanja Agencije, suština obje obaveze je potpuno istovjetna – ona egzistira samo ako je vjerovatno da će povreda uzrokovati visok rizik za prava i slobode fizičkog lica, što opet otvara prethodno istaknutu dilemu tumačenja standarda „visoki rizik“. Konkretno obavještenje mora biti učinjeno na što jasniji i jednostavniji način.

Za razliku od obaveze obavještavanja Agencije o povredi, koja je prisutna u svim situacijama, izuzev kada nije ispunjen standard „visokog rizika“, zakonodavac je u odnosu na obavještavanja nosioca podataka predvidio pojedine okolnosti usljed kojih kontrolor podataka neće biti obavezan izvršiti dato obavještavanje, i to:

1. preduzimanje odgovarajućih tehničkih i organizacionih mjera zaštite u odnosu na konkretni lični podatak, a koje primarno taj podatak čine nerazumljivim licu koje nije ovlašteno da mu pristupi, kao npr. enkripcija;
2. preduzimanje naknadnih mjera (nakon što je povreda izvršena), kojima se onemogućava pojava visokog rizika za prava i slobode nosioca podataka;
3. ukoliko obavještanje zahtijeva nesrazmjeran napor za kontrolora podataka, ova obaveza može se supstituirati obavezom javnog saopštavanja ili preduzimanja drugih sličnih mjera koje imaju učinak upoznavanja nosioca podatka o izvršenoj povredi.

- Procjena uticaja obrade na zaštitu ličnog podatka

Kako se moglo vidjeti i u prethodnim segmentima, zakonodavac prilikom normiranja prava i obaveza iz oblasti zaštite ličnih podataka izuzetno često koristi standard „vjerovatnoće“. Tako, ukoliko je vjerovatno da će neka obrada, posebno posredstvom novih tehnologija, a s obzirom na prirodu, obim, kontekst i svrhu obrade, uzrokovati visok rizik za prava i slobode fizičkih lica, kontrolor podataka je dužan, **prije obrade**, provesti procjenu uticaja predviđenih obrada na zaštitu ličnog podatka.

Dakle, u pitanju je prethodna obaveza kontrolora podatka, odnosno obaveza koja nastupa prije nego što je proces obrade podataka započeo, a opravdava se postojanjem visokog rizika po prava i slobode fizičkih lica usljed procesa obrade ličnih podataka. Njen smisao se ogleda u pravovremenoj prevenciji povrede ličnih podataka, zbog postojanja ovog visokog rizika.

Prije provođenja same procjene kontrolor podatka se savjetuje o istoj sa službenikom za zaštitu ličnih podataka, ako je imenovan.

U cilju preciziranja situacija kada se aktivira ova obaveza, zakonodavac je obavezao Agenciju da utvrdi i javno objavi listu vrste postupaka obrade podataka tokom kojih će se provoditi procjena uticaja obrade na zaštitu ličnog podatka. Dakle, prvobitni uslov koji mora biti ispunjen da bi se provodila procjena uticaja, jeste utvrđivanje oblasti, odnosno vrsta postupaka od strane regulatora, unutar kojih će se implementirati ova obaveza. Takođe, na nivou fakultativne mogućnosti, ostavljeno je da Agencija utvrdi i javno objavi listu vrsta postupaka obrade za koje nije potrebna procjena uticaja na zaštitu ličnog podatka.

Zakonom je definisan minimalan sadržaj procjena uticaja, koji obuhvata: i. sistemski opis predviđenih obrada i svrha obrada, uključujući i postojanje legitimnog interesa kontrolora podataka; ii. procjenu nužnosti i proporcionalnosti obrada povezanih s njihovim svrhama; iii. procjenu rizika za prava i slobode nosilaca podataka; iv. mjere za rješavanje rizika, koje uključuju zaštitne mjere, sigurnosne mjere i mehanizme za osiguranje zaštite ličnih podataka i dokazivanje usklađenosti sa Zakonom. Pojednostavljeno, kontrolor podataka u okviru ove procjene, obrazlaže neophodnost procesa obrade, uz dokazivanje da se postavljena svrha ne može postići primjenom drugih, blažih metoda obrade, te nudi jasne zaštitne garancije koje bi trebale spriječiti povredu ličnih podataka.

- Prethodno savjetovanje sa Agencijom

Ukoliko je prethodno opisana procjena uticaja potvrdila vjerovatnoću, odnosno pokazala da bi obrada podataka uzrokovala visok rizik za prava i slobode pojedinaca, a kontrolor nije donio mjere za ublažavanje rizika, **prije otpočinjanja obrade** dužan je savjetovati se sa Agencijom, koji se pokreće upućivanjem zahtjeva. Ako utvrdi da bi planiranom obradom podataka došlo do kršenja zakonskih odredbi, a posebno ako kontrolor podataka nije u dovoljnoj mjeri utvrdio ili umanjio rizik za prava i slobode pojedinca, Agencija će u roku od najduže 56 dana od zaprimanja zahtjeva, provesti pisani postupak savjetovanja kontrolora podataka, a po potrebi i obrađivača (navedeni rok se može produžiti za dodatna 42 dana, u zavisnosti od složenosti planirane obrade podataka).

Ono što je izuzetno važno za pojedine oblasti, jeste da se nezavisno od ove obaveze savjetovanja, posebnim zakonom (koji može biti i zakon koji je relevantan za status i djelovanje organizacija civilnog društva) može propisati obaveza kontrolora podataka da se savjetuje sa Agencijom i da pribavi prethodno odobrenje za obradu podataka, koju obavlja za izvršenje zadataka u javnom interesu.

IDENTIFIKOVANI RIZIK: Navedenim zakonodavnim ovlaštenje, otvara se prostor da se odredbama posebnih zakona konkretni sistem učini strožim za kontrolore i obrađivače podataka koji obradu provode u javnom interesu, kroz obavezno pribavljanje odobrenja od same Agencije. S obzirom da organizacije civilnog društva vrlo često preduzimaju aktivnosti koje su usmjerene ka postizanju ili zaštiti određenog javnog interesa, postoji opasnost da takvo djelovanje može biti ograničeno ili onemogućeno uskraćivanjem predmetnog odobrenja.

- Certifikacija ličnih podataka

U pitanju je aktivnost *dobrovoljnog karaktera*, čije provođenje ne umanjuju odgovornost kontrolora podataka i obrađivača u vezi sa poštovanjem i primjenom Zakona, te ne ograničava nadležnosti Agencije. Agencija će preporučiti uspostavljanje postupka certifikacije zaštite ličnih podataka, pečata i oznaka za zaštitu ličnih podataka, a kako bi se osiguralo poštovanje zakonskih obaveza, a posebno postojanje odgovarajućih zaštitnih mjera. Certifikat se kontroloru podataka ili obrađivaču izdaje najduže na tri godine, uz mogućnost obnove, a može biti i oduzet, u slučaju neispunjavanja uslova za izdavanje certifikata.

7.3. Obaveze usvajanja određenih dokumenata i akata

Zakon za kontrolore podataka i obrađivače direktno i indirektno propisuje obaveze normativnog karaktera, koje se sastoje iz usvajanja internih pravnih akata, kojima se upotpunjuje pravna zaštita predviđena zakonskim odredbama. Tako Zakon izričito predviđa usvajanje sljedećih internih akata, dok obaveza usvajanja preostalih (prezentovani u okviru Priručnika), proizlazi iz temeljnih principa ovog Zakona i GDPR-a:

- **Evidencija aktivnosti obrade ličnih podataka** – ova evidencija predstavlja pregled aktivnosti obrade podataka, te je vode zasebno kontrolor podataka i njegov predstavnik na jednoj strani, te obrađivač i njegov predstavnik na drugoj strani, ukoliko se obrada obavlja u ime kontrolora;
- **Kodeks ponašanja** – u pitanju je dokument koji odražava specifičnosti različitih sektora obrade podataka i posebnih potreba privrednih subjekata, a usvaja se prema preporukama Agencije, kako bi se osigurala pravilna primjena Zakona.

7.4. Obaveza imenovanja službenika za zaštitu ličnih podataka

GDPR je uvela i posebnu kategoriju u postupku zaštite ličnih podataka – *službenik za zaštitu ličnih podataka*, a koja je inkorporisana i u odredbe domaćeg Zakona. U pitanju je stručna osoba, koja na osnovu vlastitih kvalifikacija, pruža učinkovitu stručnu pomoć kontroloru podataka i obrađivaču u postupku obrade ličnih podataka. Kao takav, može biti zaposlen kod kontrolora podataka ili angažovan na osnovu ugovora o djelu. Podatke o konkretnom službeniku za zaštitu ličnih podataka objavljuje kontrolor podataka ili obrađivač, a isti se dostavljaju i Agenciji.

Obaveza imenovanja službenika za zaštitu ličnih podataka nije predviđena za sve kontrolore i obrađivače podataka, već samo u sljedećim slučajevima, što je determinisano posebnostima određenih djelatnosti:

1. vršenje obrade od strane javnog organa, izuzev sudova koji postupaju u okviru sudske nadležnosti;
2. ako osnovnu djelatnost kontrolora podataka ili obrađivača čini postupak obrade podataka, koji zbog svoje prirode, obima i/ili svrhe zahtijeva redovno i sistemsko praćenje nosioca podataka u velikom broju;
3. ako se osnovna djelatnost kontrolora podataka ili obrađivača sastoji od opsežne obrade posebnih kategorija podataka ili ličnih podataka u vezi sa osuđivanošću i krivičnim djelima.

Dakle, imenovanje i postupanje službenika za zaštitu ličnih podataka predviđeno je primarno za oblast javnih službi, te sistemske obrade ličnih podataka većeg broja nosilaca, odnosno obradu osjetljivih kategorija podataka, koji uživaju stroži nivo pravne zaštite, kao dodatni zaštitni mehanizam za postizanje zakonite obrade ličnih podataka. Kada su u pitanju kontrolori podataka i obrađivači koji ne potpadaju pod navedene slučajeve, Zakon je ostavio mogućnost da oni imenuju službenika za zaštitu ličnih podataka, a što mogu učiniti i udruženja ili organi koji predstavljaju te kontrolore podataka ili obrađivače, kada će službenik obavljati poslove u njihovo ime.

Međutim, Zakonom je istovremeno predviđeno da se odredbama *posebnih zakona (zakoni u određenim, specifičnim oblastima, što može uključivati i oblasti u kojima djeluju organizacije civilnog društva)*, može propisati obaveza imenovanja službenika za zaštitu ličnih podataka.

PREPORUKA ZA BUDUĆE POSTUPANJE: Provoditi stalni monitoring nad procesom usvajanja izmjena i dopuna posebnih zakona koji su relevantni za status i rad organizacija civilnog društva, te u slučaju da ova obaveza bude normirana, provesti postupak imenovanja službenika za zaštitu ličnih podataka u skladu sa odredbama ovog Zakona.

Iako ovaj službenik može biti zaposlen ili angažovan kod kontrolora podataka ili obrađivača, posebno je naglašena njegova autonomnost u odnosu na zakonom definisane poslove i zadatke službenika. Ona se ispoljava na način da on ne može dobivati nikakve instrukcije prilikom obavljanja ovih zadataka, ne može biti razriješen dužnosti ili na drugi način sankcionisan zbog obavljanja zadataka službenika, te kao takav odgovara neposredno najvišem nivou rukovodstva kontrolora podataka ili obrađivača.

Službenik za zaštitu ličnih podataka uključen je u sva pitanja koja se tiču zaštite ličnih podataka, a Zakonom su taksativno normirani njegovi zadaci:

1. informisanje i savjetovanje kontrolora podataka ili obrađivača i zaposlenih koji obavljaju obradu o njihovim obavezama iz ovog zakona i drugih zakona kojima se propisuje zaštita ličnih podataka;
2. praćenje poštovanja Zakona i drugih zakona kojima se propisuje zaštita ličnih podataka, kao i politika kontrolora podataka ili obrađivača u vezi sa zaštitom ličnih podataka, uključujući i podjelu odgovornosti, podizanje svijesti i osposobljavanje zaposlenih koji učestvuju u radnjama obrade, kao i s tim povezanim revizijama;
3. pružanje savjeta, kada je to zatraženo, u vezi s procjenom uticaja na zaštitu ličnih podataka i praćenje njenog izvršavanja;
4. saradnja s Agencijom;
5. djelovanje kao kontakt-tačka za Agenciju o pitanjima koja se tiču obrade, što uključuje i prethodno savjetovanje nakon izvršene procjene rizika, ali i savjetovanje po potrebi, o svim drugim pitanjima.

8. INSTITUCIJE ZA PROVOĐENJE ZAKONA O ZAŠTITI LIČNIH PODATAKA

8.1. Status Agencije za zaštitu ličnih podataka BiH

Agencija za zaštitu ličnih podataka BiH predstavlja centralni nadzorni organ u implementaciji ovog Zakona. U odnosu na njegovu pravnu prirodu, možemo potvrditi da je u pitanju organ uprave na nivou BiH, konkretnije samostalna upravna organizacija, u pogledu čijeg statusa i organizacije se pored odredbi ovog Zakona, primjenjuju odredbe Zakona o upravi BiH.¹⁷ U pogledu odnosa prema drugim tijelima javne vlasti, Zakon o zaštiti ličnih podataka BiH, posebno naglašava princip *nezavisnosti* Agencije, na način da Agencija djeluje nezavisno pri obavljanju svojih nadležnosti, a direktor, zamjenik direktora i zaposlenici prilikom obavljanja dodijeljenih ovlaštenja i dužnosti ne smiju biti izloženi neposrednom ili posrednom vanjskom uticaju i ne smiju ni od koga tražiti ili primati instrukcije. Agencija za svoj rad odgovara Parlamentarnoj skupštini Bosne i Hercegovine, kroz podnošenje godišnjeg izvještaja o zaštiti ličnih podataka.

8.2. Nadležnosti Agencije za zaštitu ličnih podataka BiH

Zakonom su Agenciji povjerena *izuzetno široka ovlaštenja*, koja se kao takva mogu podijeliti u dvije velike grupe: i. *regulatorna*, u vidu donošenja čitavog niza podzakonskih akata neophodnih za primjenu Zakona; ii. *nadzorna*, u smislu praćenja postupka obrade ličnih podataka u BiH u skladu sa definisanim normativnim okvirom. U nastavku ćemo navesti ključne nadležnosti Agencije utvrđene ovim Zakonom:¹⁸ praćenje i primjene Zakona, promovisanje javne svijesti i razumijevanja koncepta obrade ličnih podataka, pružanje usluga savjetovanja u vezi zaštite prava i sloboda fizičkih lica u postupku obrade, razmatranje prigovora na obradu podataka i u roku od 90 dana donošenje rješenja po izjavljenom prigovoru.

Pored ovih, načelno postavljenih nadležnosti, od posebne važnosti su sljedeća ovlaštenja Agencije: i. provođenje inspekcijskog nadzora, ii. obavljanje revizije zaštite ličnih podataka, iii. nalaganje kontroloru podataka i obrađivaču, a prema potrebi i predstavniku kontrolora podataka ili obrađivača, dostavljanje svih informacija potrebnih za obavljanje njenih zadataka; iv. obavještavanje kontrolora podataka ili obrađivača o navodnom kršenju Zakona; v. ostvarivanje pristupa svim podacima kojima raspolažu kontrolor podataka i obrađivač, a koji su potrebni za obavljanje njenih zadataka.

Takođe, u okviru njene nadzorne funkcije, Agencija raspolaže i tzv. korektivnim ovlaštenjima, od kojih posebno ističemo: i. *izricanja upozorenja* kontroloru podataka ili obrađivaču da bi namjeravana obrada mogla lako predstavljati kršenje Zakona; ii. *izricanje opomena kontroloru podataka ili obrađivaču*, ako se obradom krši Zakon; iii. nalaganje kontroloru podataka ili

¹⁷ Zakon o upravi („Službeni glasnik BiH“, broj 32/02, 102/09, 72/17)

¹⁸ Detaljan pregled: članovi 101 – 105. Zakona o zaštiti ličnih podataka BiH

obrađivaču da postupi po zahtjevu nosioca za ostvarivanje predviđenih prava; iv. nalaganje da se obrada uskladi sa zakonskim odredbama; v. privremeno ili trajno ograničavanje ili zabranjivanje obrade; vi. oduzimanje certifikata; vii. izdavanje prekršajnih naloga, odnosno podnošenje zahtjeva za pokretanje prekršajnog postupka.

8.3. Inspeksijski nadzor

Jedan od oblika nadzorne funkcije Agencije jeste i provođenje inspeksijskog nadzora, kojeg obavljaju inspektori Agencije. Inspeksijski nadzor se sastoji iz neposrednog uvida u zakonitost rada postupanja kontrolora podataka i obrađivača s ciljem provjere usklađenosti njegovog rada s Zakonom i drugim propisima koji se odnose na zaštitu ličnih podataka. Zakon prepoznaje tri vrste inspeksijskog nadzora:

- a. *Redovni* – provodi se na osnovu godišnjeg i mjesečnog plana inspeksijskog nadzora;
- b. *Vanredni* - provodi se na osnovu prigovora ili postupanja po službenoj dužnosti kada je, u odnosu na konkretni slučaj, potrebno izvršiti inspeksijski nadzor;
- c. *Revizijski* - provodi se nakon redovnog ili vanrednog inspeksijskog nadzora s ciljem provjere izvršenja naloženih upravnih mjera.

Kontrolor podataka i obrađivač dužni su inspektorom omogućiti nesmetano provođenje inspeksijskog nadzora, a prilikom provođenja inspektor ima pravo pregledati sve poslovne prostorije i objekte u kojima se obrađuju lični podaci, proces rada, uređaje, isprave i dokumentaciju.

Pored istaknutih razlika između ova tri oblika inspeksijskih nadzora, prisutna je i dodatna, a ona se tiče mogućnosti pravnog preispitivanja odluka donesenih u okviru inspeksijskog nadzora. Tako, Rješenje iz *redovnog* inspeksijskog nadzora donosi **inspektor**, protiv kojeg je dozvoljena **žalba direktoru Agencije** u roku od 15 dana od dana prijema rješenja. S druge strane, rješenje u postupku nakon izvršenog *vanrednog* i *revizijskog* inspeksijskog nadzora **donosi direktor Agencije** i ono je **konačno u upravnom postupku**.

8.4. Status odluka Agencije

Odluke Agencije nakon iscrpljivanja internih pravnih lijekova stiču svojstvo **konačnosti** u upravnom postupku, što za posljedicu ima da je njihovo preispitivanje moguće isključivo u okviru upravnog spora. S obzirom da je u pitanju upravna organizacija na nivou BiH, stvarnu nadležnost u konkretnim upravnim sporovima ima Upravno odjeljenje Suda BiH, shodno odredbi člana 8 Zakona o Sudu BiH.¹⁹ Predmetni upravni spor fizičko lice, kontrolor podataka ili obrađivač mogu pokrenuti tužbom u roku od 60 dana od dana zaprimanja odluke Agencije, a njegovo pokretanje, ne sprečava subjekte da koriste i druga upravna (predviđena Zakonom o upravnom postupku BiH) i vansudska sredstva zaštite prava. Na drugoj strani, nosilac podataka ima pravo pokrenuti upravno spor u roku od 90 dana, ukoliko Agencija ne riješi prigovor ili ne

¹⁹ Zakon o sudu BiH („Službeni glasnik BiH“, broj 49/09, 74/09, 97/09)

obavijesti nosioca podataka o napretku ili ishodu postupka po prigovoru, ne dovodeći u pitanje druga upravna ili vansudska pravna sredstva.

8.5. Sankcije za povrede Zakona

Radi sankcionisanja kršenja obaveza utvrđenih ovim normativnim okvirom, Agencija je ovlaštena izricati novčane kazne, koje se u svakom pojedinačnom slučaju, trebaju zasnivati na principima djelotvornosti, srazmjernosti i odvraćanja, a iznosi kazne utvrđeni su u različitim rasponima, zavisno od vrste i prirode konkretne povrede, te načina postupanja kontrolora podataka i obrađivača u odnosnoj situaciji.

Prilikom odlučivanja o kazni i njenom iznosu, Agencija posebno cijeni čitav niz relevantnih okolnosti: i. priroda, težina i trajanje povrede, imajući u vidu prirodu, obim i svrhu predmetne obrade, kao i broj nosilaca podataka i stepen štete koju su pretrpjeli; ii. da li povreda ima obilježje namjere ili nepažnje; iii. svaka radnja koju je kontrolor podataka ili obrađivač preduzeo kako bi ublažio štetu koju su pretrpjeli nosioci podataka; iv. stepen odgovornosti kontrolora podataka ili obrađivača, pri čemu se uzimaju u obzir tehničke i organizacione mjere koje su primijenili; v. sve utvrđene prethodne povrede od kontrolora podataka ili obrađivača; vi. stepen saradnje s Agencijom na otklanjanju povrede i ublažavanju mogućih štetnih posljedica povrede; vii. kategorija ličnih podataka na koje povreda utiče.

Interni kapaciteti Agencije

Zakonodavac je imperativno predvidio da Agencija mora imati ljudske, tehničke i finansijske resurse, prostorije i infrastrukturu potrebne za efikasno obavljanje svojih nadležnosti, uključujući i ovlaštenja koja se odnose na međunarodnu uzajamnu pomoć i saradnju. Dakle, ispunjenje ovih kadrovsko – tehničkih uslova predstavlja početnu pretpostavku za djelotvorno i zakonito vršenje dodijeljenih nadležnosti, što se u konačnici odražava i na kvalitet pravne zaštite ličnih podataka u Bosni i Hercegovini. U ovom kontekstu, posebni izazovi biće prisutni na planu kadrovskih kapaciteta Agencije, gdje trenutno prema dostupnim podacima, Odsjek za inspekcijski nadzor i prigovore ima ukupno pet zaposlenika (šef Odsjeka i četiri stručna savjetnika za inspekcijski nadzor), a raspolaže izuzetno širokim i strogim ovlaštenjima, naročito u kontekstu eventualnog kažnjavanja subjekata. Zbog toga smo mišljenja da se naročito ovi kapaciteti trebaju ojačati, kako bi sama Agencija bila u potpunosti osposobljena za učinkovito izvršavanje postavljenih zadataka.

9. KLJUČNI IZAZOVI ZA ORGANIZACIJE CIVILNOG DRUŠTVA U POSTUPKU ZAŠTITE LIČNIH PODATAKA

U nastavku analize, biće predstavljene ključne specifičnosti ove regulative u odnosu na status i djelovanje organizacija civilnog društva, uz prisutne izazove u njenoj implementaciji. Pored prethodno analiziranog pitanja „javnog interesa“, čijem postizanju teže nevladine organizacije i koji predstavlja osnov za ublažavanje strogog režima zaštite ličnih podataka, neophodno je ukazati i na dva važna aspekta ovog problema – postupanja organizacija civilnog društva kao poslodavca i afirmacija slobode izražavanja u uslovima zaštite ličnih podataka.

9.1. ORGANIZACIJE CIVILNOG DRUŠTVA KAO POSLODAVACI

Kao poslodavci, nevladine organizacije obrađuju veliki broj ličnih podataka svojih zaposlenika, volontera i vanjskih saradnika. Ovi podaci ne obuhvataju uvijek samo osnovne informacije poput imena, adrese i kontakt podataka, već ponekad i osjetljive podatke kao što su zdravstveno stanje, socijalni status ili podaci o plaćama. Zakon o zaštiti ličnih podataka postavlja jasna pravila za prikupljanje, čuvanje, korištenje i dijeljenje ovih podataka, te zahtijeva da NVO-i kao poslodavci postupaju transparentno, zakonito i odgovorno.

U praksi to znači da organizacija mora:

- imati pravnu osnovu za obradu ličnih podataka svojih zaposlenika;
- minimizirati količinu ličnih podataka koje prikuplja;
- jasno obavijestiti zaposlenike i sva druga lica o svrsi i načinu obrade njihovih podataka;
- čuvati podatke sigurno i ažurno;
- ograničiti pristup podacima samo na ovlaštene osobe;
- obrisati ili anonimizirati podatke kada više nisu potrebni za svrhu zbog koje su prikupljeni.

Ova pravila nisu formalnost, već njihovo poštivanje štiti i zaposlenike i samu organizaciju od pravnih i reputacijskih rizika.

Specifičnost NGO sektora ogleda se i u kombinaciji profesionalnog i volonterskog rada, gdje se podaci često dijele između više timova i projekata, a istovremeno postoji ograničeni kapacitet za implementaciju naprednih sigurnosnih mjera. Također, mnogi NVO-i posluju s ograničenim budžetom, što može otežati uvođenje sofisticiranih rješenja za zaštitu ličnih podataka.

U praksi, navedeno podrazumijeva da nevladina organizacija od trenutka kada započne proces izbora novog zaposlenika, volontera ili vanjskog saradnika, treba voditi računa da postupanjem ne povrijedi prava tih lica u vezi sa ličnim podacima.

Preporučljivo je da, ukoliko organizacija objavljuje svojevrstni oglas za posao, u istom zahtijeva minimalnu količinu ličnih podataka koju će kandidati za posao morati dostaviti²⁰. Spomenuto bi trebalo biti ograničeno na osnovne identifikacione i kontakt podatke kao što su ime, prezime, broj telefona i e-mail, dok se JMBG ni u kom slučaju ne smije zahtijevati, niti obrađivati u ovoj fazi. Naravno, osim navedenog, organizacija ima pravo tražiti od kandidata da dostave osnovne informacije o stručnoj spremi i radnom iskustvu.

Također, nije dozvoljeno tražiti podatke o osuđivanosti ili druge podatke koji spadaju u kategoriju posebnih podataka (podaci o zdravlju, spolnom životu, seksualnoj orijentaciji i sl). Potrebno je da kandidati za posao uz prijavu dostave i potpisan obrazac saglasnosti za obradu ličnih podataka.

U nastavku procesa, organizacija ima mogućnost obavljati testiranja i intervju sa ciljem odabira budućeg zaposlenika, pri čemu treba imati u vidu da se u takvim testiranjima prikupljaju isključivo podaci koji su neophodni za ocjenu kvalificiranosti kandidata za posao.

Nakon što organizacija izvrši izbor budućeg zaposlenika, potrebno je da ugovor o radu, također, bude zaključen uz prikupljanje što manje količine ličnih podataka. Naročito je važno imati u vidu da je Agencija za zaštitu ličnih podataka BiH dala Mišljenje²¹ u kojem se navodi da se ugovor o djelu može zaključivati bez navođenja jedinstvenog matičnog broja, te da je isti dozvoljeno obrađivati isključivo u dokumentima predviđenim za te svrhe (npr. poreske obaveze), ali ne i u samom ugovoru o djelu.

Iz navedenog jasno proizlazi potreba minimiziranja količine ličnih podataka koja se prikuplja, te razvijanje svijesti svih poslovnih subjekata, uključujući i one u civilnom sektoru, u tom smjeru.

Sva radno angažovana lica u NVO imaju pravo biti obaviještena o svojim pravima i obavezama u smislu Zakona o zaštiti ličnih podataka, slijedom čega postoji potreba donošenja odgovarajućih akata u tom smjeru. Prevažodno, misli se na pravilnike, politike privatnosti, interne procedure, ali i obavještenja koja će biti dostupna svim radno angažovanim licima u organizaciji. Nakon što se zaposlenici, volonteri i saradnici upoznaju sa svojim pravima i obavezama, a koje moraju biti jasno precizirane u aktima organizacije, pristupit će potpisivanju odgovarajućih izjava, a saglasnosti isključivo u slučajevima kada je ona zakonit pravni osnov.

Radi se o izjavi povjerljivosti kojom se zaposlenik obavezuje da će lične podatke drugih lica do kojih dođe radeći u ili za organizaciju, čuvati kao tajne, kao i o saglasnosti za obradu ličnih podataka (u slučaju ako se fotografije zaposlenika koriste za web stranicu, promocije ili publikacije).

²⁰ Agencija za zaštitu osobnih podataka (AZOP). *Smjernice o obradi osobnih podataka u području radnih odnosa*

²¹ Mišljenje Agencije za zaštitu ličnih podataka u Bosni i Hercegovini, broj 03-1-02-1-1597-2/25 od 14.01.2026. godine

Naravno, određena postupanja i organizacione ili tehničke mjere, same po sebi zahtijevaju i donošenje drugih akata pa je tako, primjerice, svaka organizacija koja posjeduje videonadzorne sisteme, u obavezi da posjeduje i akt o videonadzoru kojim se detaljno reguliše u kojim prostorijama će isti biti instaliran, sa kojom svrhom, prema kojem pravnom osnovu, koliko dugo će se takvi snimci pohranjivati, te kome se zaposleni i druga lica mogu obratiti u vezi sa predmetnim snimcima. Također, važno je da prije ulaska u prostorije koje su pod videonadzorom, o tome bude istaknuto vidljivo obavještenje.

Nadalje, ukoliko organizacija koristi usluge eksternog računovodstva, IT servisa ili drugih kompanija, a koje shodno tom angažmanu obrađuju podatke zaposlenika (plate, prisustvo na radu i sl), potrebno je da organizacija sa konkretnom kompanijom ima zaključen ugovor o povjerenoj obradi ličnih podataka, na koji način se definiše postupanje sa ličnim podacima zaposlenika i drugih lica povezanih sa organizacijom.

Nesporno je da pobrojana prava, osim što pružaju veliki obim zaštite nosiocima podataka, mogu predstavljati i svojevrsni instrument pritiska prema organizaciji kao poslodavcu. Primjera radi, nezadovoljni zaposlenik, umjesto pokretanja radnog spora koji u bh pravosudnom ambijentu u pravilu znači dugogodišnje parničenje, može odlučiti da problematizira postupanje organizacije sa njegovim ličnim podacima, a sve kako bi ostvario druga prava, a ne ona iz oblasti zaštite ličnih podataka. Naravno, na organizacijama je da adekvatnim postupanjem prema ličnim podacima zaposlenih onemoguće takvu argumentaciju, te da svojim odnosom ne ostave mogućnosti za bilo kakav vid malicioznog ili osvetničkog prijavljivanja povreda ličnih podataka.

Ukratko, NVO kao poslodavac mora balansirati između operativnih potreba i stroge odgovornosti prema Zakonu o zaštiti ličnih podataka, osiguravajući da svi podaci budu prikupljeni, obrađeni i čuvani na siguran, zakonit i transparentan način.

9.2. SLOBODA IZRAŽAVANJA

Pravo na slobodu izražavanja na evropskom pravnom prostoru svoju punu afirmaciju doživjelo je usponom liberalne demokratije, a usvajanje Evropske konvencije o ljudskim pravima, po prvi put je institucionalizirana zaštita slobode izražavanja kroz efikasan sistem nadzora – Evropski Sud za ljudska prava (ESLJP). U vlastitoj praksi, Sud je razvio standarde koji se primjenjuju na nacionalne pravne poretke i koji su postali pravno obavezujući za sve države članice Vijeća Evrope.²²

Tako ESLJP, u presudi *Magyar Helsinki Bizottság protiv Mađarske*²³, pozivajući se na prethodnu odluku u predmetu *Cengiz i drugi protiv Turske*²⁴, naglašava kako se određeni politički sadržaji koji bivaju zanemareni od strane tradicionalnih medija često dijele putem internetskih platformi, što doprinosi razvoju tzv. građanskog novinarstva. Sud ističe da

²² Tarik Velić. *Sloboda izražavanja u pravu Vijeća Evrope*. Magistarski rad (Sarajevo: Pravni fakultet Univerziteta u Sarajevu, 2025).

²³ Magyar Helsinki Bizottság protiv Mađarske, br. 18030/11, 8. novembar 2016.

²⁴ Cengiz i drugi protiv Turske, br. 48226/10 i 14027/11, 1. decembar 2015.

blokiranje takvih digitalnih servisa korisnicima oduzima važno sredstvo za ostvarivanje njihovog prava na slobodu primanja i širenja informacija i ideja.

Nesporno je da organizacije civilnog društva mogu biti usko povezane sa pojedinačnim aktivistima ili novinarima – amaterima, a uloga građanskog novinarstva je u savremenom svijetu od izuzetnog značaja, pogotovo ukoliko se radi o blogeru – „zviždaču“ sa informacijama „iznutra“.

Također, moguće je primijetiti da nevladine organizacije nerijetko i same, na svojim web stranicama i profilima na društvenim mrežama, objavljuju članke i iznose stavove o društveno-političkom životu, djelovanju drugih lica, te saznanjima koje imaju u vezi sa relevantnim događajima. Na ovaj način organizacije uzimaju svojevrsnu ulogu građanskih novinara, pri čemu je njihovo djelovanje važno sagledati u svjetlu slobode izražavanja.

Nadalje, NVO-i često djeluju u sektorima gdje kritičko mišljenje, zagovaranje ili javno komentiranje društvenih i političkih pitanja predstavljaju ključnu aktivnost. Istovremeno, ove organizacije moraju poštovati Zakon o zaštiti ličnih podataka, što stvara jedinstveni balans između **otvorenog izražavanja i privatnosti pojedinaca**.

Potrebno je voditi računa, prije svega da pravo na slobodu izražavanja iz čl. 10. Evropske konvencije o ljudskim pravima ne predstavlja apsolutno pravo, odnosno, kako propisuje stav 2 istog člana Konvencije, ne smije biti zloupotrijebljeno na štetu nacionalne sigurnosti, javnog reda, zdravlja i morala, širenja povjerljivih podataka ili prava drugih lica. Posebno je važno imati u vidu da se pravo na slobodu izražavanja često nalazi u koliziji sa pravom na privatnost i zaštitu ličnih podataka iz čl. 8. Evropske konvencije, te da se u svakom konkretnom slučaju mora uspostaviti pravična ravnoteža između ova dva prava, vodeći računa o proporcionalnosti, javnom interesu i zaštiti dostojanstva pojedinca.

U kontekstu ograničenja slobode izražavanja iz stava 2 člana 10 Evropske konvencije, posebno u dijelu koji se odnosi na zabranu širenja povjerljivih podataka, nužno je sagledati i pojam zaštite ličnih podataka, budući da se upravo lični podaci, prema svojoj prirodi, u velikom broju slučajeva mogu podvesti pod kategoriju osjetljivih podataka, čije neovlašteno objavljivanje može dovesti do ozbiljnog zadiranja u privatnost i dostojanstvo pojedinca.

Recimo, kad su u pitanju krivični postupci, Sud je u više navrata naglašavao da otkrivanje identiteta osoba povezanih sa krivičnim postupcima zahtijeva naročitu pažnju, jer objavljivanje ličnih podataka može imati dugoročne posljedice po privatni i društveni život.

U predmetu *Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft protiv Austrije*²⁵, radilo se o tome da je informativni časopis objavio dijelove iz zapisnika sačinjenog u postupku protiv stranih policajaca koji su pratili deportaciju lica koje je preminulo pod nerazjašnjenim okolnostima. Domaći sudovi su izrekli kaznu časopisu, jer su zaključili da objava identiteta policajca negativno utječe na njegov privatni i društveni život i krši njegove legitimne interese.

²⁵ Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH protiv Austrije (br. 2), br. 62746/00, 14. novembar 2002

Nakon što su iscrpljeni svi pravni lijekovi pred domaćim pravosuđem, časopis je podnio predstavku Evropskom sudu za ljudska prava, koji je istu odbio, zaključujući da austrijski sudovi imaju relevantne razloge za izricanje kazne, uzimajući u obzir ranu fazu krivičnog postupka i potrebu zaštite policajca od „suđenja u medijima“, te primjenu pretpostavke nevinosti. Na kraju, Sud je zaključio da objava punog imena policajca nije doprinijela javnom interesu u mjeri koja bi opravdala narušavanje njegovih privatnih prava.

Posebno zabrinjavajuća situacija sa aspekta slobode izražavanja nastupila je izmjenama Krivičnog zakonika Republike Srpske, kojim je kao zasebno krivično djelo, uz propisanu novčanu kaznu, inkriminisano iznošenje ili prenošenje štogod iz ličnog ili porodičnog života nekog lica, što može škoditi njegovoj časti ili ugledu, a što nije, niti može predstavljati činjenice koje su od opravdanog interesa. Strože kažnjavanje predviđeno je ukoliko je predmetno krivično djelo učinjeno putem štampe, radija, televizije, kompjuterske mreže ili drugih vidova komunikacije, na javnom skupu ili na drugi način, zbog čega je ono postalo dostupno većem broju lica, a dodatno je propisano da se istinitost ili neistinitost onog što se iznosi, ne dokazuje. U kontekstu slobode medija u BiH, u Izvještaju organizacije *Reporters without borders* (RSF)²⁶, navodi se:

„Pristup informacijama nominalno je omogućen svim novinarima, ali izmjene krivičnog zakonodavstva uvode obavezu prethodnog pristanka za objavljivanje ličnih podataka, uz mogućnost zatvorske kazne (što predstavlja pogrešan navod). Iako postoje propisi o zaštiti izvora i etički kodeksi, njihova primjena ostaje neizvjesna“

Izvještaj je imao za cilj analizirati i ocijeniti slobodu medija u Bosni i Hercegovini, ali citirani dio Izvještaja upućuje, između ostalog, i na to da je u Bosni i Hercegovini, čak i kroz odredbe krivičnog zakonodavstva, stavljen značajan naglasak na zaštitu ličnih podataka, te neovlašteno objavljivanje istih.

Shodno prethodno navedeno, a u kontekstu ostvarivanja prava na slobodu izražavanja, neophodno je ukazati na bitnost sljedećih aspekata:

- **Očuvanje anonimnosti i privatnosti:** Prilikom objavljivanja mišljenja, izvještaja ili javnih stavova, NVO mora biti naročito oprezna da ne otkriva lične podatke trećih osoba bez odgovarajućeg pravnog osnova. Ovo posebno važi za posebne kategorije ličnih podataka zaposlenika, volontera ili korisnika usluga.
- **Pravna odgovornost organizacije:** Sloboda izražavanja ne oslobađa NVO od odgovornosti za zaštitu ličnih podataka. Informacije koje se dijele u javnosti ili među članovima moraju biti obrađene u skladu sa zakonom, uz jasno definisanu svrhu i minimalizaciju rizika od povrede privatnosti.
- **Transparentnost i informisani pristanak:** Ako zaposlenici ili volonteri učestvuju u zadacima i komunikacijama koje uključuju lične podatke, organizacija mora osigurati

²⁶ Reporters Without Borders (RSF), „Bosna i Hercegovina“, dostupno na: <https://rsf.org/en/country/bosnia-herzegovina>.

da su svi uključeni informisani o obradi ličnih podataka, a saglasnost se pribavlja isključivo u slučajevima kada je ona zakonit i primjeren pravni osnov.

- **Osjetljivi konteksti:** NVO-i koji se bave ljudskim pravima, zaštitom ranjivih grupa ili političkim pitanjima često rukovode posebno osjetljivim podacima. U ovakvim slučajevima, pravo na slobodu izražavanja mora biti uravnoteženo s dodatnim mjerama zaštite privatnosti.

U praksi, ovo znači da organizacije moraju razviti **jasne interne procedure i politike privatnosti**, koje omogućavaju slobodno izražavanje zaposlenika i volontera, a istovremeno štite lične podatke svih uključenih. Balansiranje slobode izražavanja i zaštite privatnosti ne bi trebao predstavljati ograničenje kreativnosti ili misije organizacije, već biti ključni element zakonitog i odgovornog upravljanja podacima.

10. PRAKTIČNI PRIRUČNIK

U ovom dijelu Priručnika predstavljeni su praktični primjeri pojedinih akata koji se u praksi najčešće donose u postupku usklađivanja poslovanja sa Zakonom o zaštiti ličnih podataka. Važno je naglasiti da donošenje ovih akata ne smije imati za cilj samo formalno ispunjavanje zakonskih obaveza, već mora odražavati stvarne potrebe organizacije i biti u vezi sa konkretnim obradama ličnih podataka koje se u njenom radu provode. Akti koji nisu usklađeni sa stvarnom praksom organizacije ne mogu pružiti stvarnu pravnu zaštitu, bez obzira na njihovo postojanje.

Iz tog razloga, u nastavku se ne daju univerzalni obrasci primjenjivi na sve organizacije, već isključivo **okvirni primjeri i strukture pojedinih akata** koje je, uz pomoć stručnih lica, nužno prilagoditi specifičnostima svake organizacije, njenim aktivnostima, kategorijama lica čiji se podaci obrađuju, vrstama podataka i svrsi obrade.

Obim i vrsta akata koje je potrebno donijeti razlikuju se od organizacije do organizacije, u zavisnosti od njihovih objektivnih potreba. Među aktima koji se u praksi najčešće ispostavljaju kao neophodni izdvajaju se:

- pravilnik o zaštiti ličnih podataka;
- politika privatnosti/opće obavještenje o obradi ličnih podataka;
- politika kolačića;
- obavještenje o obradi ličnih podataka za zaposlene;
- akt o videonadzoru;
- izjava o čuvanju povjerljivosti i zaštiti ličnih podataka;
- saglasnosti za obradu ličnih podataka;
- ugovor o povjerenoj obradi ličnih podataka;
- interne procedure;
- evidencije aktivnosti obrade;
- evidencije povreda ličnih podataka;

- odluka o imenovanju službenika za zaštitu ličnih podataka, ukoliko za tim postoji potreba.

Posebnu pažnju organizacije trebaju posvetiti situacijama u kojima se lični podaci razmjenjuju ili prenose van Bosne i Hercegovine, naročito u saradnji sa međunarodnim organizacijama i partnerima, imajući u vidu odredbe čl. 46–51 Zakona o zaštiti ličnih podataka.

Prilog 1.

PRAVILNIK O ZAŠTITI LIČNIH PODATAKA

I OPĆE ODREDBE

Član 1. (Predmet)

(1) Ovim Pravilnikom uređuju se osnovna pravila, mjere i odgovornosti u vezi sa obradom i zaštitom ličnih podataka koje vrši *organizacija* u skladu sa važećim propisima o zaštiti ličnih podataka.

(2) Ovaj Pravilnik se primjenjuje u odnosu na sve vidove obrade ličnih podataka, bez obzira na to da li se organizacija pojavljuje u svojstvu kontrolora, obrađivača ili primaoca podataka.

Član 2. (Pojmovi i definicije)

(1) Pojmovi korišteni u ovom Pravilniku imaju značenje utvrđeno važećim propisima o zaštiti ličnih podataka.

(Komentar: Zakon o zaštiti ličnih podataka definiše pojam ličnog podatka, posebne kategorije ličnih podataka, kontrolora, obrađivača, primaoca podataka, treće strane i sl. pa se namjerno ne ponavljaju zakonske definicije.)

Član 3. (Rodna ravnopravnost)

(1) Izrazi koji se koriste u ovom Pravilniku i imaju rodno značenje, koriste se neutralno i odnose se jednako na muški i ženski rod.

Član 4. (Principi obrade ličnih podataka)

(1) Obrada ličnih podataka u okviru djelovanja organizacije provodi se u skladu sa sljedećim principima:

- a) Zakonitosti;
- b) Ograničenja svrhe;
- c) Smanjenja obima podataka;
- d) Tačnosti;
- e) Ograničenja čuvanja;
- f) Cjelovitosti i povjerljivosti;
- g) Pouzdanosti;

Član 5. (Obrada posebnih kategorija ličnih podataka)

(1) Obrada ličnih podataka koji otkrivaju rasno ili etničko porijeklo, politička mišljenja, vjerska ili filozofska uvjerenja ili pripadnost sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije lica, podataka o zdravlju ili podataka o spolnom životu ili seksualnoj orijentaciji lica je zabranjena.

(2) Izuzetno od stava (1) ovog člana, obrada posebnih kategorija podataka je dozvoljena ako je ispunjen jedan od sljedećih uslova:

- a) Nosilac podataka je dao izričitu saglasnost za obradu tih ličnih podataka za jednu ili više navedenih svrha;
- b) Obrada se vrši u okviru legitimnih aktivnosti udruženja, fondacije ili druge neprofitne organizacije sa političkim, filozofskim, vjerskim ili sindikalnim ciljem, pod uslovom da se obrada odnosi isključivo na članove ili bivše članove tog tijela ili na lica koja imaju redovne kontakte s njim u vezi sa njegovim ciljevima, te da lični podaci nisu otkriveni izvan tog tijela bez saglasnosti nosilaca podataka;
- c) Obrada je neophodna radi izvršenja obaveza i ostvarivanja posebnih prava kontrolora ili nosioca podataka u oblasti radnog prava i prava o socijalnom osiguranju;
- d) Obrada se odnosi na lične podatke za koje je očigledno da ih je nosilac podataka javno objavio.

Komentar: Detaljno definisati izuzetke od odredbe stava 1 ovog člana u skladu sa Zakonom (član 11)

Član 6. (Posebni slučajevi obrade)

(1) Organizacija obrađuje podatke u posebnim slučajevima, isključivo kada je to opravdano, zakonito i srazmjerno svrsi obrade. Posebni slučajevi obrade uključuju:

- a) Obrada u novinarske svrhe
- b) Obrada u svrhe akademskog, umjetničkog ili književnog izražavanja
- c) Obrada jedinstvenog matičnog broja (JMBG)
- d) Obrada ličnih podataka u kontekstu zaposlenja
- e) Obrada u svrhu arhiviranja u javnom interesu, u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe

Komentar: Ova odredba može biti posebno relevantna za organizacije koje se bave zagovaračkim i istraživačkim aktivnostima, s obzirom na to da takve aktivnosti često uključuju obradu ličnih podataka u širem javnom kontekstu.

Član 7. (Saradnja s Agencijom za zaštitu ličnih podataka u Bosni i Hercegovini)

(1) Organizacija i obrađivač su dužni, na obrazložen i na osnovu zakona opravdan zahtjev, saradivati s Agencijom za zaštitu ličnih podataka u obavljanju njenih zadataka, te istu na propisani način izvještavati o slučajevima povreda ličnog podatka.

(2) Organizacija ima obavezu da u zakonom propisanim slučajevima, bez odgađanja, a pisanim putem obavijesti nosioca podataka o povredi ličnog podatka, ako je vjerovatno da će povreda tog podatka uzrokovati visok rizik za prava i slobode fizičke osobe.

II SVRHA OBRADJE LIČNIH PODATAKA I PRAVNI OSNOV

Član 8. (Svrha obrade ličnih podataka)

(1) Organizacija prikuplja i obrađuje lične podatke u sljedeće svrhe:

Navesti svrhe

(2) Lični podaci se čuvaju u formi koja je najpogodnija za svrhu za koju se prikupljaju i obrađuju.

Član 9. (Pravni osnov obrade ličnih podataka)

(1) Obrada ličnih podataka iz člana 8 ovog Pravilnika vrši se na osnovu sljedećih pravnih osnova:

- a) izvršenje ugovora ili predugovornih radnji;
- b) ispunjavanje zakonskih obaveza kontrolora;
- c) legitimni interes kontrolora;
- d) saglasnost lica na koje se podaci odnose.

(2) Saglasnost iz stava (1) tačka d) ovog člana mora biti dobrovoljna, izričita, informisana i nedvosmislena, te se može povući u svakom trenutku, bez uticaja na zakonitost obrade prije njenog povlačenja.

III KATEGORIJE NOSILACA PODATAKA I KATEGORIJE PODATAKA

Član 10. (Kategorije nosilaca podataka)

(1) U smislu ovog Pravilnika, lični podaci koje obrađuje organizacija odnose se na sljedeće kategorije lica:

- a) Kandidati za zapošljavanje;
- b) Zaposlenici i bivši zaposlenici;
- c) Predstavnici donatora i poslovnih partnera;
- d) Posjetioci poslovnih prostorija i učesnici događaja;

- e) Korisnici internet stranice i digitalnih platformi;
- f) Druga lica u skladu sa zakonom.

Član 11. (Kategorije podataka)

(1) U okviru svoje djelatnosti, organizacija obrađuje sljedeće kategorije ličnih podataka, u zavisnosti od kategorije lica na koje se podaci odnose i svrhe obrade:

- a) Identifikacioni i kontakt podaci;
- b) Podaci o obrazovanju i radnom iskustvu;
- c) Podaci o zapošljavanju i radnom odnosu;
- d) Finansijski i poreski podaci;
- e) Podaci o komunikaciji i interakciji;
- f) Tehnički i elektronski podaci;
- g) Podaci prikupljeni putem videonadzora;
- h) Podaci o učešću na događajima;

(2) Organizacija obrađuje samo one lične podatke koji su **neophodni, primjereni i ograničeni na ono što je nužno** u odnosu na svrhe obrade iz ovog Pravilnika.

(3) Obrada posebnih kategorija ličnih podataka vrši se isključivo uz postojanje odgovarajućeg pravnog osnova, uz primjenu pojačanih tehničkih i organizacionih mjera zaštite.

IV ROKOVI ČUVANJA LIČNIH PODATAKA

Član 12. (Rokovi čuvanja ličnih podataka)

(1) Lični podaci se čuvaju samo onoliko dugo koliko je neophodno radi ostvarivanja svrha obrade iz ovog Pravilnika, osim ako je duži rok čuvanja propisan zakonom ili proizlazi iz ugovornih obaveza.

(2) Nakon isteka roka čuvanja, lični podaci se brišu, anonimiziraju ili trajno uništavaju, na siguran način, u skladu sa internim procedurama i važećim propisima.

(3) Okvirni rokovi čuvanja pojedinih kategorija ličnih podataka su:

Komentar: Definisati rokove za konkretne kategorije u skladu sa važećim propisima

V PRAVA NOSILACA PODATAKA

Član 13. (Prava nosilaca ličnih podataka)

(1) Nosilac ličnih podataka ima sljedeća prava u skladu sa važećim propisima o zaštiti ličnih podataka, uključujući Opštu uredbu o zaštiti podataka (GDPR):

- a) Pravo na informisanje;

- b) Pravo na pristup podacima;
- c) Pravo na ispravku;
- d) Pravo na brisanje („pravo na zaborav“);
- e) Pravo na ograničenje obrade;
- f) Pravo na prenosivost;
- g) Pravo na prigovor;
- h) Pravo na povlačenje saglasnosti;
- i) Pravo na podnošenje pritužbe;
- (j) Pravo na sudsku zaštitu.

(2) Organizacija je dužna omogućiti nosiocima podataka jednostavno, transparentno i besplatno ostvarivanje njihovih prava, osim u slučajevima predviđenim važećim zakonskim propisima u Bosni i Hercegovini.

(3) Zahtjevi nosilaca podataka podnose se pisanim putem, elektronskom poštom ili drugim odgovarajućim komunikacionim sredstvima, a Organizacija je dužna postupiti po zahtjevu bez nepotrebnog odgađanja, a najkasnije u roku od 30 dana od dana prijema zahtjeva.

(4) Organizacija može odbiti postupanje po zahtjevu ako je on očigledno neosnovan ili pretjeran, naročito zbog svog ponavljajućeg karaktera, uz obavezu da nosiocu podataka dostavi obrazloženo obavještenje.

(5) U slučaju da su podaci o kandidatu prikupljeni iz javno dostupnih izvora, Organizacija je dužna nosiocu podataka pružiti sve informacije o obradi (transparentnost) u trenutku prve komunikacije, a najkasnije u roku od 30 dana od dana prikupljanja podataka.

Komentar: U nastavku je potrebno razraditi spomenuta prava, način obraćanja organizaciji / službeniku za zaštitu ličnih podataka, upravljanje evidencijama o zahtjevima za pristup ličnim podacima itd.

VI MJERE ZAŠTITE LIČNIH PODATAKA

Član 14. (Obaveza primjene tehničkih i organizacionih mjera)

(1) Organizacija je dužna poduzeti mjere protiv neovlaštenog ili slučajnog pristupa ličnim podacima, mijenjanja, uništavanja ili gubitka ličnih podataka, neovlaštenog prenosa i drugih oblika njihove nezakonite obrade, te mjere protiv njihove zloupotrebe

Komentar: Definisati koje su tehničke i organizacione mjere, obaveze zaposlenika i rukovodilaca u odnosu na zaštitu ličnih podataka, te postupanje u slučaju saznanja o povredi ličnih podataka. Posebnu pažnju obratiti na informaciono – komunikacijske tehnologije i videonadzor

Član 15. (Prijenos ličnih podataka obrađivačima podataka)

(1) Organizacija može angažovati obrađivača za obradu ličnih podataka u ime organizacije koji u dovoljnoj mjeri garantuje primjenu odgovarajućih tehničkih i organizacionih mjera

(2) Odnos između organizacije i obrađivača bit će uređen ugovorom

Komentar: Potrebno je precizirati kategorije obrađivača (npr. IT kompanije, računovodstva) i definisati obavezne elemente pisanog ugovora. Također, treba propisati uslove za međunarodni prijenos podataka, uzimajući u obzir status BiH kao treće zemlje u odnosu na EU.

Član 16. (Službenik za zaštitu ličnih podataka)

(1) Organizacija će zbog prirode, obima i/ili svrhe obrade ličnih podataka koji se obrađuju, imenovati službenika za zaštitu ličnih podataka

(2) Organizacija je dužna obezbijediti da službenik za zaštitu ličnih podataka bude adekvatno uključen u sva pitanja koja se tiču zaštite ličnih podataka u okviru poslovnih aktivnosti

(3) Službenik za zaštitu ličnih podataka neposredno odgovara najvišem rukovodstvu u organizaciji

Komentar: Organizacije koje obrađuju velike količine podataka, a naročito ukoliko je riječ o posebnim kategorijama podataka, dužne su imenovati službenika za zaštitu ličnih podataka koji ima zadatke propisane odredbom čl. 41. Zakona. O imenovanju službenika obavještava se Agencija za zaštitu ličnih podataka.

VI EVIDENCIJE O OBRADI LIČNIH PODATAKA

Član 17. (Evidencije ličnih podataka)

(1) Evidencije o obradi ličnih podataka predstavljaju službene zapise koje vodi organizacija, a koje sadrže pregled svih aktivnosti obrade ličnih podataka, uključujući: način prikupljanja podataka, svrhu obrade, pravni osnov, rokove čuvanja, kao i druge relevantne informacije

(2) Evidencije o obradi ličnih podataka upisuju se u odgovarajuće obrasce

Komentar: Potrebno je definisati ko tačno vodi i ažurira evidencije, ko može pristupiti evidencijama, koje se konkretne evidencije ličnih podataka vode na nivou organizacije, te način čuvanja evidencija

IX ZAVRŠNE ODREDBE

Član 18 (Stupanje na snagu)

(1) Ovaj Pravilnik stupa na snagu istekom osmog dana nakon objavljivanja na oglasnoj ploči organizacije, a objavit će se i na web stranici organizacije.

Prilog 2

OBAVJEŠTENJE O OBRADI LIČNIH PODATAKA (ZA ZAPOSLENE)

Organizacija, sa sjedištem u _____ a koja ima svojstvo Kontrolora podataka u smislu Zakona o zaštiti ličnih podataka ("Službeni glasnik Bosne i Hercegovine", br. 12/2025 od: 28.02.2025), odnosno kao lice koje organizuje i odgovorno je za obradu ličnih podataka, ovim putem **obavještava zaposlene, pripravnike, volontere, vanjske saradnike**, kao i sva druga lica koja su na bilo koji način angažovana od strane organizacije, te čiji se podaci obrađuju o svim bitnim aspektima obrade njihovih podataka u skladu sa važećom regulativom.

1. KOJE PODATKE PRIKUPLJAMO I OBRADUJEMO?

Organizacija od zaposlenih prikuplja i obrađuje samo one lične podatke koji su **neophodni** za ostvarivanje konkretne, zakonite svrhe obrade, a naročito:

- identifikacione i kontakt podatke (ime i prezime, adresa, broj telefona, e-mail),
- podatke o plaćama, prisustvu na radu, godišnjim odmorima, bolovanjima i sl.
- druge podatke čija je obrada propisana zakonom ili nužna za sprovođenje programskih i projektnih aktivnosti

U posebnim slučajevima, organizacija može obrađivati i posebne kategorije podataka (npr. sindikalna pripadnost, podaci o zdravlju zaposlenih), isključivo uz vašu izričitu saglasnost ili kada je to neophodno za ostvarivanje prava iz radnog odnosa i socijalne zaštite.

Komentar: Prikupljanje JMBG ne smije biti pravilo – vidi čl. 54. Zakona

2. KOJI JE PRAVNI OSNOV OBRADJE?

Organizacija obrađuje lične podatke isključivo na osnovu važećih pravnih osnova i to:

- a) **zakonska obaveza;**
- b) **izvršavanje ugovora;**
- c) **saglasnost lica;**
- d) **legitimni interes;**

3. U KOJE SVRHE KORISTIMO PODATKE?

Lični podaci se obrađuju u sljedeće svrhe

Navesti svrhe

4. KO IMA PRISTUP PODACIMA?

Pristup ličnim podacima imaju isključivo:

Navesti lica koja imaju pristup

Svaki pristup podacima ograničen je na minimum neophodan za ostvarenje svrhe obrade.

5. KOJA PRAVA IMATE U ODNOSU NA ZAŠTITU VAŠIH PODATAKA A KOJE ORGANIZACIJA OBRADUJE?

Nosioci podataka čiji se lični podaci obrađuju imaju pravo da od organizacije zahtijevaju:

- a) pristup ličnim podacima koji se obrađuju
- b) informacije o obradi
- c) pravo na ispravku, brisanje i ograničenje obrade
- d) pravo na prigovor Agenciji
- e) pravo na sudsku zaštitu

Napomena: Ostvarivanje pojedinih prava može biti ograničeno u skladu sa zakonom.

6. KAKO SE ŠTITE VAŠI PODACI?

Organizacija primjenjuje odgovarajuće **tehničke i organizacione mjere zaštite** u cilju sprječavanja neovlaštenog pristupa, zloupotrebe, gubitka ili uništenja ličnih podataka zaposlenih i drugih radno angažovanihi lica, a naročito:

Komentar: Definisati koje su tehničke i organizacione mjere, obaveze zaposlenika i rukovodilaca u odnosu na zaštitu ličnih podataka, te postupanje u slučaju saznanja o povredi ličnih podataka. Posebnu pažnju obratiti na informaciono – komunikacijske tehnologije i videonadzor

7. KOLIKO DUGO SE ČUVAJU VAŠI PODACI?

Organizacija čuva lične podatke samo onoliko dugo koliko je to neophodno radi ostvarivanja svrhe obrade, a u skladu sa zakonskim i podzakonskim propisima.

Komentar: Potrebno je definisati rokove u skladu sa objektivnim mogućnostima i važećim propisima.

8. KOME SE MOŽETE OBRATITI ZA VIŠE INFORMACIJA?

Za sva pitanja u vezi sa obradom ličnih podataka, kao i radi ostvarivanja prava koja Vam pripadaju, možete se obratiti **Službeniku za zaštitu ličnih podataka organizacije**:

- *Kontakt podaci*

Službenik za zaštitu ličnih podataka će odgovoriti na Vaš zahtjev **bez nepotrebnog odlaganja**, a najkasnije u roku od **30 dana** od dana prijema zahtjeva, u skladu sa zakonom.

Datum _____

Prilog 3

POLITIKA PRIVATNOSTI

1. UVOD I NAČELA

Ova Politika objašnjava kako organizacija (dalje: Kontrolor) prikuplja, koristi i štiti vaše lične podatke. Naša obrada temelji se na principima zakonitosti, transparentnosti, minimalnog obima podataka i sigurnosti.

2. KATEGORIJE PODATAKA I SVRHA

- Organizacija obrađuje podatke sljedećih lica:
- Zaposleni i saradnici;
- Kandidati za posao;
- Donatori i partneri;
- Korisnici i učesnici;
- Posjetioci.

Posebne kategorije podataka u pravilu se ne obrađju ili se obrađju uz izričitu saglasnost nosilaca podataka, te uz strogo poštovanje sigurnosnih mjera i zakonskih izuzetaka koji se odnose na rad neprofitnog sektora.

3. PRAVNI OSNOV OBRADJE

Podatke obrađujemo isključivo:

- Radi ispunjenja zakonskih obaveza;
- Radi izvršenja ugovora ili radnji prije zaključenja ugovora;
- Na osnovu vaše saglasnosti;
- Radi legitimnog interesa.

4. PRIMAOCI I PRIJENOS PODATAKA

Vaši podaci mogu biti ustupljeni samo:

- Nadležnim organima (Poreska uprava, sudovi) po zakonskom nalogu.
- Obradivačima s kojima postoji ugovor o povjerenj obradi podataka (računovodstvo, IT podrška).

Napomena: Podaci se u pravilu ne iznose iz BiH, osim uz primjenu zaštitnih mjera u skladu sa Zakonom.

5. ROKOVI ČUVANJA

Podaci se čuvaju samo onoliko koliko je potrebno za svrhu obrade:

Komentar: Definisati rokove

6. VAŠA PRAVA

Kao nosilac podataka imate pravo na:

- Pristup podacima i informacije o obradi
- Ispravku netačnih podataka
- Brisanje podataka ili ograničenje obrade
- Povlačenje saglasnosti
- Prenosivost
- Prigovor Agenciji za zaštitu ličnih podataka BiH
- Sudsku zaštitu

7. SIGURNOST I KONTAKT

Primjenjujemo tehničke i organizacione mjere (šifre, zaključavanje arhiva, obuka osoblja) kako bismo spriječili zloupotrebu.

Za sva pitanja obratite se našem Službeniku za zaštitu ličnih podataka: *Kontakt*

Prilog 4

SAGLASNOST ZA OBRADU LIČNIH PODATAKA

Ja, _____ (ime i prezime), rođen/a _____, dajem **dobrovoljnu, izričitu i informisanu saglasnost organizaciji** da obrađuje moje lične podatke u svrhu _____ (*upisati svrhu*).

Potvrđujem da sam **imao/la priliku upoznati se sa Obavještenjem o obradi ličnih podataka i Politikom privatnosti organizacije**, koji su dostupni u prostorijama organizacije i internet stranici, te da sam obaviješten/a o svojim pravima u vezi sa zaštitom ličnih podataka.

Upoznat/a sam sa činjenicom da u svakom trenutku mogu povući saglasnost, što neće uticati na zakonitost obrade izvršene prije povlačenja.

Datum _____

Potpis

Prilog 5

IZJAVA O POVJERLJIVOSTI I ČUVANJU LIČNIH PODATAKA

Ja, _____, zaposlen u organizaciji _____
na poziciji _____, obavezujem se da ću, u skladu sa važećim propisima
koji uređuju oblast zaštite ličnih podataka:

- a) **čuvati povjerljivost svih ličnih podataka kojima imam pravo i mogućnost pristupa**, a koji se nalaze u organizaciji, te da iste neću koristiti, obrađivati, saopštavati, niti prenositi trećim licima bez izričite saglasnosti ovlaštenog lica i nosioca podataka, osim kada to nalaže zakon
- b) **lične podatke do kojih dođem koristiti isključivo u svrhu za koju su prikupljeni**
- c) **da ću preduzeti sve razumne mjere kako bih spriječio/la neovlašten pristup podacima** (zaključavanje računara, čuvanje lozinki i fizičkih dokumenata na sigurnom).

Upoznat/a sam da bilo kakvo neovlašteno korištenje, otkrivanje ili dijeljenje ličnih i podataka predstavlja povredu radne obaveze i može imati posljedice u smislu pokretanja različitih disciplinskih, sudskih i upravnih postupaka.

Datum _____

Potpis _____

Prilog 6

Evidencije o obradi ličnih podataka utvrđena od strane Agencije za zaštitu ličnih podataka, te su dostupne na sljedećem linku:

https://azlp.ba/Provođenje_ZZLP/default.aspx?id=4834&langTag=bs-BA&template_id=149&pageIndex=1

Prilog 7

ODLUKA

O imenovanju službenika za zaštitu ličnih podataka

Član 1

_____, imenuje se za službenika za zaštitu ličnih podataka u *Organizaciji*

Kontakt podaci imenovanog službenika za zaštitu ličnih podataka su:

-Upisati-

Član 2

Službenik za zaštitu ličnih podataka ima status, zadatke i nadležnosti propisane odredbama članova 39 - 41. Zakona o zaštiti ličnih podataka („Službeni glasnik BiH“ broj: 12/25), te je sve podatke do kojih dođe dužan čuvati kao službenu tajnu.

Član 3

Ova Odluka stupa na snagu danom donošenja.

Datum _____
