

Na podlagi določil Splošne uredbe o varstvu osebnih podatkov (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016) in Zakona o varstvu osebnih podatkov ZVOP-2 (Uradni list RS, št. 163/22) je Občni zbor Študentskega kluba Kamnik, dne 22. 4. 2024 sprejel

## Pravilnik o varovanju osebnih podatkov

### 1. člen

#### (splošne določbe)

(1) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za varnost osebnih podatkov v Študentskem klubu Kamnik (v nadaljevanju: Klub) z namenom, da se prepreči slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščenno razkritje, dostop ali drugo nepooblaščenno obdelavo osebnih podatkov.

(2) Določbe tega pravilnika se smiselno uporabljajo tudi za varnost podatkov, ki so v dokumentaciji tehničnega in poslovnega značaja s strani Kluba in/ali zunanjih izvajalcev označeni kot poslovna skrivnost in/ali imajo oznako zaupno.

(3) Določbe tega pravilnika veljajo za člane organov Kluba in sodelavce Kluba ter zunanje izvajalce, ki pri svojem delu obdelujejo in uporabljajo osebne podatke. Za navedene osebe velja, da so seznanjene z vsakokrat veljavnimi predpisi s področja varstva osebnih podatkov, kot jih določa v nadaljevanju ta pravilnik.

### 2. člen

#### (uporaba spola)

V tem pravilniku uporabljeni izrazi, zapisani v moški spolni slovnični obliki, se uporabljajo kot nevtralen izraz za moške in ženske.

### 3. člen

#### (pomen izrazov)

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

a) **Osebni podatek** – katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

b) **Obdelava osebnih podatkov** – vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje.

p) **Poslovna skrivnost** – so podatki, ki so označeni z oznako zaupnosti v skladu z Zakonom o gospodarskih družbah.

#### **4. člen**

##### **(evidenca dejavnosti obdelav in vzpostavitve zbirke osebnih podatkov)**

- (1) Klub vodi evidenco dejavnosti obdelav. Del evidence dejavnosti obdelav so posamezne zbirke osebnih podatkov, katerih upravljavec ali obdelovalec je Klub.
- (2) Zbirko osebnih podatkov na posameznem delovnem področju Kluba vzpostavi odgovorna oseba za določeno zbirko osebnih podatkov (v nadaljevanju: odgovorna oseba), ki jo določi zakoniti zastopnik Kluba.
- (3) Člani organov Kluba in sodelavci, ki obdelujejo osebne podatke (v nadaljevanju: pooblaščen obdelovalci), morajo biti seznanjeni z evidenco dejavnosti obdelav, vpogled v evidenco dejavnosti obdelav osebnih podatkov pa je potrebno omogočiti vsakomur, ki to zahteva.
- (4) Zbirka osebnih podatkov v evidenci dejavnosti obdelav se dopolnjuje ob vsaki spremembi vrste osebnih podatkov.

#### **5. člen**

##### **(seznam zbirk osebnih podatkov)**

Klub je dolžen voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, kdo je odgovorna oseba za posamezno zbirko osebnih podatkov ter katere osebe so pooblaščen obdelovalci. V seznam se vpisujejo sledeči podatki:

- a) naziv zbirke osebnih podatkov,
- b) osebno ime in funkcija odgovorne osebe ter
- c) funkcija pooblaščenih obdelovalcev.

#### **6. člen**

##### **(obdelava osebnih podatkov)**

- (1) V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno pravno podlago, ki je določena v 6. členu Splošne uredbe (primer: zakon, privolitev posameznika, pogodba itd.).
- (2) Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, razen če zakon določa drugače.
- (3) Odgovorne osebe in pooblaščen obdelovalci morajo biti pred obdelavo osebnih podatkov seznanjene z določbami predpisov s področja varstva osebnih podatkov.
- (4) V primeru, da je pravna podlaga za obdelavo osebnih podatkov podana osebna privolitev posameznika, mora biti slednji obveščen o obdelavi osebnih podatkov na način kot določa 13. člen Splošne uredbe.
- (5) Obdelava osebnih podatkov lahko poteka na način, da se osebni podatki posameznikov psevdonimizirajo.

(3) Določbe 6. in 7. člena se smiselno uporabljajo tudi za posredovanje osebnih podatkov funkcionarjev znotraj Kluba.

## **9. člen**

### **(hramba osebnih podatkov)**

- (1) Osebnih podatki se lahko shranjujejo le toliko časa, kot je razvidno iz posamezne zbirke osebnih podatkov. Za brisanje/uničenje podatkov se uporabljajo določbe področne zakonodaje.
- (2) Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če zakon za posamezne vrste osebnih podatkov ne določa drugače.
- (3) Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča obnovitev vseh ali dela brisanih podatkov.
- (4) Osebnih podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja). Prepovedano je odmetavati odpadne nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).
- (5) Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa.

## **10. člen**

### **(varovanje prostorov)**

- (1) Klub ima poslovne prostore na naslovu Fužine 10, 1241 Kamnik. Vhod v poslovne prostore je varovan z vrati, ki se zaklepajo.
- (2) Nosilci osebnih podatkov se nahajajo v ustrezno varovanih prostorih/mestih, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
- (3) Varovani prostori morajo biti varovani s tehničnimi in organizacijskimi ukrepi, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščen razkritje, dostop ali drugo nepooblaščenno obdelavo.
- (4) Dostop v prostore je mogoč le v času uradnih ur, izven tega časa pa samo po predhodni odobritvi zakonitega zastopnika Kluba.
- (5) Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti oseb, ki so zadolžene za njihov nadzor.
- (6) V času odsotnosti oseb, odgovornih za varnost osebnih podatkov, morajo biti omare, pisalne mize in druga nahajališča nosilcev osebnih podatkov zaklenjeni, računalniki in druga strojna oprema izklopljeni in kako drugače fizično ali programsko zaklenjeni. Ključi se hranijo v skladu z navodili in se ne puščajo v ključavnici v vratih na zunanji strani vrat.
- (7) Funkcionarji in zunanji izvajalci ne smejo puščati nosilcev osebnih podatkov na mizah in drugih nezavarovanih mestih v prisotnosti oseb, ki nimajo pravice vpogleda v te podatke, nosilci podatkov in računalniški prikazovalniki pa morajo biti nameščeni tako, da nepooblaščenim osebam nimajo vpogleda vanje.
- (8) Vzdrževanje in popravila strojne računalniške in druge opreme lahko izvajajo pooblaščenih servisi in vzdrževalci, ki imajo s Klubom sklenjeno ustrezno pogodbeno razmerje.

- (3) Obdelovalec, ki za Klub opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.
- (4) Navedeno v 6. členu tega pravilnika velja tudi za pogodbene obdelovalce, ki vzdržujejo obstoječo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo.
- (5) Klub vodi seznam zunanjih izvajalcev, ki vsebuje:
  - a) naziv in sedež zunanjega izvajalca,
  - b) ime in priimek oseb, ki izvajajo zunanje storitve ter kontaktne podatke teh oseb (naslov e-pošte in telefonska številka).
- (6) Določbe tega pravilnika se smiselno uporabljajo tudi v primerih, ko je Klub obdelovalec osebnih podatkov.
- (7) Klub lahko za vsak primer pogodbene obdelave poda pisno privolitev, da se obdelava osebnih podatkov podeli v obdelavo drugemu obdelovalcu (podobdelava).

### 13. člen

#### **(ukrepanje ob sumu nepooblaščenega dostopa in obveščanje o kršitvah varnosti)**

- (1) Klub redno načrtuje, izvaja in upravlja procese, ki so potrebni za izpolnjevanje zahtev informacijske varnosti. V kolikor, kljub skrbnemu načrtovanju, izvajanju in upravljanju varnostnih procesov, pride do kršitve varstva osebnih podatkov, mora Klub reagirati na način in v rokih kot jih določa ta pravilnik.
- (2) Člani organov Kluba in sodelavci so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, nevestnim ravnanjem, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali ogrožanju celovitosti sistemov/strežnikov, odpovedovanje dostopnosti storitev (npr. denial of service – DOS/DDOS), spreminjanju ali okvari spletnih strani ali strežnikov, vdoru ali poizkusu vdora v sistem, prevari ipd. (v nadaljevanju: varnostni incident), nemudoma po zaznanem varnostnem incidentu obvestiti zakonitega zastopnika Kluba, sami pa poskušajo takšno aktivnost preprečiti. Prijava varnostnega incidenta se poda preko različnih kanalov (telefonski klic, elektronska pošta). V primeru, da se pri pregledu varnosti odkrije zlorabo pooblastil, mora biti o tem obveščen zakoniti zastopnik Kluba.
- (3) V kolikor se pri pregledu varnosti odkrije, da je za varnostni incident odgovoren član organa Kluba ali sodelavec Kluba, mora biti o tem obveščen zakoniti zastopnik Kluba.
- (4) Z nastankom varnostnega incidenta se začne voditi ažuren, natančen in verodostojen zapis incidentov (v nadaljevanju: dnevnik aktivnosti), ki vsebuje vse informacije in akcije, povezane z varnostnim incidentom. Za vsak vnos v dnevnik je potrebno dodati datum, čas in vir informacije.
- (5) Po končani aktivnosti osebe iz prejšnjega odstavka tega člena potrdijo odpravo incidenta. Vsi varnostni incidenti se beležijo v dokument »Varnostni incidenti«, ki je na strežniku Kluba dostopen osebam, ki opravljajo preiskave incidentov. Ni dovoljeno razkrivati podatkov o preiskavi, njenega namena, podrobnosti ali rezultatov nikomur, razen tistim, za katere zakoniti zastopnik Kluba odloči, da se jim lahko razkrije.
- (6) V kolikor je Klub upravljavec osebnih podatkov mora v primeru varnostnega incidenta, na podlagi 33. člena Splošne uredbe, obvestiti nadzorni organ najpozneje v 72 urah. V primeru, da je Klub obdelovalec osebnih podatkov, mora po seznanitvi z varnostnim incidentom brez nepotrebnega odlašanja uradno obvestiti upravljavca.

izvajalce pripravi izobraževanje na temo varnosti osebnih podatkov in tveganj, ki jim je Klub izpostavljen zaradi neizvajanja predmetnega pravilnika.

(5) Varnostna politika Kluba, veljavnost predmetnega pravilnika in njihovega izvajanja v praksi, se morajo redno (najmanj enkrat letno) preverjati in dokumentirati.

#### 16. člen

##### (končne določbe)

(1) Pravilnik stopi v veljavo naslednji dan po sprejetju tega pravilnika.

Kamnik, 22. 4. 2024

Predsednica Občnega zbora ŠKK,  
Maja Toni

