Na osnovu Statuta KJP "ZOI'84" OCS d.o.o. Sarajevo, čl. 26, 27, 32, 34, 35, 36, 37, 39, 40. i 41. Zakona o zaštiti ličnih podataka ("Službeni glasnik BiH", broj 12/25), Nadzorni odbor KJP "ZOI'84" OCS d.o.o. Sarajevo, na sjednici održanoj dana 07.09.2026, donosi

# PRAVILNIK
# O ZAŠTITI LIČNIH PODATAKA

## DIO PRVI - OPĆE ODREDBE

### Član 1.
### (Predmet Pravilnika)

(1) Ovim pravilnikom uređuju se pravila, procedure i odgovornosti za zakonitu, pravičnu, transparentnu i sigurnu obradu ličnih podataka u KJP "ZOI'84" OCS d.o.o. Sarajevo (u daljem tekstu: Društvo).

(2) Pravilnikom se naročito uređuju: principi i pravni osnovi obrade, evidencija aktivnosti obrade, prava nosilaca podataka, uloga službenika za zaštitu ličnih podataka, davanje i otkrivanje ličnih podataka korisnicima, angažman obrađivača, prijenos podataka u druge države ili međunarodne organizacije, sigurnosne mjere, postupanje u slučaju povrede ličnih podataka, procjena uticaja na zaštitu ličnih podataka, čuvanje i brisanje podataka, te obaveza edukacije i nadzora nad primjenom ovog pravilnika.

(3) Ovaj pravilnik primjenjuje se na sve organizacione dijelove Društva, uključujući Zetra, ski-centar i druge poslovne objekte, službe, sektore, odjele, radne jedinice, komisije i druga radna tijela Društva, bez obzira na to da li se obrada vrši u papirnom, elektronskom, audio-vizuelnom ili drugom obliku.

### Član 2.
### (Značenje izraza)

(1) Izrazi upotrijebljeni u ovom pravilniku imaju značenje utvrđeno Zakonom o zaštiti ličnih podataka.

(2) Radi primjene ovog pravilnika, pojedini izrazi imaju sljedeće operativno značenje:

- **Društvo** je kontrolor podataka kada samo ili zajedno s drugim licem određuje svrhe i sredstva obrade ličnih podataka;
- **nosilac podataka** je svako fizičko lice čiji se lični podaci obrađuju, uključujući zaposlenog, kandidata za zaposlenje, člana organa Društva, korisnika usluga, posjetioca objekta, zakupca, dobavljača, predstavnika pravnog lica, podnosioca zahtjeva, učesnika postupka javne nabavke i drugo fizičko lice;
- **obrađivač** je pravno ili fizičko lice koje obrađuje lične podatke u ime Društva, na osnovu ugovora ili drugog pravnog akta;
- **primalac** je pravno ili fizičko lice, javni organ, agencija ili drugo tijelo kojem su lični podaci otkriveni;
- **povreda ličnih podataka** je povreda sigurnosti koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa ličnim podacima;
- **službenik za zaštitu ličnih podataka** je lice imenovano u skladu sa Zakonom koje savjetuje, prati usklađenost i djeluje kao kontakt-tačka za nosioce podataka i Agenciju za zaštitu ličnih podataka u BiH.

### Član 3.
### (Oblast primjene)

(1) Ovaj pravilnik primjenjuje se na automatiziranu obradu ličnih podataka, kao i na neautomatiziranu obradu ličnih podataka koji čine dio zbirke, evidencije, predmeta, registra, dosijea, baze podataka ili drugog uređenog skupa podataka.

(2) Ovaj pravilnik primjenjuje se i na obradu ličnih podataka putem videonadzora, sistema kontrole pristupa, elektronske pošte, informacionih sistema, aplikacija, web stranice, društvenih mreža kada njima upravlja Društvo, blagajničkog i finansijskog poslovanja, sistema prodaje karata/usluga, evidencija posjetilaca i drugih sistema koje koristi Društvo.

(3) Ovaj pravilnik ne isključuje primjenu posebnih zakona, podzakonskih propisa, kolektivnog ugovora, internih akata Društva i ugovornih obaveza, ako su oni relevantni za pojedinu obradu ličnih podataka. U slučaju nesaglasnosti, primjenjuje se pravilo koje osigurava viši nivo zaštite prava nosilaca podataka, osim kada je drukčije propisano zakonom.

**Član 4.**
**(Principi obrade)**

Društvo je dužno svaku obradu ličnih podataka zasnivati na sljedećim principima:

- zakonitost, pravičnost i transparentnost obrade;
- ograničenje svrhe - lični podaci prikupljaju se za posebne, izričite i zakonite svrhe i ne obrađuju se na način koji nije u skladu s tim svrhama;
- smanjenje obima podataka - obrađuju se samo podaci koji su primjereni, relevantni i neophodni za konkretnu svrhu;
- tačnost i ažurnost podataka;
- ograničenje čuvanja - podaci se čuvaju samo onoliko dugo koliko je potrebno za svrhu obrade ili koliko je propisano zakonom, listom kategorija registraturne i arhivske građe ili drugim obavezujućim aktom;
- cjelovitost i povjerljivost - podaci se štite od neovlaštene ili nezakonite obrade, slučajnog gubitka, uništenja ili oštećenja;
- pouzdanost - Društvo mora biti u mogućnosti dokazati usklađenost obrade sa Zakonom i ovim pravilnikom.

**Član 5.**
**(Pravni osnov obrade)**

(1) Obrada ličnih podataka u Društvu dopuštena je samo ako postoji valjan pravni osnov, uključujući naročito:

- poštovanje pravne obaveze Društva kao poslodavca, javnog preduzeća, ugovornog organa, računovodstvenog i poreskog obveznika;
- izvršenje ugovora ili preduzimanje radnji prije zaključenja ugovora, kada je nosilac podataka ugovorna strana ili nastupa kao zastupnik, punomoćnik, kontakt osoba ili korisnik usluge;
- izvršenje zadatka od javnog interesa ili zadatka koji proizlazi iz posebnog statusa Društva kao kantonalnog javnog preduzeća, kada je takva obrada propisana ili potrebna u skladu sa zakonom;
- zaštita ključnih interesa nosioca podataka ili drugog fizičkog lica, posebno u hitnim situacijama, povredama, nesrećama ili sigurnosnim incidentima;
- legitimni interes Društva ili treće strane, kada je primjenjiv i kada nad njim ne pretežu interesi ili osnovna prava i slobode nosioca podataka;
- saglasnost nosioca podataka, kada ne postoji drugi odgovarajući pravni osnov i kada je saglasnost data slobodno, posebno, informirano i nedvosmisleno.

(2) Saglasnost se ne smije koristiti kao primarni pravni osnov u situacijama u kojima je obrada potrebna radi izvršenja zakonske obaveze, ugovora, radnopravnog odnosa, javne nabavke ili drugog odnosa u kojem nosilac podataka realno nema slobodu da odbije obradu bez posljedica po ostvarivanje prava ili usluge.

(3) Svaka organizaciona jedinica koja pokreće novu obradu dužna je prije početka obrade utvrditi i dokumentovati pravni osnov, svrhu, kategorije podataka, rok čuvanja, primaoce i sigurnosne mjere.

DIO DRUGI - ULOGE I ODGOVORNOSTI

**Član 6.**
**(Društvo kao kontrolor podataka)**

(1) Društvo je kontrolor podataka za obrade ličnih podataka koje obavlja u okviru svoje registrovane djelatnosti, radnopravnih odnosa, javnih nabavki, finansijsko-računovodstvenog poslovanja, pružanja usluga, upravljanja objektima i imovinom, sigurnosti, videonadzora, arhivskog i kancelarijskog poslovanja, pravnih postupaka i drugih zakonitih poslovnih procesa.

(2) Kao kontrolor, Društvo je dužno:

- utvrditi svrhu i pravni osnov obrade prije početka obrade;
- voditi i ažurirati evidenciju aktivnosti obrade;
- osigurati transparentne informacije nosiocima podataka;
- omogućiti ostvarivanje prava nosilaca podataka;
- primijeniti odgovarajuće tehničke i organizacione mjere zaštite;
- osigurati da zaposleni i angažovana lica podatke obrađuju samo po ovlaštenju i uputstvu Društva;
- urediti odnos s obrađivačima pisanim ugovorom ili drugim pravnim aktom;
- dokumentovati usklađenost i sarađivati sa Agencijom za zaštitu ličnih podataka u BiH.

**Član 7.**
**(Službenik za zaštitu ličnih podataka)**

(1) Društvo imenuje službenika za zaštitu ličnih podataka posebnom odlukom, u skladu sa Zakonom.

(2) Kontakt-podaci službenika za zaštitu ličnih podataka objavljuju se na službenoj web stranici Društva, na oglasnoj ploči ili drugom lako dostupnom mjestu, te se dostavljaju Agenciji za zaštitu ličnih podataka u BiH.

(3) Službenik za zaštitu ličnih podataka neposredno odgovara najvišem nivou rukovodstva Društva, ne prima instrukcije u pogledu obavljanja svojih zakonskih zadataka i ne može biti razriješen, kažnjen ili doveden u nepovoljniji položaj zbog zakonitog obavljanja tih zadataka.

(4) Službenik za zaštitu ličnih podataka naročito:

- informiše i savjetuje organe Društva, rukovodioce i zaposlene o obavezama u oblasti zaštite ličnih podataka;
- prati usklađenost obrade sa Zakonom, ovim pravilnikom i drugim internim aktima;
- učestvuje u izradi i ažuriranju evidencije aktivnosti obrade;
- daje mišljenje o novim obradama, posebno o obradama koje mogu predstavljati visok rizik;
- daje savjet i prati provođenje procjene uticaja na zaštitu ličnih podataka;
- sarađuje sa Agencijom i djeluje kao kontakt-tačka za Agenciju i nosioce podataka;
- predlaže edukacije zaposlenih i interne provjere usklađenosti;
- vodi ili koordinira evidencije propisane ovim pravilnikom, ako posebnom odlukom nije drugačije određeno.

(5) Službenik za zaštitu ličnih podataka ne smije biti u sukobu interesa. Prije imenovanja i tokom obavljanja dužnosti provjerava se da li druge dužnosti tog lica uključuju određivanje svrha i sredstava obrade ličnih podataka na način koji bi ugrozio njegovu nezavisnost.

**Član 8.**
**(Rukovodioci organizacionih jedinica)**

(1) Rukovodioci sektora, službi, odjela, radnih jedinica i drugih organizacionih dijelova odgovorni su za zakonitu obradu ličnih podataka u procesima kojima rukovode.

(2) Rukovodilac organizacione jedinice dužan je naročito:

- identifikovati obrade ličnih podataka u svojoj nadležnosti i dostaviti podatke službeniku za zaštitu ličnih podataka radi evidencije aktivnosti obrade;
- osigurati da pristup podacima imaju samo ovlaštena lica kojima je pristup potreban za rad;
- obavijestiti službenika za zaštitu ličnih podataka o namjeri uvođenja nove aplikacije, evidencije, obrasca, videonadzora, online usluge ili drugog sistema koji uključuje lične podatke;
- bez odgađanja prijaviti svaku sumnju na povredu ličnih podataka;
- provoditi preporuke službenika za zaštitu ličnih podataka i mjere iz Plana sigurnosti.

**Član 9.**

**(Zaposleni, članovi organa i angažovana lica)**

(1) Zaposleni, članovi organa Društva, članovi komisija, lica angažovana po ugovoru i druga lica koja u okviru rada ili angažmana imaju pristup ličnim podacima smiju obrađivati lične podatke samo u granicama ovlaštenja, dodijeljenih poslova i uputstava Društva.

(2) Lica iz stava (1) ovog člana dužna su čuvati povjerljivost ličnih podataka tokom i nakon prestanka radnog odnosa, mandata ili angažmana.

(3) Svako lice iz stava (1) ovog člana potpisuje izjavu o povjerljivosti ili se obaveza povjerljivosti ugrađuje u ugovor, rješenje, odluku o imenovanju ili drugi pravni akt.

**Član 10.**

**(Obrađivači i druga treća lica)**

(1) Kada Društvo povjeri obradu ličnih podataka obrađivaču, takav odnos mora biti uređen pisanim ugovorom ili drugim pravnim aktom, uključujući elektronsku formu, kojim se naročito uređuju predmet i trajanje obrade, priroda i svrha obrade, vrsta ličnih podataka, kategorije nosilaca podataka, obaveze i prava Društva, obaveza povjerljivosti, sigurnosne mjere, podobrađivači, pomoć u ostvarivanju prava nosilaca podataka, postupanje po povredi ličnih podataka, vraćanje ili brisanje podataka po prestanku usluge i pravo kontrole.

(2) Bez prethodne provjere i ugovornog uređenja nije dopušteno davati lične podatke subjektima koji pružaju IT usluge, hosting, cloud usluge, video-nadzorne usluge, fizičko-tehničku zaštitu, računovodstvene, pravne, revizorske, marketinške, konsultantske, zdravstvene ili druge usluge koje uključuju obradu ličnih podataka u ime Društva.

(3) Organizacione jedinice ne smiju samostalno uvoditi aplikacije, online servise, platforme ili vanjske alate koji uključuju lične podatke bez prethodnog mišljenja službenika za zaštitu ličnih podataka i saglasnosti ovlaštenog lica Društva.

## DIO TREĆI - AKTIVNOSTI OBRADE I POSEBNA PRAVILA

**Član 11.**

**(Evidencija aktivnosti obrade)**

(1) Društvo vodi evidenciju aktivnosti obrade za koje je odgovorno kao kontrolor podataka.

(2) Evidencija aktivnosti obrade vodi se u pisanom i/ili elektronskom obliku i sadrži najmanje: naziv i kontakt-podatke Društva, kontakt-podatke službenika za zaštitu ličnih podataka, svrhe obrade, kategorije nosilaca podataka, kategorije ličnih podataka, kategorije primalaca, podatke o prijenosu u drugu državu ili međunarodnu organizaciju ako je primjenjivo, predviđene rokove brisanja i opći opis tehničkih i organizacionih mjera.

(3) Evidencija iz stava (1) ovog člana ažurira se bez odgađanja po svakoj promjeni svrhe, pravnog osnova, kategorija podataka, korisnika, sistema obrade, obrađivača, roka čuvanja ili sigurnosnih mjera.

(4) Službenik za zaštitu ličnih podataka koordinira vođenje evidencije, a rukovodioci organizacionih jedinica odgovorni su za tačnost i potpunost podataka za obrade u svojoj nadležnosti.

**Član 12.**

**(Tipične aktivnosti obrade u Društvu)**

(1) Društvo naročito vodi ili može voditi sljedeće aktivnosti obrade, zavisno od stvarnih poslovnih procesa:

- evidencije zaposlenih, radnih odnosa, ugovora o radu, aneksa, rješenja, odsustava, godišnjih odmora, disciplinskih postupaka i prestanka radnog odnosa;
- evidencije kandidata za zaposlenje, konkursne dokumentacije, intervjua, testiranja i izbora kandidata;
- obračun plaća, naknada, poreza, doprinosa, putnih naloga, komisija, ugovora o djelu i drugih isplata;
- evidencije članova Skupštine, Nadzornog odbora, Odbora za reviziju, Uprave, komisija i drugih organa ili radnih tijela;
- evidencije iz oblasti zaštite na radu, osposobljavanja, ljekarskih pregleda, povreda na radu i sigurnosnih procedura;
- evidencije ugovora, zakupaca, korisnika poslovnih prostora, dobavljača, kontakt osoba i lica ovlaštenih za zastupanje;
- evidencije javnih nabavki, ponuđača, podugovarača, članova komisija, žalbi i komunikacije sa nadležnim organima;
- evidencije korisnika usluga Društva, uključujući kupce karata, sezonskih i drugih propusnica, učesnike sportskih i turističkih programa, škole skijanja, reklamacije, zahtjeve za povrat, rezervacije i korisničku podršku;
- evidencije posjetilaca, ulazaka u objekte, akreditacija, dozvola i drugih pristupnih ovlaštenja;
- videonadzor objekata, pristupnih prostora, skijaških kapaciteta, garaža, parkinga, službenih ulaza i drugih prostora u kojima se provodi zaštita lica i imovine;
- evidencije incidenata, nesreća, povreda posjetilaca, izgubljenih stvari, šteta, potraživanja i osiguranja;
- finansijsko-računovodstvene evidencije, blagajničko poslovanje, fakture, naplata, potraživanja, opomene i izvršni/sudski postupci;
- evidencije zahtjeva za pristup informacijama, predstavki, pritužbi, dopisa, zahtjeva organa vlasti i službene korespondencije;
- evidencije IT naloga, elektronske pošte, dodjele opreme, logova pristupa i informaciono-sigurnosnih događaja;
- web stranica, kontakt forme, newsletter ili drugi oblici elektronske komunikacije, samo ako ih Društvo stvarno koristi i ako je pravni osnov dokumentovan;
- arhivska i kancelarijska evidencija, protokol, interne dostavne knjige i registraturna građa.

(2) Spisak iz stava (1) ovog člana ne predstavlja zatvorenu listu. Svaka stvarna obrada mora biti posebno opisana u evidenciji aktivnosti obrade.

**Član 13.**

**(Posebne kategorije ličnih podataka, JMB i podaci o krivičnoj osuđivanosti)**

(1) Posebne kategorije ličnih podataka, uključujući podatke koji se odnose na zdravlje, biometrijske podatke, podatke o sindikalnom članstvu ili druge posebno zaštićene podatke, obrađuju se samo kada za to postoji izričit zakonski osnov ili drugi dopušten osnov propisan Zakonom, uz pojačane mjere zaštite.

(2) Jedinstveni matični broj, broj lične karte, broj pasoša, broj bankovnog računa i drugi identifikatori obrađuju se samo kada su neophodni za tačno utvrđenu svrhu i kada je obrada propisana ili potrebna radi izvršenja zakonske, ugovorne ili druge zakonite obaveze.

(3) Podaci o krivičnoj osuđivanosti ili prekršajima obrađuju se samo kada je takva obrada propisana posebnim zakonom, potrebna u postupku koji se vodi pred nadležnim organom ili kada je nužna radi zaštite pravnog položaja Društva, uz primjenu posebnih zaštitnih mjera i ograničen pristup.

(4) Dokumentacija koja sadrži podatke iz ovog člana ne smije se kopirati, skenirati, slati elektronskom poštom ili čuvati na zajedničkim lokacijama bez jasne poslovne potrebe i odgovarajućih mjera zaštite.

**Član 14.**
**(Videonadzor)**

(1) Videonadzor se može koristiti radi zaštite lica, imovine, sigurnosti objekata, kontrole ulaza i izlaza, sprečavanja i dokumentovanja incidenata, zaštite skijaške i sportske infrastrukture, te drugih zakonitih sigurnosnih svrha.

(2) Videonadzor se ne smije koristiti za svrhe koje nisu unaprijed određene i dokumentovane, niti za neopravdano praćenje rada zaposlenih, osim ako je takva obrada nužna, proporcionalna i zasnovana na zakonu ili drugom valjanom osnovu.

(3) Prostori pod videonadzorom moraju biti jasno označeni obavještenjem koje najmanje sadrži informaciju da se prostor snima, naziv kontrolora, svrhu snimanja, kontakt službenika za zaštitu ličnih podataka i način ostvarivanja prava nosilaca podataka.

(4) Kamere se postavljaju tako da se snima samo prostor potreban za ostvarenje legitimne i zakonite svrhe. Nije dopušteno postavljanje kamera u sanitarnim prostorijama, garderobama, prostorima za presvlačenje, prostorima za odmor zaposlenih ili drugim prostorima gdje bi snimanje bilo nesrazmjerno svrsi.

(5) Pristup snimcima imaju samo ovlaštena lica. Svaki pristup, pregled, izvoz, kopiranje ili davanje snimka dokumentuje se u evidenciji pristupa snimcima.

(6) Rok čuvanja snimaka određuje se u evidenciji aktivnosti obrade i Planu sigurnosti, u pravilu najkraće koliko je potrebno za sigurnosnu svrhu, osim kada je snimak izdvojen radi incidenta, zahtjeva nadležnog organa, sudskog, upravnog, prekršajnog ili drugog postupka.

**Član 15.**
**(Obrada u kontekstu zaposlenja)**

(1) Lični podaci zaposlenih i kandidata za zaposlenje obrađuju se radi zasnivanja i izvršavanja radnog odnosa, ispunjavanja zakonskih obaveza poslodavca, obračuna plaća i naknada, vođenja kadrovske evidencije, zaštite na radu, organizacije rada, edukacije, disciplinskih i drugih postupaka, zaštite imovine i ostvarivanja prava i obaveza iz radnog odnosa.

(2) Od kandidata za zaposlenje mogu se tražiti samo podaci i dokumenti koji su relevantni za uslove radnog mjesta, konkursnu proceduru i zakonske obaveze. Dokumentacija kandidata koji nije izabran čuva se u roku određenom zakonom, internim aktom ili rokovima pravne zaštite, a nakon toga se briše, vraća ili arhivira u skladu sa propisima.

(3) Pristup personalnim dosijeima zaposlenih imaju samo lica ovlaštena za kadrovske, pravne, finansijske, revizorske, rukovodne ili druge zakonite poslove u mjeri u kojoj je pristup neophodan.

(4) Podaci o zdravlju zaposlenih, ljekarskim uvjerenjima, povredama na radu i invaliditetu obrađuju se uz pojačane mjere zaštite i samo u obimu potrebnom za izvršenje obaveza iz radnog odnosa, zaštite na radu, socijalnog osiguranja i drugih zakonom propisanih obaveza.

**Član 16.**

**(Javne nabavke, ugovori i transparentnost)**

(1) Lični podaci u postupcima javnih nabavki obrađuju se radi provođenja postupka, provjere ispunjenosti uslova, evaluacije ponuda, zaključenja i izvršenja ugovora, objave podataka propisanih zakonom i zaštite prava učesnika postupka.

(2) Kod objave odluka, izvještaja, ugovora, planova nabavki, zapisnika i drugih dokumenata, organizaciona jedinica koja priprema objavu dužna je provjeriti da li dokument sadrži lične podatke koji nisu nužni za objavu. Podaci koji nisu neophodni anonimiziraju se ili pseudonimiziraju, osim ako poseban zakon nalaže objavu.

(3) Ugovori sa dobavljačima, zakupcima, korisnicima prostora i drugim partnerima smiju sadržavati samo one lične podatke koji su potrebni za identifikaciju ugovornih strana, kontakt, izvršenje ugovora, naplatu, zaštitu prava i ispunjenje zakonskih obaveza.

**Član 17.**

**(Sloboda pristupa informacijama i javni interes)**

(1) Prilikom postupanja po zahtjevima za pristup informacijama, Društvo usklađuje pravo javnosti na pristup informacijama s pravom na zaštitu ličnih podataka.

(2) Lični podaci se u odgovoru na zahtjev za pristup informacijama otkrivaju samo kada za to postoji zakonski osnov, pretežan javni interes ili drugi zakonit razlog. U suprotnom, dokument se dostavlja uz anonimizaciju podataka koji nisu nužni za svrhu pristupa informaciji.

(3) Prije dostavljanja dokumenata koji sadrže lične podatke većeg broja lica, posebne kategorije podataka, podatke djece, JMB ili podatke o zdravlju, obavezno se pribavlja mišljenje službenika za zaštitu ličnih podataka.

## DIO ČETVRTI - PRAVA NOSILACA PODATAKA

**Član 18.**

**(Transparentnost i obavještenja o obradi)**

(1) Društvo nosiocima podataka pruža informacije o obradi u sažetoj, transparentnoj, razumljivoj i lako dostupnoj formi, uz upotrebu jasnog jezika.

(2) Informacije se mogu pružiti putem obavještenja o privatnosti na web stranici, obrasca, ugovora, konkursne dokumentacije, obavještenja na lokaciji, obavještenja uz videonadzor, interne obavijesti zaposlenima ili drugim odgovarajućim putem.

(3) Obavještenje o obradi, kada je primjenjivo, sadrži: identitet i kontakt Društva, kontakt službenika za zaštitu ličnih podataka, svrhu i pravni osnov obrade, kategorije podataka, primaoce, rok čuvanja, informaciju o prijenosu u drugu državu ili međunarodnu organizaciju, prava nosioca podataka, pravo na prigovor Agenciji, te informaciju da li je davanje podataka zakonska ili ugovorna obaveza i posljedice nedavanja podataka.

**Član 19.**

**(Prava nosilaca podataka)**

(1) Nosilac podataka ima pravo, pod uslovima propisanim Zakonom, zahtijevati:

- informacije o obradi njegovih ličnih podataka;
- pristup ličnim podacima;
- ispravku netačnih i dopunu nepotpunih ličnih podataka;
- brisanje ličnih podataka;
- ograničenje obrade;
- prenosivost podataka, kada je primjenjivo;
- prigovor na obradu, kada je primjenjivo;

- da se na njega ne primjenjuje odluka zasnovana isključivo na automatiziranoj obradi, uključujući profiliranje, ako takva odluka proizvodi pravni učinak ili na sličan način značajno utiče na njega.

(2) Prava iz stava (1) ovog člana ostvaruju se u skladu sa Zakonom, pri čemu se uzimaju u obzir zakonske obaveze čuvanja podataka, prava i slobode drugih lica, zaštita pravnog položaja Društva, javni interes, sigurnost i drugi zakonom dopušteni razlozi ograničenja.

**Član 20.**

**(Postupak po zahtjevu nosioca podataka)**

(1) Zahtjev nosioca podataka podnosi se pisanim putem, elektronskom poštom, putem protokola, neposredno službeniku za zaštitu ličnih podataka ili drugim kanalom koji Društvo učini dostupnim.

(2) Prije postupanja po zahtjevu, Društvo može zatražiti dodatne informacije potrebne za potvrdu identiteta podnosioca zahtjeva, ako postoji razumna sumnja u identitet.

(3) Društvo nosiocu podataka pruža informacije o preduzetim radnjama bez nepotrebnog odgađanja, a najkasnije u roku od 30 dana od dana zaprimanja zahtjeva. Rok se može produžiti za dodatnih 60 dana kada je to potrebno zbog složenosti ili broja zahtjeva, o čemu se nosilac podataka obavještava u roku od 30 dana od zaprimanja zahtjeva, uz navođenje razloga produženja.

(4) Ako Društvo ne postupi po zahtjevu, nosioca podataka bez odgađanja, a najkasnije u roku od 30 dana od zaprimanja zahtjeva, obavještava o razlozima nepostupanja i o mogućnosti podnošenja prigovora Agenciji za zaštitu ličnih podataka u BiH ili korištenja drugog pravnog sredstva.

(5) Postupanje po zahtjevu nosioca podataka u pravilu je besplatno. Ako su zahtjevi očigledno neosnovani ili pretjerani, posebno zbog učestalog ponavljanja, Društvo može postupiti u skladu sa Zakonom.

**Član 21.**

**(Evidencija zahtjeva nosilaca podataka)**

(1) Društvo vodi evidenciju zahtjeva nosilaca podataka, koja sadrži: datum prijema zahtjeva, podatke o podnosiocu, vrstu zahtjeva, organizacionu jedinicu na koju se zahtjev odnosi, rok za odgovor, preduzete radnje, datum odgovora, odluku o zahtjevu i napomenu o eventualnom prigovoru ili pravnom sredstvu.

(2) Evidenciju vodi službenik za zaštitu ličnih podataka ili drugo lice određeno posebnom odlukom, uz obavezu redovne koordinacije sa službenikom za zaštitu ličnih podataka.

**Član 22.**

**(Prigovor Agenciji i sudska zaštita)**

Ako nosilac podataka smatra da je Društvo povrijedilo njegovo pravo u vezi s obradom ličnih podataka, može se obratiti službeniku za zaštitu ličnih podataka, podnijeti prigovor Agenciji za zaštitu ličnih podataka u BiH ili koristiti druga pravna sredstva u skladu sa Zakonom.

## DIO PETI - DAVANJE, OTKRIVANJE I PRIJENOS LIČNIH PODATAKA

**Član 23.**

**(Davanje podataka korisnicima i javnim organima)**

(1) Lični podaci mogu se dati korisniku, javnom organu ili trećem licu samo ako postoji valjan pravni osnov i ako je davanje podataka ograničeno na podatke koji su neophodni za zakonitu svrhu.

(2) Zahtjev javnog organa za dostavljanje ličnih podataka mora biti u pisanom obliku, obrazložen i zasnovan na zakonu, osim u hitnim situacijama kada se pisani trag osigurava naknadno bez odgađanja.

(3) Prije dostavljanja podataka provjerava se identitet i nadležnost tražioca, pravni osnov, svrha, kategorije traženih podataka i proporcionalnost obima podataka.

(4) O svakom davanju ličnih podataka vodi se evidencija koja sadrži najmanje: datum davanja, korisnika, pravni osnov, svrhu, kategorije podataka, kategorije nosilaca podataka, način dostavljanja, lice koje je odobrilo davanje i napomenu o pratećoj dokumentaciji.

**Član 24.**
**(Objavljivanje podataka)**

(1) Objavljivanje ličnih podataka na web stranici, oglasnoj ploči, društvenim mrežama, u izvještajima, saopštenjima, javnim pozivima, odlukama, zapisnicima ili drugim dokumentima dopušteno je samo ako je propisano zakonom, potrebno radi transparentnosti javnog preduzeća, izvršenja ugovora ili drugog zakonitog cilja, i ako je obim objavljenih podataka sveden na neophodnu mjeru.

(2) Prije objave dokumenata primjenjuje se pravilo prethodne provjere: uklanjaju se ili zatamnjuju JMB, adrese stanovanja, brojevi ličnih dokumenata, potpisi, brojevi bankovnih računa, kontakt telefoni privatnih lica, podaci o zdravlju i drugi podaci koji nisu nužni za svrhu objave.

(3) Za fotografije i video materijale sa događaja Društva procjenjuje se pravni osnov objave. Kada se obrada zasniva na saglasnosti, saglasnost mora biti dokumentovana i povlačiva, bez negativnih posljedica za nosioca podataka kada je to primjenjivo.

**Član 25.**
**(Prijenos podataka u drugu državu ili međunarodnu organizaciju)**

(1) Prijenos ličnih podataka u drugu državu ili međunarodnu organizaciju dopušten je samo pod uslovima propisanim Zakonom.

(2) Prije korištenja cloud servisa, aplikacija, hosting usluga, platformi za e-mail, online obrazaca, analitike, newslettera ili drugih servisa kod kojih postoji mogućnost prijenosa podataka van Bosne i Hercegovine, obavezno se pribavlja mišljenje službenika za zaštitu ličnih podataka i provjerava postojanje odgovarajućeg mehanizma prijenosa.

(3) O prijenosu iz stava (1) ovog člana vodi se dokumentacija u evidenciji aktivnosti obrade, uključujući državu ili međunarodnu organizaciju, kategorije podataka, pravni osnov prijenosa i odgovarajuće zaštitne mjere.

## DIO ŠESTI - SIGURNOST, POVREDE PODATAKA I PROCJENA UTICAJA

**Član 26.**
**(Tehničke i organizacione mjere)**

(1) Društvo primjenjuje tehničke i organizacione mjere kojima se osigurava odgovarajući nivo sigurnosti s obzirom na rizik, uključujući naročito:

- kontrolu fizičkog pristupa prostorijama i arhivi;
- kontrolu korisničkih naloga i ovlaštenja u informacionim sistemima;
- princip najmanjih privilegija - pristup samo podacima potrebnim za konkretan posao;
- zaštitu lozinki, dvofaktorsku autentifikaciju gdje je primjenjivo i zabranu dijeljenja korisničkih naloga;
- redovno pravljenje sigurnosnih kopija i provjeru mogućnosti obnove podataka;
- zaštitu računara, servera i mreže od zlonamjernog softvera i neovlaštenog pristupa;
- enkripciju ili druge mjere zaštite podataka na prenosivim medijima i uređajima kada je primjenjivo;
- evidentiranje pristupa i promjena u sistemima kada je tehnički moguće;
- sigurno uništavanje papirne i elektronske dokumentacije po isteku rokova čuvanja;
- edukaciju zaposlenih i provjeru poštivanja ovog pravilnika.

(2) Mjere se razrađuju Planom sigurnosti ličnih podataka, IT sigurnosnim procedurama, pravilima arhivskog i kancelarijskog poslovanja, ugovorima sa obrađivačima i drugim internim aktima Društva.

**Član 27.**

**(Plan sigurnosti ličnih podataka)**

(1) Društvo donosi Plan sigurnosti ličnih podataka kao poseban akt ili kao prilog ovom pravilniku.

(2) Plan sigurnosti sadrži najmanje: opis sistema i lokacija obrade, klasifikaciju podataka, ovlaštenja pristupa, fizičke mjere zaštite, IT mjere zaštite, pravila sigurnosnih kopija, pravila korištenja prenosivih uređaja i medija, postupak sigurnog slanja podataka, mjere zaštite papirne dokumentacije, postupak uništavanja dokumentacije, način evidentiranja incidenata i plan oporavka nakon incidenta.

(3) Adekvatnost tehničkih i organizacionih mjera preispituje se najmanje jednom godišnje, kao i nakon većeg sigurnosnog incidenta, uvođenja novog sistema obrade ili značajne promjene poslovnog procesa.

**Član 28.**

**(Pravila pristupa i povjerljivosti)**

(1) Pristup ličnim podacima dodjeljuje se pojedinačno, na osnovu radnog mjesta, zadatka, mandata ili konkretnog ovlaštenja.

(2) Rukovodilac organizacione jedinice predlaže dodjelu, izmjenu ili ukidanje pristupa, a IT ili druga nadležna služba provodi tehničku dodjelu pristupa po odobrenju ovlaštenog lica.

(3) Po prestanku radnog odnosa, mandata, angažmana ili potrebe za pristupom, pristup se ukida bez odgađanja.

(4) Zabranjeno je slanje ličnih podataka na privatne e-mail adrese, čuvanje poslovnih ličnih podataka na privatnim uređajima bez odobrenja, neovlašteno fotografisanje dokumenata, dijeljenje lozinki, ostavljanje dokumentacije bez nadzora i iznošenje dokumentacije iz prostorija Društva bez odobrenja.

**Član 29.**

**(Povreda ličnih podataka)**

(1) Svaki zaposleni ili angažovano lice dužno je odmah, a najkasnije istog radnog dana po saznanju, prijaviti službeniku za zaštitu ličnih podataka i neposrednom rukovodiocu svaku stvarnu ili sumnjivu povredu ličnih podataka.

(2) Povredom ličnih podataka smatra se naročito: gubitak dokumentacije, slanje podataka pogrešnom primaocu, neovlašten pristup sistemu, gubitak laptopa ili USB uređaja, krađa dokumentacije, objava podataka bez osnova, ransomware ili drugi cyber incident, neovlašteno preuzimanje snimka videonadzora, uništenje ili izmjena podataka i svaki drugi događaj koji može ugroziti povjerljivost, cjelovitost ili dostupnost ličnih podataka.

(3) Službenik za zaštitu ličnih podataka, u saradnji sa odgovornom organizacionom jedinicom, IT službom i rukovodstvom, bez odgađanja procjenjuje prirodu povrede, kategorije i broj nosilaca podataka, moguće posljedice, rizik za prava i slobode fizičkih lica i mjere za ublažavanje posljedica.

(4) Ako je vjerovatno da povreda može ugroziti prava i slobode fizičkih lica, Društvo obavještava Agenciju za zaštitu ličnih podataka u BiH bez nepotrebnog odgađanja, a ako je moguće najkasnije u roku od 72 sata od saznanja za povredu. Ako obavještavanje nije izvršeno u roku od 72 sata, navode se razlozi kašnjenja.

(5) Ako je vjerovatno da će povreda uzrokovati visok rizik za prava i slobode fizičkih lica, Društvo bez odgađanja obavještava nosioce podataka jasnim i jednostavnim jezikom, osim u slučajevima kada Zakon dopušta izuzetak.

(6) Društvo dokumentuje svaku povredu ličnih podataka, uključujući činjenice, posljedice, odluku o obavještavanju ili neobavještavanju Agencije i nosilaca podataka, kao i preduzete mjere.

**Član 30.**

**(Procjena uticaja na zaštitu ličnih podataka)**

(1) Prije uvođenja obrade koja zbog prirode, obima, konteksta ili svrhe može uzrokovati visok rizik za prava i slobode fizičkih lica, Društvo provodi procjenu uticaja na zaštitu ličnih podataka.

(2) Procjena uticaja je obavezna naročito kada se uvodi: sistemsko i obimno praćenje javno dostupnih područja, nova ili proširena mreža videonadzora, sistem kontrole pristupa s naprednom identifikacijom, obimna obrada posebnih kategorija podataka, automatizirano odlučivanje ili profiliranje, veća online platforma za korisnike usluga ili druga obrada koja prema procjeni može predstavljati visok rizik.

(3) Procjena uticaja sadrži najmanje: opis obrade i svrhe, pravni osnov, procjenu nužnosti i proporcionalnosti, procjenu rizika za nosioce podataka, mjere za smanjenje rizika i mišljenje službenika za zaštitu ličnih podataka.

(4) Ako procjena uticaja pokaže da bi obrada, bez dodatnih mjera, uzrokovala visok rizik koji Društvo ne može odgovarajuće umanjiti, Društvo se prije početka obrade savjetuje s Agencijom za zaštitu ličnih podataka u BiH.

**Član 31.**

**(Edukacija i provjera usklađenosti)**

(1) Društvo osigurava periodičnu edukaciju zaposlenih koji obrađuju lične podatke, posebno lica u kadrovskim, pravnim, finansijskim, IT, komercijalnim, sigurnosnim, javnonabavnim, arhivskim i korisničkim poslovima.

(2) Službenik za zaštitu ličnih podataka predlaže godišnji plan edukacije i interne provjere usklađenosti.

(3) Interna provjera može obuhvatiti pregled evidencije aktivnosti obrade, ugovora s obrađivačima, videonadzora, pristupnih ovlaštenja, zahtjeva nosilaca podataka, objava na web stranici, rokova čuvanja i postupanja po incidentima.

## DIO SEDMI - ROKOVI ČUVANJA, ARHIVIRANJE I BRISANJE

**Član 32.**

**(Rokovi čuvanja)**

(1) Lični podaci čuvaju se samo onoliko dugo koliko je potrebno za svrhu obrade, odnosno u rokovima propisanim zakonom, listom kategorija registraturne i arhivske građe s rokovima čuvanja, ugovorom, pravosnažnim aktom, pravilima računovodstvenog i poreskog čuvanja ili drugim obavezujućim aktom.

(2) Rokovi čuvanja po pojedinim aktivnostima obrade unose se u evidenciju aktivnosti obrade.

(3) Ako za određenu kategoriju podataka nije propisan rok čuvanja, rukovodilac organizacione jedinice, uz mišljenje službenika za zaštitu ličnih podataka i lica zaduženog za arhivsko poslovanje, predlaže najkraći razuman rok čuvanja uzimajući u obzir svrhu obrade, rokove zastare, zakonske obaveze i rizik za nosioce podataka.

**Član 33.**

**(Brisanje, anonimizacija i uništavanje)**

(1) Po isteku roka čuvanja, lični podaci se brišu, anonimiziraju ili uništavaju na siguran način, osim ako postoji zakonski osnov za daljnje čuvanje.

(2) Uništavanje papirne dokumentacije vrši se na način koji onemogućava rekonstrukciju podataka, uz zapisnik kada se radi o dokumentaciji koja sadrži veći obim ličnih podataka, posebne kategorije podataka ili podatke od veće povjerljivosti.

(3) Brisanje elektronskih podataka provodi se tako da podaci više nisu dostupni u operativnim sistemima, uzimajući u obzir sigurnosne kopije i tehničke mogućnosti sistema. Kada trenutno brisanje iz sigurnosnih kopija nije tehnički izvodljivo, pristup se ograničava, a podaci se brišu u redovnom ciklusu obnove sigurnosnih kopija.

## DIO OSMI - ZAVRŠNE ODREDBE

**Član 34.**

**(Odnos prema drugim aktima)**

(1) Odredbe ovog pravilnika primjenjuju se zajedno sa Statutom Društva, pravilnikom o radu, pravilnikom o unutrašnjoj organizaciji i sistematizaciji, pravilnikom o kancelarijskom i arhivskom poslovanju, pravilnikom o javnim nabavkama, pravilnikom o IT sigurnosti ako je donesen, pravilima videonadzora, pravilima korištenja službenih uređaja i drugim internim aktima.

(2) Ako drugi interni akt sadrži odredbe koje nisu usklađene s ovim pravilnikom ili Zakonom, pokrenut će se postupak usklađivanja tog akta.

**Član 35.**
**(Obrasci i prilozi)**

(1) Sastavni dio ovog pravilnika čine sljedeći obrasci i prilozi:

- Prilog 1 - Obrazac evidencije aktivnosti obrade;
- Prilog 2 - Obrazac zahtjeva nosioca podataka;
- Prilog 3 - Evidencija zahtjeva nosilaca podataka;
- Prilog 4 - Evidencija davanja/otkrivanja ličnih podataka;
- Prilog 5 - Obrazac prijave i evidencije povrede ličnih podataka;
- Prilog 6 - Kontrolna lista za procjenu potrebe provođenja procjene uticaja;
- Prilog 7 - Izjava o povjerljivosti.

(2) Obrasci se mogu tehnički prilagođavati bez izmjene ovog pravilnika, ako se time ne smanjuje nivo zaštite ličnih podataka i ako ostaju očuvani elementi propisani Zakonom i ovim pravilnikom.

**Član 36.**
**(Odgovornost za primjenu)**

(1) Za primjenu ovog pravilnika odgovorni su Uprava/Direktor, rukovodioci organizacionih jedinica, službenik za zaštitu ličnih podataka, zaposleni i druga angažovana lica, svako u okviru svojih ovlaštenja i odgovornosti.

(2) Povreda odredbi ovog pravilnika može predstavljati povredu radne obaveze, ugovorne obaveze ili drugu odgovornost u skladu sa zakonom, kolektivnim ugovorom, ugovorom o radu, internim aktima i drugim važećim propisima.

**Član 37.**
**(Stupanje na snagu)**

Ovaj pravilnik stupa na snagu danom donošenja, odnosno [osmog/narednog] dana od dana objavljivanja na oglasnoj ploči ili drugom internom komunikacijskom kanalu Društva, a primjenjuje se od dana stupanja na snagu.

*Broj:* 2251-8/2026
*Datum:* 07.09.2026 godine

Predsjednik Nadzornog odbora:

Damir Maglajlić

## PRILOZI / OBRASCI

Prilog 1 - Obrazac evidencije aktivnosti obrade

| **Element evidencije** | **Podaci / opis** |
|---|---|
| Naziv aktivnosti obrade | |
| Organizaciona jedinica / vlasnik procesa | |
| Svrha obrade | |
| Pravni osnov obrade | |
| Kategorije nosilaca podataka | |
| Kategorije ličnih podataka | |
| Posebne kategorije podataka / JMB / krivične osude | Da / Ne - opisati ako je primjenjivo |
| Kategorije primalaca | |
| Obrađivači / podobrađivači | |
| Prijenos u drugu državu ili međunarodnu organizaciju | Da / Ne - osnov i mjere |
| Rok čuvanja / kriterij za brisanje | |
| Tehničke i organizacione mjere | |
| Procjena rizika / potreba DPIA | |
| Datum uspostave i posljednjeg ažuriranja | |

Prilog 2 - Obrazac zahtjeva nosioca podataka

| **Element evidencije** | **Podaci / opis** |
|---|---|
| Ime i prezime podnosioca zahtjeva | |
| Adresa / e-mail / telefon za kontakt | |
| Vrsta zahtjeva | Pristup / ispravka / brisanje / ograničenje / prenosivost / prigovor / drugo |
| Opis zahtjeva | |
| Način dostave odgovora | Poštom / e-mailom / lično / drugo |
| Datum i potpis | |

Prilog 3 - Evidencija zahtjeva nosilaca podataka

| R.br. | Datum prijema | Podnosilac | Vrsta zahtjeva | Rok | Ishod / odgovor | Napomena |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Prilog 4 - Evidencija davanja/otkrivanja ličnih podataka

| R.br. | Datum | Korisnik / primalac | Pravni osnov | Svrha | Podaci / kategorije | Odobrio | Napomena |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Prilog 5 - Obrazac prijave i evidencije povrede ličnih podataka

| Element | Opis |
|---|---|
| Datum i vrijeme saznanja za incident | |
| Lice koje prijavljuje incident | |
| Opis incidenta / povrede | |
| Kategorije i približan broj nosilaca podataka | |
| Kategorije i približan broj evidencija podataka | |
| Moguće posljedice | |
| Hitne mjere koje su preduzete | |
| Procjena rizika | Nizak / srednji / visok |
| Da li je obaviještena Agencija | Da / Ne - datum i broj akta |
| Da li su obaviješteni nosioci podataka | Da / Ne - način i datum |
| Konačne korektivne mjere | |

Prilog 6 - Kontrolna lista za procjenu potrebe provođenja procjene uticaja

| Pitanje | Da/Ne | Napomena |
|---|---|---|
| Da li obrada uključuje obimnu obradu posebnih kategorija podataka? | | |
| Da li obrada uključuje podatke o krivičnoj osuđivanosti ili krivičnim djelima? | | |
| Da li se uvodi novi ili prošireni videonadzor javno dostupnog prostora? | | |
| Da li se koristi automatizirano odlučivanje ili profiliranje? | | |
| Da li obrada uključuje djecu ili posebno ranjive kategorije lica? | | |
| Da li obrada uključuje velik broj nosilaca podataka? | | |
| Da li se uvodi nova tehnologija, aplikacija, cloud servis ili integracija sistema? | | |
| Da li postoji prijenos podataka u drugu državu ili međunarodnu organizaciju? | | |
| Da li bi incident mogao uzrokovati ozbiljne posljedice po nosioce podataka? | | |
| Zaključak službenika za zaštitu ličnih podataka: DPIA potrebna / nije potrebna | | |

Prilog 7 - Izjava o povjerljivosti

Ja, _____, zaposlen/a ili angažovan/a u KJP "ZOI'84" OCS d.o.o. Sarajevo na poslovima _____, potvrđujem da sam upoznat/a s obavezom zaštite i čuvanja povjerljivosti ličnih podataka do kojih dođem u radu ili po osnovu angažmana.

Obavezujem se da ću lične podatke obrađivati isključivo u okviru ovlaštenja, radnih zadataka i uputstava Društva, da ih neću neovlašteno otkrivati, kopirati, iznositi, objavljivati, dostavljati ili koristiti za privatne svrhe, te da ću svaku sumnju na povredu ličnih podataka odmah prijaviti nadležnom rukovodiocu i službeniku za zaštitu ličnih podataka.

Obaveza povjerljivosti traje i nakon prestanka radnog odnosa, mandata ili angažmana, osim ako je oslobađanje od obaveze čuvanja povjerljivosti propisano zakonom ili odobreno na zakonit način.

U Sarajevu, dana _____ godine

Potpis: _____