

BOSNA I HERCEGOVINA
REPUBLIKA SRPSKA
OSNOVNI SUD U MRKONJIĆ GRADU
Broj: 075-0-Su-23-000 403/2
Mrkonjić Grad, 26.12.2023. godine

Na osnovu člana 48. stav 2. Zakona o sudovima Republike Srpske („Službeni glasnik Republike Srpske“, broj 37/12, 44/15 i 100/17) i člana 8. tačka i) Pravilnika o unutrašnjem sudskom poslovanju („Službeni glasnik Republike Srpske“, broj 9/14, 71/17, 67/18 i 6/19, Pravilnika o provođenju Zakona o zaštiti ličnih podataka u Osnovnom sud u Mrkonjić Gradu broj 075-0-Su-23-000 403, predsjednik Osnovnog suda u Mrkonjić Gradu, donosi:

PLAN SIGURNOSTI LIČNIH PODATAKA
U OSNOVNOM SUDU U MRKONJIĆ GRADU

POGLAVLJE I – OPŠTE ODREDBE

Član 1.
(Predmet)

Planom sigurnosti ličnih podataka propisuju se organizacione i tehničke mjere u Osnovnom sud u Mrkonjić Gradu (u daljem tekstu OSMG) u vezi sa obradom ličnih podataka u okviru evidencija iz Pravilnika o provođenju Zakona o zaštiti ličnih podataka u Osnovnom sud u Mrkonjić Gradu (u daljem tekstu Pravilnik).

Član 2.
(Pojmovi)

Pojedini pojmovi korišteni u ovom Planu imaju isto značenje kao pojmovi definisani u Zakonu o zaštiti ličnih podataka i pozitivnim propisima donesenim na temelju istog.

POGLAVLJE II – PRIMJENA PRINCIPA ZAŠTITE LIČNIH PODATAKA –
ORGANIZACIONE I TEHNIČKE MJERE

Član 3.
(Primjena osnovnih principa zaštite)

- (1) Organizacionim i tehničkim mjerama zaštite ličnih podataka u OSMG-u osigurava se primjena osnovnih principa obrade ličnih podataka i to: povjerljivosti, integriteta, raspoloživosti, autentičnosti, mogućnosti revizije i transparentnosti.

- (2) Organizacione i tehničke mjere zaštite ličnih podataka preduzimaju se u OSMG-u u okviru povjerenih nadležnosti.

Član 4.
(Povjerljivost i integritet)

- (1) Ličnim podacima koji se obrađuju u okviru nadležnosti OSMG-a mogu pristupati samo osobe koje su za to ovlaštene, u skladu sa članom 4. Pravilnika.
- (2) Zaposlenici OSMG-a koji vrše obradu ličnih podataka imaju obavezu da osiguraju da lični podaci za vrijeme obrade ostanu nepromijenjeni, potpuni i ažurni.
- (3) Zaposlenici OSMG-a koji vrše obradu ličnih podataka imaju obavezu da čuvaju tajnost ličnih podataka i pridržavaju se utvrđenog načina osiguranja istih.
- (4) Obaveza čuvanja tajnosti ličnih podataka ostaje na snazi i nakon prestanka radnog odnosa, odnosno određenog zadatka.
- (5) Ovlaštene osobe iz stava (1) ovog člana disciplinski su odgovorne za svaki vid zloupotrebe ličnih podataka koji su im dostupni.

Član 5.
(Autentičnost i mogućnost revizije)

- (1) Osobe koje obavljaju poslove obrade ličnih podataka u postupku obrade istih utvrđuju porijeklo ličnih podataka, pohranjujući dokaze o tome, koji se daju na uvid u postupku nadzora nad primjenom propisa iz ove oblasti.
- (2) Obradeni lični podaci mogu u slučaju potrebe biti podvrgnuti reviziji kojom se utvrđuje ko je, kada, koje lične podatke i na koji način obrađivao, nakon čega se na osnovu izvedenih dokaza vrši revizija podataka.

Član 6.
(Raspoloživost i transparentnost)

- (1) Osobe koje obavljaju poslove obrade ličnih podataka i administriranje zbirki ličnih podataka, odgovorne su za dostupnost i raspoloživost ličnih podataka, te ispravnost njihove obrade.
- (2) Svaki postupak pri obradi ličnih podataka mora biti potpun, ažuran i na odgovarajući način evidentiran.

Član 7.
(Organizacione mjere zaštite)

- (1) Obrada ličnih podataka vrši se u adekvatno opremljenim radnim prostorijama OSMG-a.

- (2) OSMG je dužan osigurati da se lični podaci, koji se vode u pisanoj formi, čuvaju u ormarićima pod ključem, te da pristup tim podacima imaju samo ovlaštene osobe zaposlene u OSMG-u, a koje obavljaju poslove obrade i administriranja ličnih podataka i koje su adekvatno obučeni za obavljanje ovih poslova.

Tehničke mjere zaštite

Član 8.

(Tehničke mjere zaštite unutar radnih prostorija OSMG-a)

- (1) Za obezbjeđenje radnih prostorija u toku radnog vremena odgovorni su zaposleni u OSMG-u koji obrađuju lične podatke.
- (2) Oprema unutar radnih prostorija, u koju se odlažu dokumenti koji sadrže lične podatke zaključava se u neradno vrijeme i tako se onemogućava pristup neovlaštenim licima. Ključevi od opreme odlažu se na mjesto dostupno samo zaposlenicima OSMG-a.

Član 9.

(Tehničke mjere u automatskoj obradi ličnih podataka)

- (1) Lični podaci koji se obrađuju putem automatske obrade osiguravaju se tehničkim mjerama i to:
 - (a) upotreba korisničkih imena i lozinki sastavljenih od kombinacije sa minimumom od sedam (7) karaktera, brojeva ili slova. Kao lozinka se ne smiju koristiti imena, lični podaci poznati drugim osobama, geografski i slični pojmovi i uobičajene riječi;
 - (b) da maksimalno trajanje lozinke je šezdeset (60) dana, nakon čega sistem automatski zahtjeva od korisnika promjenu lozinke;
 - (c) uvođenjem pravila da sistem prilikom promjene lozinke pamti pet (5) zadnjih korištenih lozinki i ne dozvoljava njihovo ponovno korištenje;
 - (d) ograničavanjem pristupa izvršiocima samo do dijelova sistema potrebnih izvršiocu za izvršavanje njegovih radnih zadataka;
 - (e) automatskim odjavljivanjem sa sistema po isteku perioda neaktivnosti u trajanju od petnaest (15) minuta, tako da je za ponovno aktiviranje potrebno upisati korisničko ime i lozinku;
 - (f) automatskom zabranom pristupa sistemu nakon tri (3) neuspješna pokušaja prijavljivanja na sistem i automatskim upozorenjem izvršiocu da potraži instrukciju od administratora sistema. Otključavanje korisničkog naloga vrši administrator sistema, isključivo po ličnom zahtjevu korisnika;
 - (g) efikasnom i sigurnom antivirusnom zaštitom sistema. Antivirusnom zaštitom će se upravljati putem centralne aplikacije koja će osigurati redovno ažuriranje antivirusnog programa i otklanjati slučajeve pojave virusa u informacionom sistemu;

- (h) osiguravanjem da se kompjuterska, programska i ostala neophodna oprema, na elektromagnetsku mrežu, priključuje putem uređaja za neprekidno napajanje.
- (2) Zaposleni koji obavlja kadrovske poslove dužan je redovno i pravovremeno izvještavati administratora zbirke ličnih podataka o zaposlenju ili angažiranju svakog zaposlenog s pravom pristupa informacijskom sistemu, kako bi se istima dodijelili korisničko ime i lozinka, kao i po prestanku zaposlenja ili angažiranja, da bi se korisničko ime i lozinka izbrisali odnosno zabranio daljnji pristup.
 - (3) Izvještavanje iz stava (2) ovog člana vrši se i prilikom bilo koje druge promjene radnog statusa zaposlenika, koja utiče na nivo ili obim pristupu zbirke ličnih podataka.
 - (4) Za zbirke ličnih podataka koje se obrađuju putem automatske obrade podataka OSMG, pored zaposlenih koji rade na obradi, osigurava i administratora zbirke ličnih podataka.

Član 10.

(Mjere fizičke zaštite prostorija u kojima se vrši automatska obrada podataka)

- (1) OSMG će osigurati odgovarajuće mjere tehničke zaštite prostorija u kojima se nalazi centar za obradu podataka i druge prostorije u kojima se vode ili obrađuju zbirke ličnih podataka, na način da će iste biti opremljene sistemom video nadzora i elektronske kontrole pristupa.
- (2) Ulazak u prostorije centra za obradu podataka je omogućen isključivo IKT službeniku OSMG-a. Ostali zaposleni ili treće osobe, mogu ući u centar za obradu podataka samo po ovlaštenju IKT službenika, i to uz njegovu pratnju.

Član 11.

(Organizacione mjere kod automatske obrade)

OSMG provodi organizacione mjere zaštite ličnih podataka koji se obrađuju automatski time što osigurava:

- (a) potpunu tajnost i sigurnost lozinki i ostalih formi za identifikaciju pristupa ličnim podacima;
- (b) uništavanje dokumenata koji sadrže lične podatke po isteku roka za obradu;
- (c) svako iznošenje bilo kojeg medija koji sadrži lične podatke van radnih prostorija mora biti sa posebnom dozvolom predsjednika suda kako ne bi došlo do gubljenja ili nezakonitog korištenja. Zabranjeno je pohranjivanje ličnih podataka na privatne prenosive medije;
- (d) da slanje ličnih podataka putem elektronske pošte predstavlja neprihvatljivu upotrebu elektronske pošte koja će biti sankcionirana u skladu sa internim propisima o disciplinskoj odgovornosti OSMG-a;
- (e) mjere fizičke zaštite radnih prostorija i opreme gdje se obrađuju lični podaci;
- (f) poštivanje tehničkih uputstava pri instaliranju i korištenju opreme koja služi za obradu ličnih podataka. IKT službenik će dosljedno poštivati uputstva pri instaliranju opreme koja služi za obradu ličnih podataka.

Član 12.
(Mrežna barijera)

IKT službenik OSMG-a osigurava odgovarajuću zaštitu od neovlaštenog upada – mrežnu barijeru između sistema i Internet mreže, ili bilo koje druge forme spoljne mreže.

Član 13.
(Sigurnosna kopija)

- (1) Administrator zbirki ličnih podataka ima obavezu da redovno snima sigurnosne kopije ili arhivira podatke u sistemu, da ne bi došlo do njihovog gubljenja i uništenja.
- (2) Administrator će provjeravati upotrebljivost sigurnosnih kopija zbirki uz provjeru postupka povrata zbirki pohranjenih na prenosivom informatičkom mediju tako da vraćeni podaci nakon izvršene provjere budu u cjelosti raspoloživi za upotrebu, bez gubitka informacija.
- (3) Svaki primjerak pohranjenih podataka na prenosivom informatičkom mediju mora biti označen brojem, vrstom, datumom pohranjivanja, te imenom lica koje je pohranjivanje izvršilo.
- (4) Zabranjeno je umnožavanje informatičkih medija koji sadrže podatke iz zbirki posebnih kategorija ličnih podataka bez nadzora i odobrenja predsjednika suda.

Član 14.
(Evidencija, praćenje pristupa i pokušaj neovlaštenog pristupa sistemu)

- (1) Svaki pristup informacionom sistemu za vođenje zbirki ličnih podataka će biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave. IKT službenik će elektronski evidentirati i kontrolisati pristup ovlaštenih korisnika van informacionog sistema prema lokalnoj računarskoj mreži koja se ostvaruje putem VPN tehnologije ili na drugi dozvoljeni način.
- (2) Svaki pokušaj neovlaštenog pristupa sistemu će biti automatski zabilježen korisničkim imenom, datumom i vremenom, ako je to moguće i mjestom s kojeg je takav pristup pokušan.
- (3) Administrator zbirki ličnih podataka dužan je obavijestiti predsjednika suda o svakom pokušaju neovlaštenog pristupa informacionom sistemu.

Član 15.
(Obavezna upotreba jedinstvenih korisničkih imena i propusnica za pristup sistemu)

- (1) Pristup podacima pohranjenim u zbirkama ličnih podataka dozvoljen je upotrebom dodijeljenog jedinstvenog korisničkog imena i lozinke.
- (2) Ukinuto korisničko ime ne smije se dodijeliti drugom licu.

- (3) Korisničko ime i pripadajuća lozinka ne smiju se odati ili dati drugom licu. Svaki korisnik informacionog sistema je odgovoran za postavljanje i upotrebu lozinke korisničkog naloga koji koristi, te istu ne smije na bilo koji način otkrivati drugima. U suprotnom, smatrat će se da je izvršena povreda službene dužnosti.
- (4) Prvu lozinku za kreirani nalog postavlja administrator zbirke ličnih podataka prilikom kreiranja korisničkog imena.

Član 16.

(Osoba odgovorna za zaštitu ličnih podataka)

Za uredno provođenje mjera osiguranja, pohranjivanja i zaštite ličnih podataka odgovaraju osobe koje vrše obradu istih i administratori zbirke ličnih podataka.

Član 17.

(Osobe ovlaštene za dodjeljivanje korisničkih imena i lozinki)

IKT službenik OSMG-a je ovlašten za dodjeljivanje i uklanjanje korisničkih imena i dodjeljivanje lozinki osobama ovlaštenim za rad u sistemu, a kojima je dozvoljen pristup zbirkama ličnih podataka.

Član 18.

(Zaštita posebne kategorije ličnih podataka)

- (1) Prilikom obrade posebne kategorije ličnih podataka u svim fazama obrade označava se da se radi o obradi navedene kategorije podataka, te se za to preduzimaju dopunske organizacione i tehničke mjere.
- (2) Prijenos posebnih kategorija ličnih podataka preko telekomunikacijskih sistema se mora ostvarivati korištenjem VPN tehnologije.

Član 19.

(Sedmično, mjesečno i godišnje provjeravanje rada sistema)

Administrator zbirke ličnih podataka je obavezan da sedmično, mjesečno i godišnje provjerava rad svih dijelova sistema.

Član 20.

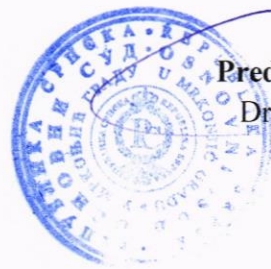
(Posebne mjere zaštite podataka)

Lični podaci koji se obrađuju u okviru evidencija čija zaštita zahtjeva posebne mjere propisane drugim propisima, kao što su evidencije koje se tiču tajnih podataka, mogu biti zaštićeni posebnim organizacionim i tehničkim mjerama u skladu sa propisima iz te oblasti.

POGLAVLJE III – PRELAZNE I ZAVRŠNE ODREDBE

Član 21. (Stupanje na snagu)

Ovaj Plan stupa na snagu danom donošenja i objavljuje se na oglasnoj tabli suda i službenoj web stranici.



Predsjednik suda,
Drazen Vulin