

Na podlagi Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 94/07) in Uredbe (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Ur. l. EU 119/1) izdaja Andrej Pompe, direktor FEBBS družba za izobraževanje d.o.o., matična št.: 3397467000, davčna št.: 19358032

## **PRAVILNIK O POSTOPKIH IN UKREPIH ZA ZAVAROVANJE OSEBNIH PODATKOV**

### **I. SPLOŠNE DOLOČBE**

#### **1. člen**

Vsebina in namen pravilnika

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov, ki se obdelujejo v FEBBS družba za izobraževanje d.o.o. (v nadaljevanju: FEBBS) z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava osebnih podatkov.

#### **2. člen**

Pomen izrazov

V tem pravilniku uporabljeni izrazi imajo pomen, kot določen v Uredbi (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Ur. l. EU 119/1) (v nadaljevanju: Splošna uredba o varstvu podatkov), in sicer na primer:

1. **Osebni podatek** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom, ne glede na obliko v kateri je izražen;
2. **Posebne vrste osebnih podatkov** pomenijo osebne podatke, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;
3. **Posameznik** pomeni določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njegovo fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov ali ne zahteva veliko časa;
4. **Upravljavec** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec

ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;

5. **Obdelovalec** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
6. **Uporabnik** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne;
7. **Obdelava** pomeni 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;
8. **Nosilec podatkov** pomeni vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, knjige, računalniška oprema, vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov ipd.).

### 3. člen

#### Uporaba pravilnika

Ta pravilnik velja za zaposlene v FEBBS, kakor tudi za osebe, ki v FEBBS opravljajo dela na podlagi pogodbe o delu, ter za dijake in študente, ki v FEBBS opravljajo dela preko napotnic oziroma prakso.

V zadevah, ki jih ne ureja ta pravilnik, se neposredno uporablja vsakokrat veljavni Zakon o varstvu osebnih podatkov in Splošna uredba o varstvu podatkov.

## II. OBDELAVA OSEBNIH PODATKOV

### 4. člen

#### Obdelava osebnih podatkov

FEBBS lahko obdeluje le tiste osebne podatke, za obdelavo katerih razpolaga z ustrežno zakonito podlago.

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, če zakon ne določa drugače.

Odgovorne osebe ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke (v nadaljevanju: pooblaščenči obdelovalci), morajo biti pred obdelavo osebnih podatkov seznanjene z določbami zakona, Splošne uredbe o varstvu podatkov ter z vsebino tega pravilnika in pri obdelavi osebnih podatkov zavezane k zaupnosti.

O seznanjenosti iz prejšnjega odstavka morajo osebe iz prejšnjega odstavka podpisati posebno izjavo, iz katere je razvidno, da je podpisnik seznanjen s predpisi iz prejšnjega odstavka.

### **III. ZAVAROVANJE OSEBNIH PODATKOV**

#### 5. člen

##### Varovani osebni podatki

Za varovane osebne podatke štejejo katerekoli informacije, v zvezi z določenim ali določljivim posameznikom, ne glede na obliko v kateri so izražene.

FEBBS pri sprejetju varnostnih ukrepov in postopkov upošteva naravo osebnih podatkov in stopnjo tveganja, ki ga pomeni obdelava, zlasti zaradi nenamerne ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov.

#### 6. člen

##### Varovanje prostorov

Prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke, strojna in programska oprema (v nadaljevanju: varovani prostori), morajo biti varovani z organizacijskimi in/ali tehničnimi ukrepi iz tega pravilnika, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Varovani prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo posebne vrste osebnih podatkov, morajo biti varovani tako, da je zagotovljen popolni nadzor nad delom in gibanjem v teh prostorih.

Pisarne morajo biti stalno pod nadzorom zaposlenih, ki v njih delajo. Ob odsotnosti mora zaposleni pisarno zakleniti. Ključi se ne smejo puščati v ključavnici v vratih.

V varovanih prostorih morajo biti po zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke, zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.

Omare, mize in drugo pohištvo z nosilci podatkov, ki vsebujejo osebne podatke, ki se nahajajo izven varovanih prostorov (hodniki, skupni prostori) mora biti stalno zaklenjeno.

Osebe, ki niso zaposlene v FEBBS (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji) se smejo gibati v varovanih prostorih samo z vednostjo zaposlenega, ki nadzoruje varovani prostor, kjer se oseba giba.

Zaposleni, kot so čistilke, varnostniki idr., se lahko izven delovnega časa 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).

#### 7. člen

##### Varovanje nosilcev podatkov, ki vsebujejo osebne podatke

Zaposleni v FEBBS ne smejo puščati nosilcev podatkov, ki vsebujejo osebne podatke, na vidnem mestu (npr. na mizah) v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci podatkov, ki vsebujejo posebnih vrst osebnih podatkov, se ne smejo hraniti izven varovanih prostorov.

Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni v FEBBS odnašajo izven prostorov **FEBBS** samo z dovoljenjem direktorja FEBBS.

Nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, zaposleni v **FEBBS** ne smejo odnašati izven prostorov FEBBS, razen izjemoma z dovoljenjem direktorja FEBBS, če je to nujno potrebno za reševanje zadeve, ki vsebuje te osebne podatke.

V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov, ki vsebujejo osebne podatke, in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

#### 8. člen

##### Varovanje strojne in programske opreme

Vzdrževanje in popravila strojne računalniške in druge opreme so dovoljena samo z odobritvijo osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščenih servisi in vzdrževalci, ki imajo z FEBBS sklenjeno ustrezno pogodbo.

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo zaposlenim v FEBBS ali pravnim in fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščenih servisi in organizacije ter posamezniki, ki imajo z FEBBS sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme ustrezno dokumentirati.

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega pravilnika.

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se vsakodnevno preveri z vidika prisotnosti računalniških virusov. Ob pojavu

računalniškega virusa se tega čim prej odpravi s pomočjo ustrezne strokovne službe, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu FEBBS.

Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo na **FEBBS** na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo preverjeni z vidika prisotnosti računalniških virusov.

Zaposleni v FEBBS ne smejo inštalirati programske opreme in odnašati programske opreme iz prostorov **FEBBS** brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil.

Oseba, zadolžena za delovanje računalniškega informacijskega sistema, določi način dodeljevanja, hranjenja in spreminjanja gesel in o tem seznanji vse zaposlene v FEBBS.

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervisorska gesla), administriranje elektronske pošte in administriranje aplikativnih programov, se hranijo v zapečatenih ovojnica in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki nahajajo tam.

Kopije iz prejšnjega odstavka se hranijo na za to določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

#### **IV. POSREDOVANJE OSEBNIH PODATKOV**

##### 9. člen

##### Posredovanje osebnih podatkov

Osebni podatki se na zahtevo uporabnika posredujejo samo tistim uporabnikom, ki se izkažejo z ustrežno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

Posredovanje osebnih podatkov iz prejšnjega odstavka lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne zahteve mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k zahtevi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščen obdelovalec v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.

Posredovanje občutljivih osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna zahteva mora biti po vsebini enaka pisni zahtevi iz prejšnjega odstavka.

Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

Osebne podatke je dovoljeno posredovati z informacijskimi, komunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Ne glede na prejšnji odstavek je občutljive osebne podatke dovoljeno posredovati preko komunikacijskih omrežij le, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

Če se posreduje originalni dokument, ki vsebuje osebne podatke, mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

#### 10. člen Evidenca posredovanj

Vsako posredovanje osebnih podatkov iz prejšnjega člena se zaznamuje z navedbo naslednjih podatkov:

- kateri osebni podatki so bili posredovani,
- osebno ime/firno/ime in naslov/sedež osebe, ki so ji bili posredovani osebni podatki,
- datum in ura posredovanja osebnih podatkov ter
- podlaga, na kateri so bili posredovani osebni podatki.

Zaznamek iz prejšnjega odstavka se v pisni ali elektronski obliki, odvisno od nosilca podatkov, ki vsebuje posredovani osebni podatek, evidentira v zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek, v posebno rubriko "Evidenca posredovanj osebnih podatkov".

Zaznamek iz prvega odstavka tega člena naredi odgovorna oseba ali pooblaščen obdelovalec, ki je osebne podatke posredoval uporabniku.

## 11. člen

### Posredovanje osebnih podatkov znotraj upravljavca osebnih podatkov

Dokumenti, ki vsebujejo osebne podatke zaposlenega v FEBBS, se zaposlenemu, na katerega se osebni podatki nanašajo, posredujejo v skladu z 10. členom tega pravilnika.

Osebni podatki zaposlenih v FEBBS in ostalih oseb se lahko posredujejo znotraj **FEBBS** tistim osebam, ki jih potrebujejo v okviru opravljanja svojih del in nalog.

Oseba iz tretjega odstavka 10. člena mora zaznamovati vsako posredovanje posebnih vrst osebnih podatkov znotraj FEBBS v skladu s prejšnjim členom.

## V. HRAMBA OSEBNIH PODATKOV

## 12. člen

### Hramba osebnih podatkov

Osebni podatki se lahko shranjujejo le toliko časa, kolikor je to potrebno, da se doseže namen, za katerega se zbirajo in vodijo oziroma po poteku zakonsko določenega roka. Po prenehanju potrebe po vodenju osebnih podatkov, se podatki zbršejo oziroma anonimizirajo. Morebitne kopije osebnih podatkov se izbrišejo najkasneje v 90 dneh od izpolnitve namena, za katerega so bili zbrani in uporabljeni oziroma od poteka zakonsko določenega roka.

Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug predpis za posamezne vrste osebnih podatkov ne določa drugače.

Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča rekonstrukcija vseh ali dela brisanih podatkov.

Osebni podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja).

Uničenje nosilcev podatkov in pomožnega gradiva se zagotovi v skladu tretjim in četrtem odstavkom tega člena.

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

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov.

Prenos nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, na mesto uničenja ter uničevanje takih nosilcev podatkov nadzoruje posebna tričlanska komisija, ki jo imenuje direktor upravljavca osebnih podatkov.

Komisijo iz prejšnjega odstavka sestavljajo zaposleni v **FEBBS**, pri čemer je en član komisije odgovorna oseba. O uničenju iz osmega odstavka tega člena komisija sestavi ustrezen zapisnik.

#### 13. člen

##### Hramba in roki hrambe zbirk osebnih podatkov

Za hrambo zbirk osebnih podatkov je odgovoren direktor FEBBS.

## VI. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

#### 14. člen

##### Pogodbena obdelava

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (v nadaljevanju: pogodbeni obdelovalec), **FEBBS** sklene pisno pogodbo s sestavinami kot določenimi v 28. členu Splošne uredbe o varstvu podatkov.

**FEBBS** s pogodbenim obdelovalcem sklene pogodbo zgolj ob izkazanem jamstvu, da ima pogodbeni obdelovalec implementirane vse ustrezne ukrepe za varstvo osebnih podatkov in izpolnjuje svoje dolžnosti, kot jih določa vsakokrat veljavna zakonodaja in Splošna uredba o varstvu podatkov ter ta pravilnik.

Pogodbeni obdelovalci lahko opravljajo storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe iz prvega odstavka tega člena in dokumentiranih navodil FEBBS ter podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

## VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

#### 15. člen

##### Obveščanje

Zaposleni pri upravljavcu osebnih podatkov so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti odgovorno osebo ali nadrejenega, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.



Odgovorna oseba oziroma nadrejeni mora ob vsakem sumu kršitve varstva osebnih podatkov takšno kršitev sporočiti državnemu nadzornemu organu za varstvo osebnih podatkov, v primeru suma storitve kaznivega dejanja pa policiji ali tožilstvu.

## **VIII. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA ZAVAROVANJE OSEBNIH PODATKOV**

### 16. člen

#### Izvajanje postopkov in ukrepov

Vsak, ki obdeluje osebne podatke, je dolžan izvajati s tem pravilnikom predpisane postopke in ukrepe za zavarovanje osebnih podatkov in varovati osebne podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

### 17. člen

#### Odgovornost za izvajanje in nadzor nad izvajanjem

Direktor FEBBS je odgovoren za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov, določenih s tem pravilnikom.

### 18. člen

#### Izjava

Pred nastopom dela na delovnem mestu, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami zakona, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega pravilnika in zakona.

### 19. člen

#### Odgovornost za kršitev

Za kršitev določil iz tega pravilnika so zaposleni pri upravljavcu osebnih podatkov disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

Odgovornost iz prejšnjega odstavka ne izključuje prekrškovne, kazenske ali odškodninske odgovornosti.

## **IX. KONČNE DOLOČBE**

20. člen  
Veljavnost pravilnika

Ta pravilnik začne veljati 15. dan po podpisu.

Spremembe tega pravilnika so veljavne, v kolikor so sprejete v pisni obliki.

V Ljubljani, dne 26.4.2018

---

Andrej Pompe, direktor

**FEBBS d.o.o.**  
Dunajska 5, 1000 Ljubljana  
SLOVENIA 1

