

PRAVILNIK O VAROVANJU OSEBNIH PODATKOV

pripravljen na podlagi Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov, v nadaljevanju: GDPR)

UVODNE DOLOČBE

1. člen

(namen in pravna narava pravilnika)

S tem pravilnikom se opredeljujejo tehnični in organizacijski ukrepi, s katerimi Judo klub Olimpija (v nadaljevanju klub) varuje osebne podatke.

Ukrepi iz prejšnjega odstavka se izvajajo z namenom, da:

- so osebni podatki obdelani zakonito, pošteno in na pregleden način;
- so osebni podatki zbrani za določene, izrecne in zakonite namene, in se ne obdelujejo na način, ki ni združljiv s temi nameni;
- se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave; ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost;
- se spoštujejo in zaščitijo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- se zagotovi varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo;
- lahko klub dokaže skladnost z zakonodajo s področja varstva osebnih podatkov.

Ta pravilnik poleg za zaposlene velja tudi za osebe, ki v klubu ali za klub opravljajo delo na podlagi pogodb, ki niso pogodbe o zaposlitvi, vključno z dijaki in študenti.

Katerakoli od oseb, navedenih v 3. ali 4. odstavku tega člena, je dolžna ob kakršnemkoli dvomu glede pomena določb tega pravilnika poiskati strokovno razlago oziroma pomoč pri zakonitem zastopniku kluba.

2. člen

(Opredelitev pojmov)

V tem pravilniku imajo izrazi »osebni podatek«, »posebne vrste osebnih podatkov«, »zbirka«, »obdelava«, »posameznik«, »upravljavec«, »obdelovalec«, »uporabnik«, »tretja oseba« in »privolitev posameznika, na katerega se nanašajo osebni podatki« enak pomen kot v GDPR.

»Nosilec podatkov« pomeni vse vrste sredstev, na katerih so zapisani ali posneti osebni podatki (listine, akti, gradiva, spisi, računalniška oprema, fotokopije, zvočno in slikovno gradivo, itd.).

»Zaposleni« pomeni osebe, ki imajo s klubom sklenjeno pogodbo o zaposlitvi, osebe, ki opravljajo delo v klubu kot dijaki ali študenti, osebe, ki opravljajo delo v klubu na podlagi pogodb civilnega prava.

»Varnostni incident« pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

3. člen

(Obdelava osebnih podatkov, varnost in obveščanje posameznikov)

V klubu oziroma za potrebe kluba se lahko obdelujejo le tisti osebni podatki, za katere obstaja ustrezna pravna podlaga po določbah GDPR ali druge zakonodaje.

Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo dalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.

Zbirka osebnih podatkov se vodi v katalogu članstva Judo kluba Olimpija. Vsi pooblaščen obdelovalci morajo biti pred obdelavo osebnih podatkov seznanjeni z določbami GDPR .

Posameznik ima pravico doseči, da klub brez nepotrebnega odlašanja popravi netočne oziroma dopolni nepopolne osebne podatke v zvezi z njim.

Posameznik ima pravico doseči, da klub brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, kadar velja eden od naslednjih razlogov:

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik prekliče privolitev, na podlagi katere poteka obdelava in za obdelavo ne obstaja nobena druga pravna podlaga;
- posameznik obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- osebni podatki so bili obdelani nezakonito;
- osebni podatki so bili zbrani v zvezi s ponudbo storitev informacijske družbe od mladoletnega posameznika.

Posameznik ima pravico doseči, da klub omeji obdelavo, kadar velja en od naslednjih primerov:

- posameznik oporeka točnosti podatkov, in sicer za obdobje, ki klubu omogoča preveriti točnost osebnih podatkov;
- je obdelava nezakonita in posameznik nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe;

- klub osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- je posameznik vložil ugovor v zvezi z obdelavo, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

UKREPI ZA VAROVANJE OSEBNIH PODATKOV

4. člen

(Varovanje prostorov in nosilcev podatkov)

Prostori, v katerih se nahajajo nosilci podatkov in strojna ter programska oprema (v nadaljnjem besedilu: varovani prostori), so varovani z organizacijskimi ter tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop v varovane prostore je mogoč in dopusten na podlagi dovoljenja zakonitega zastopnika kluba.

Varovani prostori ne smejo ostajati nenadzorovani oziroma jih je treba zaklepati ob odsotnosti zaposlenih, ki jih nadzorujejo.

V varovane prostore ne smejo brez spremstva ali prisotnosti zaposlenega, ki te prostore nadzoruje, vstopati osebe, ki niso zaposlene v društvu. Zaposleni, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ga ob zapustitvi zakleniti.

Vzdrževalci, čistilci, varnostniki, serviserji, obiskovalci, poslovni partnerji se smejo zadrževati v varovanih prostorih samo z vednostjo zaposlenih. Izven delovnega časa se lahko delavci, kot so čistilci ali varnostniki, če je to nujno potrebno, gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

Nosilci osebnih podatkov, hranjeni izven aktivnih delovnih prostorov oz. izven varovanih prostorov (hodniki, skupni prostori ipd.), morajo biti stalno zaklenjeni, razen kadar so neposredno v uporabi.

Posebnih vrst osebnih podatkov v nobenem primeru ni dovoljeno hraniti izven varovanih prostorov.

Zaposleni, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme nenadzorovano puščati nosilcev osebnih podatkov na pisalni mizi ali jih kako drugače izpostavljati nevarnosti, da bi nepooblaščene osebe dobile vpogled v osebne podatke.

Ključne, kartice, gesla in ostala sredstva, ki omogočajo dostop do varovanih prostorov, je treba varovati, upravljati in hraniti vestno in skrbno. Vsako izgubo ali odtujitev ali sum o zlorabi, mora zaposleni takoj sporočiti zakonitemu zastopniku, ki mora sprejeti ustrezne ukrepe.

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo zakonitega zastopnika kluba.

5. člen

(Obdelava osebnih podatkov)

Obdelava osebnih podatkov je dovoljena v prostorih kluba ali ob uporabi tehnologije dostopa na daljavo izven kluba, pri tem pa morajo biti zagotovljeni vsi potrebni ukrepi za zavarovanje osebnih podatkov, kakor so opredeljeni v tem Pravilniku.

VAROVANJE PROGRAMSKE OPREME ZA OBDELAVO OSEBNIH PODATKOV

6. člen

(Splošno)

Dostop do programske opreme, s katero ali s pomočjo katere se obdelujejo osebni podatki, mora biti varovan na način, ki dovoljuje dostop samo za to vnaprej določenim zaposlenim in osebam, ki za klub po pogodbi opravljajo servisiranje ali vzdrževanje strojne ali programske opreme, pri čemer si zaposleni med seboj ali s tretjimi osebami ne smejo izmenjevati ali razkrivati podatkov za dostop (ne glede na nivo pravic, ki jim je dodeljen).

Za dodeljevanje dostopa do programske opreme za zaposlene in vodenje evidence o tem je pristojno vodstvo kluba.

Popravljanje, spreminjanje in dopolnjevanje (posodabljanje) programske opreme oziroma sestava navodil v zvezi s tem so v pristojnosti vodstva kluba.

Zaposleni, ki v okviru svojih delovnih nalog ustvari ali dovoli ustvariti kopijo (baze) osebnih podatkov za namene servisiranja, popravila, spreminjanja ali dopolnjevanja programske opreme ali za nudenje podpore, je dolžan poskrbeti, da se, ko preneha potreba, kopija učinkovito uniči ali izbriše.

7. člen

(Hramba podatkov izven baz)

Osebni podatki se lahko zgolj izjemoma, kadar je to glede na naravo dela nujno potrebno, shranjujejo in obdelujejo lokalno (na lokalnih računalnikih in drugih podobnih napravah). Po prenehanju potrebe po takem shranjevanju in obdelavi

osebnih podatkov, se morajo osebni podatki prenesti v centralizirane baze podatkov ali pa se trajno izbrisati.

Morebitne kopije vsebin zbirk osebnih podatkov na lokalnih nosilcih (zunanji diski, USB-ključi in drugo) se hranijo v zaklenjenih omarah.

POGODBENA OBDELAVA OSEBNIH PODATKOV

8. člen

(Splošno)

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (obdelovalec), se sklene pisna pogodba, predvidena v 28. členu Splošne uredbe o varstvu podatkov. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

Obdelovalci smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen, k čemur se jih zaveže s pogodbo.

Obdelovalec mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

Poleg drugih zahtev si mora klub v pogodbah z obdelovalci zagotoviti pravico, da občasno pri pogodbenem obdelovalcu izvede pregled ali revizijo na področju varstva osebnih podatkov. Pregled ali revizijo je potrebno izvesti ob vsakem sumu ali indicu, da obdelovalec krši sklenjeno pogodbo ali da ne zagotavlja zadostne ravni varstva osebnih podatkov. Revizija se izvede na stroške kluba, pri čemer obdelovalec morebitnega angažmaja svojih ljudi in/ali podpogodbenih obdelovalcev društvu ne sme zaračunati.

BRISANJE, UNIČENJE IN ANONIMIZACIJA PODATKOV

9. člen

(Splošno)

Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe, če tega roka ni, pa toliko časa, kolikor določa zakon ali dokler traja pogodba (članstvo) s posameznikom, čigar podatki se obdelujejo, in še 5 let po njenem prenehanju, ali za čas, za katerega je posameznik privolil v obdelavo svojih osebnih podatkov ali

dokler ni dosežen namen obdelave. Rok hrambe za konkretne (baze) osebnih podatkov določi zakoniti zastopnik.

Podatki se hranijo na način in v obliki, ki omogoča dostop in obdelavo identifikacijskih podatkov zgolj za tisti čas, ki je nujno potreben za dosego namena, zaradi katerega se podatki zbirajo in/ali obdelujejo.

Osnovne kadrovske osebne podatke hranimo ves čas, dokler ima oseba status zaposlenega.

Osebne podatke, ki jih obdelujemo na podlagi članstva, hranimo trajno.

Podatke o izdanih računih hranimo 10 let od izdaje.

Po preteku roka hrambe se osebni podatki učinkovito izbrišejo, uničijo ali anonimizirajo, razen če zakon ali drug akt določa drugače. Uničenje, izbris ali anonimizacija osebnih podatkov odredi zakoniti zastopnik kluba. O uničenju, izbrisu ali anonimizaciji osebnih podatkov se napravi zapisnik, ki ne sme vsebovati osebnih podatkov posameznikov, katerih podatki so se izbrisali, uničili ali anonimizirali.

Za brisanje podatkov z računalnikov, strežnikov in podobnih naprav se uporabi takšna metoda brisanja, da je nemogoča rekonstrukcija brisanih podatkov.

Podatki na fizičnih nosilcih, ki jih ni mogoče izbrisati, se uničijo na način, ki zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv.

Prepovedano je odmetavati nosilce podatkov na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).

UKREPANJE OB VARNOSTNIH INCIDENTIH V ZVEZI Z OSEBNIMI PODATKI

14. člen

(Splošno)

Zaposleni so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik.

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščen uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti zakonitega zastopnika kluba, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.

Zakoniti zastopnik kluba mora ob vsakem sumu kršitve varstva osebnih podatkov takšno kršitev sporočiti Informacijskemu pooblaščenču v 72 urah. Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora zakoniti zastopnik poskrbeti za to, da

so prizadeti posamezniki brez nepotrebnega odlašanja obveščeni o tem, da je prišlo do kršitve varstva osebnih podatkov.

15. člen

(Interni ukrepi)

Zakoniti zastopnik kluba je dolžan poskrbeti za to, da se po varnostnem incidentu opravi analiza vzrokov in predlog ukrepov, ki naj zmanjšajo ali izničijo tveganje za take in bodoče varnostne incidente, ter da se, če je to smiselno in mogoče, predlagani ukrepi tudi izvedejo.

Če se izkaže, da je varnostni incident povzročil ali bil pri njem udeležen zaposleni ali je do varnostnega incidenta prišlo zaradi malomarnosti s strani zaposlenega, zakoniti zastopnik kluba, ne glede na ostale določbe tega pravilnika, sprejme ustrezne delovnopravne ukrepe zoper zaposlenega.

ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

16. člen

(Splošno)

Za nadzor nad izvajanjem postopkov in ukrepov za zavarovanje osebnih podatkov je odgovoren zakoniti zastopnik, ki lahko za posamezne naloge pooblasti druge osebe, ki niso zaposlene pri klubu.

Nadzor iz 1. odstavka tega člena vključuje tudi postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave. Pri tem so dolžni sodelovati vsi zaposleni in druge osebe v klubu.

Vsak, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, s katerimi je bil seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja ali pogodbe.

KONČNE DOLOČBE

17. člen

(Datum uveljavitve)

Ta pravilnik velja in se uporablja od 25.5.2018 naprej.

18. člen

(Objava, dostopnost)

Ta pravilnik se objavi na spletni www.judo-olimpija.com, vsem zaposlenim pa je na vpogled tudi v pisarni Judo kluba Olimpija, Celovška cesta 25, Ljubljana.

Pripravil: Judo klub Olimpija

Zadnja sprememba: 24. 5. 2018