

Bosna i Hercegovina
Federacija Bosne i Hercegovine
USTANOVA ZA SOCIJALNO ZBRINJAVANJE, ODGOJ I OBRAZOVANJE –
SARAJEVO
SARAJEVO

PLAN SIGURNOSTI
PODATAKA KOJIM SE ODREĐUJU TEHNIČKE I ORGANIZACIONE MJERE
ZA SIGURNOST LIČNIH PODATAKA U USTANOVU ZA SOCIJALNO
ZBRINJAVANJE, ODGOJ I OBRAZOVANJE -SARAJEVO

Decembar, 2025.godine

Ustanova za socijalno zbrinjavanje, odgoj i obrazovanje – Sarajevo, Humska 81.
tel. 033 726 320 fax. 033 654 895 e-mail: info@ustanovahum.ba www.ustanovahum.ba

Na osnovu člana 44. Zakona o ustanovama socijalne zaštite Federacije Bosne i Hercegovine („Službeni novine FBiH“ broj 64/22), i člana 37. Pravila Ustanove za socijalno zbrinjavanje, odgoj i obrazovanje-Sarajevo, Upravni odbor Ustanove, na .sjednici, održanoj dana 08.12.2025. godine donosi:

PLAN SIGURNOSTI

PODATAKA KOJIM SE ODREĐUJU TEHNIČKE I ORGANIZACIONE MJERE ZA SIGURNOST LIČNIH PODATAKA U USTANOVU ZA SOCIJALNO ZBRINJAVANJE, ODGOJ I OBRAZOVANJE-SARAJEVO

I. - OPĆE ODREDBE

Član 1.

Planom sigurnosti podataka određuju se tehničke i organizacione mjere za sigurnost ličnih podataka, te se bliže propisuje način čuvanja i posebne mjere tehničke zaštite ličnih podataka (u daljnjem tekstu: Plan) u Ustanovi za socijalno zbrinjavanje, odgoj i obrazovanje-Sarajevo (U daljnjem tekstu: Ustanova).

Izrazi koji se koriste u ovom Planu imaju isto značenje kao u Zakonu.

Član 2.

Pojedini pojmovi korišteni u ovom Planu imaju sljedeće značenje:

- a) "Operater za informaciono-dokumentacione poslove - Administrator zbirke ličnih podataka" je fizičko lice ovlašteno i odgovorno za sistem upravljanja zbirkom ličnih podataka i za osiguranje tajnosti i zaštite obrade ličnih podataka.
- b) "Izvršilac" je fizičko lice, zaposleno ili angažirano kod kontrolora (u daljem tekstu: Centar) koje izvršava poslove vezane za obradu ličnih podataka.

II. - NAČIN ČUVANJA LIČNIH PODATAKA

Član 3.

Način čuvanja ličnih podataka podrazumijeva poduzimanje organizacijskih i tehničkih mjera zaštite ličnih podataka.

Član 4.

Ustanova osigurava organizacijske mjere zaštite ličnih podataka koje obuhvataju: informiranje i obuku zaposlenih koji rade na obradi ličnih podataka, fizičke mjere zaštite radnih prostorija i opreme u kojima se vrši obrada ličnih podataka, sprečavanje neovlaštenog umnožavanja, kopiranja i prepisivanja ličnih podataka, uništavanja ličnih podataka i drugo.

Nakon prijema u radni odnos, a prije otpočinjanja obavljanja radnih dužnosti, svako lice koje će u okviru poslova i zadataka obrađivati lične podatke upoznaće se sa mjerama zaštite ličnih podataka.

Prije neposrednog otpočinjanja obavljanja poslova vezanih za obradu ličnih podataka, Ustanove, dodatno upoznaće zaposlenog sa konkretnim obavezama po pitanju zaštite ličnih podataka.

Ustanova osigurava stalnu fizičku zaštitu (najmanje jedan zaštitar u objektu) objekata i podataka u radnom vremenu tokom 24:00 sata, svih dana u sedmici.

Ustanova osigurava tehničku zaštitu (alarmni nadzor, vatro dojava, plinodojava) objekata i podataka tokom 24:00 sata, svih dana u sedmici.

Član 5.

Ustanova osigurava odgovarajuće mjere tehničke zaštite prostorija i opreme u kojima se vrši obrada ličnih podataka.

Posebnim mjerama tehničke zaštite ličnih podataka treba onemogućiti neovlašten pristup i obradu istih.

Tehničke mjere zaštite ličnih podataka, između ostalog, obuhvataju kontrolu pristupa prostorijama i opremi za obradu ličnih podataka, zaštitu od uništenja i oštećenja ličnih podataka i drugo.

Sve zbirke evidencija ličnih podataka a koje se vode u pismenom obliku su zaštićene i nalaze se zaključane u sigurnosne kase.

Član 6.

Osnovna načela Plana su:

- povjerljivost - samo ovlaštena lica mogu znati lične podatke;
- integritet - da za vrijeme obrade lični podaci ostanu nepromijenjeni, potpuni i ažurni;
- raspoloživost - da su podaci stalno dostupni, da su na raspolaganju i da se mogu ispravno obrađivati;
- autentičnost - da se u svako doba može utvrditi porijeklo ličnih podataka;
- mogućnost revizije - da se može utvrditi ko, kada, koje je lične podatke i na koji način obrađivao;
- transparentnost - da će postupak pri obradi ličnih podataka biti potpun, ažuran i na

odgovarajući način evidentiran.

Plan sigurnosti ličnih podataka sadrži kategorije ličnih podataka koje se obrađuju i popis instrumenata zaštite odnosno organizacijske i tehničke mjere zaštite.

Plan sigurnosti ličnih podataka je sačinjen u pismenoj formi, ažuriran i stalno dostupan Agenciji za zaštitu ličnih podataka u Bosni i Hercegovini.

III. - ZAŠTITA LIČNIH PODATAKA U AUTOMATSKOJ OBRADI

Član 7.

Ustanova pri automatskoj obradi ličnih podataka osigurava tehničke mjere zaštite ličnih podataka i to:

- a) jedinstveno korisničko ime i lozinku sastavljenu od kombinacije minimum šest karaktera, brojeva ili slova;
- b) automatsku izmjenu lozinke po utvrđenom vremenskom periodu koji ne može biti duži od šest mjeseci;
- c) korisničko ime i lozinka dozvoljava pristup samo do dijelova sistema potrebnih izvršiocu za izvršenje njegovih radnih zadataka;
- d) automatsko odjavljivanje sa sistema po isteku određenog perioda neaktivnosti, ne duže od 15 minuta, a za ponovno aktiviranje sistema potrebno je nanovo upisati korisničko ime i lozinku;
- e) automatsku zabranu pristupa sistemu nakon tri neuspješna pokušaja prijavljivanja na sistem i automatsko upozorenje izvršiocu da potraži instrukciju od Operatera za informaciono-dokumentacione poslove;
- f) efikasnu i sigurnu antivirusnu zaštitu sistema, koje će se stalno ažurirati radi preventive od nepoznate ili neplanirane opasnosti od novih virusa;
- g) kompjuterska, programska i ostala neophodna oprema na elektorenergetsku mrežu se priključuje putem uređaja za neprekidno napajanje.

U slučaju iz tačke e. stav (1) ovog člana operater za informaciono-dokumentacione poslove odobrava daljnji pristup sistemu.

Izvršilac koji obavlja kadrovske poslove, izvještava operatera za informaciono-dokumentacione poslove o zaposlenju ili angažiranju svakog izvršioca s pravom pristupa informacijskom sistemu, kako bi se dodijelili korisničko ime i lozinka, kao i po prestanku zaposlenja ili angažiranja, da bi se korisničko ime i lozinka izbrisali odnosno zabranio daljnji pristup.

Izveštavanje iz stava (3) ovog člana vrši se i prilikom bilo koje druge promjene radnog statusa izvršioca, koja utiče na nivo ili obim pristupu zbirke ličnih podataka.

Član 8.

Ustanova pri automatskoj obradi ličnih podataka osigurava organizacijske mjere zaštite ličnih podataka i to:

- potpunu tajnost i sigurnost lozinki i ostalih formi za identifikaciju pristupa ličnim podacima;
- organizacijska pravila za pristup izvršioca internetu koja se odnose na preuzimanje i snimanje dokumenata putem elektronske pošte ili drugih izvora;
- uništavanje dokumenata koji sadrže lične podatke po isteku roka za obradu;
- svako iznošenje bilo kojeg medija koji sadrži lične podatke van radnih prostorija mora biti sa posebnom dozvolom i kontrolom da ne dođe do gubljenja ili nezakonitog korištenja;
- mjere fizičke zaštite radnih prostorija i opreme gdje se obrađuju lični podaci; i
- poštivanje tehničkih uputstava pri instaliranju i korištenju opreme koja služi za obradu ličnih podataka.

Član 9.

Ustanova će osigurati odgovarajuću zaštitu - mrežnu barijeru između njegovog sistema i Internet mreže, ili bilo koje druge forme spoljne mreže, kao zaštitu protiv nedozvoljenog pokušaja ulaza u sistem.

Član 10.

Pristup podacima pohranjenim u zbirkama ličnih podataka dozvoljen je ovlaštenim licima uposlenim u Ustanovi ili obrađivaču i ovlaštenim licima zaduženim za održavanje i razvoj sistema za vođenje zbirke ličnih podataka.

Ustanova određuje lica iz stava (1) ovoga člana.

Obrađivač nema ovlaštenja za određivanje lica iz stava (1) ovog člana.

Zahtjev za pristup ili obradu te zahtjev za prestanak ovlaštenja za pristup zbirkama ličnih podataka ili obradu ličnih podataka podnosi se Ustanovi koji daje ili ukida dozvolu za pristup zbirkama.

Član 11.

Ustanova redovno snima sigurnosne kopije ili arhivira podatke u sistemu, da ne bi došlo do njihovog gubljenja ili uništenja.

Ustanova provjerava upotrebljivost sigurnosnih kopija zbirki uz provjeru postupka povrata zbirki pohranjenih na prenosivom informatičkom mediju tako da vraćeni podaci nakon izvršene provjere budu u cijelosti raspoloživi za upotrebu, bez gubitka informacija.

Svaki primjerak pohranjenih podataka na prenosivom informatičkom mediju mora biti označen brojem, vrstom, datumom pohranjivanja, te imenom lica koje je pohranjivanje izvršilo.

Zabranjeno je bez nadzora i odobrenja centra na bilo koji način umnožavanje informatičkih medija koja sadrže podatke iz zbirke posebnih kategorija ličnih podataka.

Član 12.

Pristup u informacijski sistem za vođenje zbirke ličnih podataka ili obradu podataka iz zbirke dozvoljen je uz upotrebu odgovarajućih korisničkih imena i pripadajućih propusnica.

Ustanova će evidentirati i kontrolisati svako pravo pristupa zaposlenih vanjskim mrežama, kao i pravo pristupa kompjuterskim sistemima ili lokalnoj mreži korisnicima van kompjuterskog sistema.

Modemski priključci i njihovi brojevi, koji se koriste za pristup sistemu, na kojem su pohranjene zbirke ličnih podataka ne objavljuju se u telefonskim imenicima i ne smiju biti dostupni preko službe za davanje telefonskih brojeva.

Član 13.

Pristup podacima pohranjenim u zbirka ličnih podataka dozvoljen je upotrebom dodjeljenoga jedinstvenog korisničkog imena i propusnice.

Ukinuto korisničko ime ne smije se dodijeliti drugom licu.

Korisničko ime i pripadajuća propusnica ne smiju se odati ili dati drugom licu.

Način dodjeljivanja i obavezu izmjene propusnice određuje Ustanova.

Član 14.

Svaki pristup informacijskom sistemu za vođenje zbirke ličnih podataka mora biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave.

Svaki pokušaj neovlaštenog pristupa sistemu mora biti automatski zabilježen korisničkim imenom, datumom i vremenom, ako je to moguće i mjestom s kojeg je takav pristup pokušan.

Operater za informaciono-dokumentacione poslove i izvršilac dužni su obavijestiti odgovorno lice u službi-Šefa Službe o svakom pokušaju neovlaštenog pristupa sistemu.

Član 15.

Za uredno provođenje mjera osiguranja, pohranjivanja i zaštite ličnih podataka odgovara šef Službe.

Član 16.

Ustanova određuje zaposlenika ovlaštenog za dodjeljivanje i uklanjanje korisničkih imena i dodjeljivanje propusnica licima ovlaštenim za rad u sistemu, a kojima je dozvoljen pristup zbirkama ličnih podataka.

Član 17.

Prilikom obrade posebne kategorije ličnih podataka u svim fazama obrade Ustanova označava da se radi o obradi navedene kategorije podataka.

Ustanova preduzima dopunske tehničke i organizacijske mjere pri obradi posebnih kategorija ličnih podataka.

Putem dopunskih tehničkih i organizacijskih mjera pri obradi posebne kategorije ličnih podataka osigurava se:

- mogućnost za prepoznavanje svakog pojedinačnog ovlaštenog pristupa informacijskom sistemu;
- rad sa podacima tokom redovnog radnog vremena Ustanove; i
- kriptazaštita podataka pri prijenosu preko telekomunikacionih sistema sa odgovarajućim softverskim i tehničkim mjerama.

Član 18.

Ustanova sedmično, mjesečno i godišnje provjerava rad svih dijelova sistema.

Član 19.

Nadzor nad provedbom ovog Plana vrši Ustanova.

Član 20.

Ovaj Plan stupa na snagu osmog dana od dana donošenja.

Donošenjem ovog plana, prestaje da važi Plan sigurnosti podataka kojim se određuju tehničke i organizacione mjere za sigurnost ličnih podataka u Zavodu za vaspitanje muške djece i omladine -Sarajevo broj 477/13 od 31.05.2013. godine.

Broj: 05-2840-6/25

Datum: 08.12.2025. godine

Predsjednik
Upravnog odbora

Lejla Jusufrić, prof. pedagogije

