



e - mediacija: Digitalna prihodnost reševanja sporov

Tehnični in organizacijski vidiki izvedbe

Operacija se izvaja v okviru javnega razpisa Problemsko učenje študentov v delovno okolje 2024–2027 (PUŠ v delovno okolje 2024–2027). Operacijo sofinancirata Republika Slovenija, Ministrstvo za izobraževanje, znanost in mladino ter Evropska unija iz Evropskega socialnega sklada plus (ESS+).

Ljubljana, 2026



Kazalo

SPLOŠNE DOLOČBE	3
TEHNIČNA INFRASTRUKTURA IN VARNOST.....	3
PREVERJANJE IDENTITETE IN VAROVANJE ZAUPNOSTI	3
ORGANIZACIJA IN VODENJE VIRTUALNIH SREČANJ	4
ZAČETEK POSTOPKA	4
PRIDOBITEV SOGLASJA.....	5
RAVNANJE OB TEHNIČNIH ZAPLETIH IN PREKINITVAH POVEZAVE.....	5
PRAVILA KOMUNIKACIJE V DIGITALNEM OKOLJU	6
Primer PRAVILNIKA O VARNI IZMENJAVI DOKUMENTACIJE IN ELEKTRONSKEM	
PODPISOVANJU V POSTOPKIH E-MEDIACIJE	6
NAMEN IN PODROČJE UPORABE	6
PROTOKOL ZA VARNO IZMENJAVO PODATKOV	7
PROTOKOL ZA ELEKTRONSKO PODPISOVANJE DOKUMENTOV.....	7
HRAMBA IN IZBRIS PODATKOV PO ZAKLJUČKU POSTOPKA	7
Pregled ključne dokumentacije in tehničnih standardov	9
Tabela 1: osnovne procesne dokumentacije	9
Tabela 2: Tehnične rešitve in varnostni ukrepi	10

SPLOŠNE DOLOČBE

Ta protokol določa minimalne tehnične standarde, varnostne ukrepe in organizacijska pravila za izvedbo mediacijskega postopka v digitalnem okolju (v nadaljevanju: e-mediacija).

Določbe tega protokola zavezujejo mediatorja, stranke in njihove morebitne pooblaščenke ter druge udeležence, ki s podpisom Sporazuma o mediaciji potrjujejo izpolnjevanje tehničnih pogojev in pristajajo na spodaj navedena pravila.

E-mediacija se izvaja v skladu z določili Zakona o mediaciji v civilnih in gospodarskih zadevah (ZMCGZ), Uredbe (EU) 2016/679 (GDPR) ter splošnimi načeli alternativnega reševanja sporov.

TEHNIČNA INFRASTRUKTURA IN VARNOST

Izbira platforme: Postopek se izvaja prek avtorizirane videokonferenčne poti, ki zagotavlja varno šifriranje podatkovnega toka (end-to-end encryption). Za potrebe tega postopka se določi uporaba platforme, ki gostuje na strežniški infrastrukturi znotraj Evropske unije. Iskanje primerne programske opreme (npr. Zoom, MS Teams, Cisco Webex), ki omogoča stabilno avdio-video povezavo. Ključno je, da platforma podpira funkcijo "sejnih sob" (*breakout rooms*), kar je nujno za izvedbo ločenih srečanj z vsako od strank.

Zahteve za strojno opremo: Udeleženci morajo zagotoviti stabilno internetno povezavo, delujočo spletno kamero z visoko ločljivostjo ter zanesljiv mikrofonski in zvočnik (uporaba slušalk je priporočljiva zaradi preprečevanja akustičnega odmeva in zagotavljanja zasebnosti).

Prepoved lokalnega snemanja: Strogo je prepovedano vsakršno zvočno ali slikovno snemanje e-mediacije (lokalno, v oblaku ali prek zunanjih naprav). Kršitev te določbe pomeni hudo kršitev načela zaupnosti in je podlaga za takojšnjo prekinitve postopka s strani mediatorja.

PREVERJANJE IDENTITETE IN VAROVANJE ZAUPNOSTI

Avtentikacija: Pred uradnim začetkom prvega e-srečanja mediator izvede identifikacijo strank. Stranke morajo neposredno pred kamero predložiti veljaven osebni dokument s sliko. Če tehnologija to omogoča, se za vstop v virtualno okolje lahko zahteva predhodna prijava prek državnega sistema za enotno prijavo (SI-PASS).

Varna izmenjava dokumentacije: Določitev protokolov in varnih poti (npr. šifriran e-naslov, varne oblačne shrambe z nadzorom dostopa), preko katerih si stranke in mediator izmenjujejo dokazila ali predloge sporazumov.

Elektronsko podpisovanje dokumentov: Izbira pravno veljavne metode za podpisovanje ključnih dokumentov (kot sta sporazum o vključitvi in končni mediacijski sporazum) na daljavo, na primer z uporabo kvalificiranih digitalnih potrdil (npr. SIGOV-CA, SI-PASS) ali platform, kot je DocuSign.

Po pozitivno opravljeni presoji primernosti spora ter pridobitvi ustreznega soglasja obeh strank je naloga mediatorja opraviti zanesljivo preverjanje identitete vseh udeležencev v postopku. Sama preverba identitete ter pooblastil zastopnikov strank v postopku temelji na 3. členu ZMCGZ ter Uredbi (EU) 910/2014 (eIDAS). Metode, ki jih lahko mediator pri tem uporabi so kvalificirane oblike elektronske identifikacije preko uporabe sistema SI-PASS ali sheme eIDAS, ali preko kvalificiranega digitalnega potrdila. V primeru, da stranka ne bi imela imela urejenih navedenih oblik elektronske identifikacije se lahko uporabi tudi video-identifikacija. Obenem pa mora mediator preveriti tudi veljavnost pooblastil zastopnikov podjetij preko izpiska iz Poslovnega registra Slovenije (AJPES) ali preko kvalificiranega digitalnega potrdila zakonitega zastopnika.

Pri izvajanju video-identifikacije se uporabi protokol vizualne uskladitve v živo, kjer mora stranka svoj veljaven osebni dokument s sliko pokazati neposredno pred delujočo kamero visoke ločljivosti. Za zagotavljanje popolne zaupnosti postopka je mediator dolžan izvesti tudi nadzor nad fizičnim prostorom; vsaka stranka mora zagotoviti, da se nahaja v zaprtem in izoliranem prostoru brez prisotnosti nepooblaščenih tretjih oseb. Mediator ima pravico pred začetkom obravnave zahtevati, da stranka s kamero izvede 360-stopinjski pregled prostora, če obstaja sum o prisotnosti drugih oseb.

ORGANIZACIJA IN VODENJE VIRTUALNIH SREČANJ

Skupna srečanja: Vsi udeleženci morajo imeti ves čas trajanja skupnega srečanja vklopljeno kamero in mikrofona, razen če mediator odredi drugače.

Ločena srečanja (Breakout Rooms): Mediator lahko tekom postopka odredi prehod na ločena srečanja. Tehnična izvedba se zagotovi prek funkcije virtualnih ločenih sob, ki popolnoma izolirajo zvok in sliko med mediatorjem in posamezno stranko. Medtem ko mediator opravlja pogovor z eno stranko, druga stranka počaka v primarni virtualni sobi ali digitalni čakalnici, pri čemer sta njena komunikacija in dostop do ločenega pogovora tehnično blokirana.

ZAČETEK POSTOPKA

Pobuda, presoja primernosti spora, prva komunikacija. Sam začetek postopka temelji na 6. in 7. členu ZMCGZ, ki urejata način začetka mediacije ter njegovo vodenje. Ker zakon eksplicitno ne določa pravil, ki bi urejala način izvedbe mediacije v digitalni obliki, smo v modelu online mediacije določili, da sta lahko pobuda in vabilo podana v pisni ali elektronski obliki, s čimer zagotavljamo sledljivost ter dokazljivost procesnih dejanj med postopkom. Postopek se začne na podajanje pobude ene izmed strank ali obeh strank hkrati, ki jo tej posredujejo izbranemu

mediatorju. Pobuda mora vsebovati osnovne podatke o strankah ter kratek opis spora. Pred začetkom e-mediacije mora mediator opraviti presojo primernosti spora in pri tem preveriti ali zadevani spor spada na področje uporabe ZMCGZ, torej ali gre za civilni, gospodarski, družinski ali premoženjskopravni spor. Poleg tega pa mora preveriti tudi ali je pri vseh strankah spora prisotna prostovoljna volja za udeležbo ter ali sama narava spora dopušča njegovo reševanje na daljavo, pri čemer mora biti mediator pozoren predvsem na morebitno odsotnost ravnovesja moči ali potrebe po neposrednem fizičnem stiku. V primeru, da mediator po predhodni preverbi ugotovi neprimernost spora for izvedbo online mediacije, mora o ugotovitvi pisno obvestiti pobudnika ter mu predlagati druge alternativne oblike za reševanje spora. V nasprotnem primeru, pa mediator pošlje nasprotni stranki vabilo k mediaciji. Po sprejemu vabila nasprotne stranke, mediator obema strankama posreduje ključne informacije o izvedbi postopka mediacije, o njenih pravilih, tehničnih zahtevah, varstvu osebnih podatkov ter predlog termina. Vabilo k mediaciji, ki ga mediator posreduje nasprotni stranki, mora obvezno vsebovati tudi natančne tehnične zahteve za sodelovanje (seznam potrebne strojne in programske opreme) ter obrazec Soglasja za digitalno izvedbo mediacijskega postopka. Nasprotna stranka mora to soglasje vrniti izpolnjeno in podpisano še pred določitvijo prvega termina, saj prejem tega dokumenta predstavlja procesni pogoj za nadaljevanje e-postopka.

PRIDOBITEV SOGLASJA

Obe stranki morata pred začetkom postopka prav tako podati svoje izrecno pisno soglasje o svojem prostovoljnem sodelovanju. Soglasje je lahko podano preko varnega elektronskega obrazca na izbrani platformi ali preko kvalificiranega elektronskega podpisa, preko česa se še dodatno zagotavlja večja dokazljivost ter sledljivost procesnega dejanja. Poleg varnega elektronskega obrazca in kvalificiranega elektronskega podpisa se lahko pridobitev soglasij in izjav izvede tudi preko potrditvenega polja (angl. checkbox) ob sami registraciji ali vstopu uporabnika v zaprt sistem e-mediacije. Takšen sistem uporabniku tehnično onemogoči vstop v virtualno sobo ali napredovanje skozi postopek, dokler z označitvijo polja izrecno ne potrdi seznanjenosti s pravili zaupnosti in varstva osebnih podatkov. Pridobitev soglasja temelji na 3. členu ZMCGZ, ki v svoji vsebini določa, da mora biti postopek mediacije izveden prostovoljno. Obenem pa podpisano soglasje predstavlja tudi pravno podlago oziroma dovoljenje for obdelavo osebnih podatkov posameznika in sicer na podlagi 6. člena GDPR. V primeru, da stranka ne bi želela podati soglasja za izvedbo mediacije na daljavo, se postopek ne more nadaljevati, saj bi s tem kršili osnovno načelo prostovoljnosti ter zahtevo za varstvo osebnih podatkov.

RAVNANJE OB TEHNIČNIH ZAPLETIH IN PREKINITVAH POVEZAVE

Če med e-srečanjem pride do prekinitve internetne povezave ali druge tehnične napake pri enem izmed udeležencev, se postopek začasno zaustavi.

Stranka, ki je izgubila povezavo, mora nemudoma poskusiti ponovno vstopiti v virtualno sobo. Če ponovna vzpostavitev povezave ni mogoča v roku 10 minut, se e-mediacija prekine.

Kot alternativni komunikacijski kanal se določi telefonska povezava na telefonsko številko mediatorja, prek katere se udeleženci dogovorijo o nadaljevanju ali preložitvi srečanja.

Preložitev ali prehod na hibridni model: Če je napaka na strani ponudnika platforme ali gre za trajnejšo motnjo na omrežju stranke, mediator določi nov termin e-srečanja ali pa (skladno s smernicami za hibridni model) predlaga, da se naslednje srečanje izvede v fizični obliki na sedežu institucije, s čimer se zavaruje načelo ekonomičnosti in učinkovitosti postopka.

PRAVILA KOMUNIKACIJE V DIGITALNEM OKOLJU

Pravila, ki določajo zaupnost mediacije ter uporabo ustreznih tehničnih in organizacijskih ukrepov za zagotovitev varnosti pri obdelavi osebnih podatkov, temeljijo na 11. členu ZMCGZ ter 32. členu GDPR. Preko ustreznega izvajanja teh ukrepov poskušamo preprečiti kakršenkoli nepooblaščen dostop do komunikacije med strankami ter zagotavljati zaupnost postopka, ki je ključna for izvedbo uspešne mediacije. Zaradi navedenega predlagamo, da pretežni del komunikacije med strankami in mediatorjem poteka preko izbrane varne platforme, ki mora zagotavljati ustrezne tehnične predpostavke, kot so uporaba end-to-end enkripcije (E2EE), protokola HTTPS/TLS 1.3 ter dvofaktorske avtentikacije. V začetni fazi postopka, ko se morajo pridobiti pobuda, vabilo ali izvesti druga procesna dejanja, je dovoljena komunikacija tudi preko varne elektronske pošte ali elektronskih obrazcev, pod pogojem da so uporabljeni ustrezni tehnični ukrepi za zagotavljanje varnosti. Stranke se morajo strinjati, da bo vsa komunikacija potekala preko izbranih varnih kanalov. Med izvedbo mediacije je prepovedano snemanje, fotografiranje ali shranjevanje vsebine ali drugih podatkov brez predhodnega soglasja vseh udeležencev.

Zaradi preprečevanja akustičnega odmeva in dodatnega zagotavljanja zasebnosti je za vse udeležence med trajanjem e-srečanja priporočljiva uporaba slušalk z mikrofonom. S tem se tehnično prepreči, da bi zvok iz mediacije slišale osebe v okolici udeleženca.

Strogo je prepovedano vsakršno zvočno ali slikovno snemanje e-mediacije, bodisi lokalno na trdi disk računalnika, v oblaku ali prek zunanjih naprav (npr. pametni telefoni, diktafoni). Kršitev te določbe se šteje za hudo kršitev načela zaupnosti in predstavlja zakonsko podlago, da mediator nemudoma trajno prekine postopek mediacije.

Primer PRAVILNIKA O VARNI IZMENJAVI DOKUMENTACIJE IN ELEKTRONSKEM PODPISOVANJU V POSTOPKIH E-MEDIACIJE

NAMEN IN PODROČJE UPORABE

Pravilnik ureja tehnične in organizacijske ukrepe, ki jih morajo mediatorji in strokovno osebje spoštovati pri ravnanju z gradivi, prenosu dokumentov in podpisovanju končnih sporazumov, kadar postopki mediacije potekajo na daljavo.

PROTOKOL ZA VARNO IZMENJAVO PODATKOV

1. Prepoved nezaščitenih kanalov: Izmenjava kakršnih koli dokumentov, ki vsebujejo osebne podatke, poslovne skrivnosti ali podrobnosti o sporu, prek splošnih nešifriranih aplikacij za klepet ali javnih oblačnih shramb je strogo prepovedana.
2. Dovoljeni kanali: Vsi dokumenti se prednostno izmenjujejo prek šifrirane e-pošte, pri čemer morajo biti datoteke v formatu PDF, po potrebi zaščitene z geslom, ki ga mediator strankam posreduje prek ločenega komunikacijskega kanala (SMS ali telefonski klic). Če je na voljo centralna e-platforma (npr. nadgrajen sistem e-Sodstva ali specializiran zaprt portal), se izmenjava izvaja izključno znotraj te platforme s sledljivostjo dostopa.
3. Pravilo minimalnega obsega podatkov: Mediator od strank zahteva le tisto dokumentacijo, ki je nujno potrebna za razumevanje predmeta spora, s čimer se zmanjša izpostavljenost podatkov v digitalnem okolju.

PROTOKOL ZA ELEKTRONSKO PODPISOVANJE DOKUMENTOV

1. Zavezujoča oblika podpisovanja: Za sklenitev Sporazuma o vključitvi v mediacijo ter končnega Mediacijskega sporazuma (ki lahko pridobi status izvršilnega naslova) se zahteva uporaba kvalificiranega elektronskega podpisa (KEP).
2. Uporaba državnih in evropskih standardov: Stranke v Republiki Sloveniji listine podpisujejo z uporabo kvalificiranih digitalnih potrdil ali prek državne infrastrukture SI-PASS. V primeru mednarodnih ali čezmejnih sporov se upoštevajo določila Uredbe eIDAS (Uredba EU št. 910/2014), kar omogoča veljavno podpisovanje s tujo nacionalno e-identiteto.
3. Izvedba podpisa v realnem času: Po uskladitvi vsebine sporazuma na e-srečanju mediator generira končni dokument v PDF formatu in ga predstavi na zaslonu (funkcija Screen Sharing). Stranke dokument podpišejo na daljavo prek integrirane varne podpisne komponente ali pa si podpisan dokument zaporedno izmenjajo v roku, ki ga določi mediator, brez zapuščanja varnega e-okolja.

HRAMBA IN IZBRIS PODATKOV PO ZAKLJUČKU POSTOPKA

1. Vsa elektronska korespondenca, začasni osnutki in gradiva, ki so jih stranke posredovale tekom e-mediacije, se po zaključku postopka (bodisi z uspešnim sporazumom, neuspešno mediacijo ali prekinitvijo) varno arhivirajo v skladu z zakonskimi roki oziroma trajno izbrišejo iz lokalnih diskov in začasnih map e-platform, če zakonska podlaga za hrambo preneha.
2. Interni evidenčni zapisnik postopka, ki ga vodi mediator, ne sme vsebovati podrobnih vsebinskih navedb strank, ampak zgolj procesne podatke (identifikacijski podatki, datumi srečanj, izid postopka), kar je skladno z načelom zaupnosti.

3. Po zaključku mediacije mora mediator zagotoviti ustrezno hrambo oziroma izbris dokumentacije v skladu z načelom omejitve shranjevanja iz 5. člena GDPR ter obveznostmi glede zaupnosti iz 11. člena ZMCGZ. Hranijo se zgolj dokumenti, ki so nujni za dokazovanje izvedbe postopka, izpolnjevanje zakonskih obveznosti ali zaščito pravnih interesov udeležencev.
4. Dokumentacija se hrani v elektronski obliki na ustrezno zaščitenih informacijskih sistemih, ki zagotavljajo nadzor dostopa, šifriranje podatkov in redno varnostno kopiranje. Dostop do dokumentacije imajo le mediator in druge pooblaščen osebe, kadar je to potrebno zaradi izpolnjevanja zakonskih obveznosti. Vsa elektronska korespondenca, začasni delovni osnutki in gradiva, ki so jih stranke posredovale tekom e-mediacije, se po uradnem zaključku postopka (bodisi z uspešnim sporazumem ali neuspešno mediacijo) trajno izbrišejo iz lokalnih diskov računalnikov mediatorja in začasnih map uporabljenih e-platform, s čimer se prepreči kakršno koli kasnejše tveganje za razkritje podatkov.
5. Po poteku obdobja hrambe se dokumentacija trajno izbriše oziroma anonimizira na način, ki preprečuje ponovno identifikacijo posameznikov. Posnetki srečanj se praviloma ne ustvarjajo. Če bi bili izjemoma ustvarjeni na podlagi izrecnega soglasja vseh udeležencev, se po izpolnitvi namena obdelave nemudoma izbrišejo.
6. Mediator mora strankam na njihovo zahtevo zagotoviti informacije o obdelavi njihovih osebnih podatkov, obdobju hrambe ter pravicah, ki jim pripadajo po GDPR. S tem se zagotavljata transparentnost postopka in učinkovito varstvo zasebnosti vseh udeležencev e-mediacije.

Pregled ključne dokumentacije in tehničnih standardov

Tabela 1: osnovne procesne dokumentacije

Naziv dokumenta	Namen in pravna podlaga	Način potrditve / Podpis
Sporazum o vključitvi v mediacijo	Formalni vstop v postopek, opredelitev spora (3. člen ZMCGZ).	Kvalificirani elektronski podpis (KEP) / SI-PASS
Soglasje za digitalno izvedbo	Seznanjenost s tehničnim načinom dela in spletno platformo.	Potrditveno polje (Checkbox) ali elektronski podpis
Soglasje za obdelavo osebnih podatkov	Zakonnost zbiranja podatkov udeležencev (6. člen GDPR).	Klik ob registraciji v sistem
Izjava o zaupnosti	Zaveza o nesnemanju in varovanju informacij (11. člen ZMCGZ).	Elektronski podpis pred prvim srečanjem
Protokol izvedbe e-srečanja	Operativna pravila vodenja skupnih in ločenih virtualnih sob.	Interni akt (izvaja mediator)
Tehnična navodila za udeležence	Navodila za strojno opremo, krizni protokol ob prekinitvi.	Priloga k vabilu (v seznanitev)
Predlog / Osnutek sporazuma	Delovna različica sporazuma v PDF formatu za usklajevanje.	Pregled preko deljenja zaslona (Screen sharing)
Evidenčni interni zapis postopka	Dnevnik procesnih dejanj (brez vsebine pogajanj).	Vodi mediator (stranke nimajo dostopa)

Tabela 2: Tehnične rešitve in varnostni ukrepi

Področje	Tehnični standard / Varnostni ukrep	Operativni cilj v praksi
Izbira platforme	Namensko okolje z EU gostovanjem strežnikov + Breakout rooms.	Skladnost z GDPR in tehnična izolacija ločenih pogovorov.
Verifikacija identitete	SI-PASS enotna prijava + vizualni pregled dokumenta na kameri.	Preprečevanje lažne identitete in vstopa nepooblaščenih oseb.
Nadzor prostora	Možnost uporabe slušalk + možnost 360-stopinjskega pregleda sobe.	Zagotavljanje fizične zasebnosti v okolici stranke.
Zaščita komunikacije	End-to-End šifriranje (E2EE) + sistemska blokada snemanja.	Onemogočanje nepooblaščenega zajema avdio/video toka.
Krizni protokol	Pravilo 10 minut + takojšen prehod na telefonsko linijo.	Hitro in koordinirano reševanje tehničnih motenj povezave.