Svet zavoda

Univerze Sigmunda Freuda Dunaj - podružnica Ljubljana

je na svoji seji dne 4. 4. 2023 sprejel

PRAVILNIK O VARSTVU IN VAROVANJU OSEBNIH PODATKOV

Univerze Sigmunda Freuda Dunaj - podružnica Ljubljana (SFU Ljubljana)

I. SPLOŠNE DOLOČBE

1. člen

[I] Univerza Sigmunda Freuda Dunaj – podružnica Ljubljana (v nadaljevanju: SFU LJUBLJANA) z namenom zagotavljanja varstva osebnih podatkov in skladnosti varstva osebnih podatkov z določbami in standardi Splošne uredbe o varstvu osebnih podatkov (GDPR) ter Zakona o varstvu osebnih podatkov (ZVOP-2) s Pravilnikom o varstvu osebnih podatkov (v nadaljevanju: Pravilnik) določa administrativne, organizacijske in tehnične postopke ter ukrepe.

[II] Postopki in ukrepi se sprejemajo, da se prepreči slučajno ali namerno nepooblaščeno obdelava osebnih podatkov, njihova sprememba, uničenje, uporaba (zloraba) ali posredovanje.

[III] Zaposleni in zunanji sodelavci SFU LJUBLJANA, ki pri svojem delu obdelujejo in uporabljajo osebne in zaupne podatke SFU LJUBLJANA, so pri svojem delu zavezani spoštovati določbe GDPR in ZVOP-2 in zagotavljati standarde ravnanja z osebnimi podatki in varstva osebnih podatkov, kot jih določa Pravilnik.

2. člen

[I] V Pravilniku uporabljeni izrazi imajo naslednji pomen:

1. »osebni podatki« pomenijo katero koli informacijo v zvezi z določenim ali določljivim posameznikom;
2. »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, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
3. »obdelava osebnih podatkov« pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave);
4. »upravljavec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave;
5. »obdelovalec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

6. »pooblaščena oseba za varstvo osebnih podatkov (v nadaljevanju: DPO)« je oseba, ki upravljavcu ali obdelovalcu na neodvisen način svetuje pri zagotavljanju skladnosti z GDPR, ZVOP-2 in zakonodajo na področju varstva osebnih podatkov;

7. »privolitev posameznika, na katerega se nanašajo osebni podatki« pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj;

8. »posebne vrste osebnih podatkov« so osebni podatki, 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;

9. »storitev informacijske družbe« je katerakoli storitev, ki se običajno opravi odplačno, na daljavo (storitev se opravi, ne da bi bile stranke sočasno navzoče), elektronsko (storitev se pošlje na začetnem kraju in sprejme na cilju z elektronsko opremo za obdelavo in shranjevanje podatkov ter se v celoti prenaša, pošilja in sprejema po žici, radijsko, z optičnimi ali drugimi elektromagnetnimi sredstvi) in na posamezno zahtevo prejemnika storitev (storitev opravi s prenosom podatkov na posamezno zahtevo);

10. »pogodbeni obdelovalci« so vsi pogodbeno sodelujoči s SFU LJUBLJANA, ki se na podlagi privolitve zaposlenih, študentov ali klientov SFU LJUBLJANA v najmanjšem obsegu in na s pogodbo predviden zakonit način lahko seznanijo z osebnimi podatki ter so jih dolžni varovati;

11. »najmanjši obseg obdelave« pomeni obdelavo, ki za zakonit namen ob zagotovljenem varstvu ustrezno uporablja najmanjšo relevantno kategorijo osebnih podatkov;

12. »varnostni dogodek« je dogodek, ki ima vpliv na varnost osebnih podatkov in dogodek, ki predstavlja kršitev varnosti osebnih podatkov.

3. člen

Vsebina varstva osebnih podatkov iz 1. člena Pravilnika se dopolnjuje z uporabo internih povezanih aktov ali dokumentov:

- Evidenca dejavnosti obdelave za vodenje evidenc vrste obdelave osebnih podatkov;

- Dnevnik obdelave: za vodenje dejanskih obdelav osebnih podatkov v primeru
  1. vpogleda zaradi odločanja o pravicah in dolžnostih posameznikov
  2. spreminjanju osebnih podatkov
  3. upravičenega prenosa osebnih podatkov
  4. uničenja osebnih podatkov
  5. zakonitega razkritja podatkov tretjim osebam, ki izkažejo zakoniti interes
  6. ostalih v internih aktih predvidenih primerih

- Dokumenti v zvezi z raziskavami: če se osebni podatki zbiranju v znanstveni-raziskovalne namene;

- Ocena učinkov dejavnosti obdelave posebnih vrste osebnih podatkov.

II. VRSTE OSEBNIH PODATKOV

4. člen

[I] SFU LJUBLJANA za kategorije posameznikov obdeluje naslednje vrste osebnih podatkov (v nadaljevanju: osebni podatki):

1. Zaposleni: ime in priimek, datum rojstva, naslov stalnega prebivališča, naslov začasnega prebivališča, naslov elektronske pošte, telefonska številka, EMŠO, davčna številka, številka transakcijskega računa, podatek o sedanjem delovnem mestu in prejšnjih delovnih mestih, podatki o vrsti in ravni izobrazbe, funkcionalnem in specialnem znanju, udeležbi na različnih oblikah izpopolnjevanja in usposabljanja in o opravljenih strokovnih izpitih in preizkusih znanja ter drugi podatki o strokovni usposobljenosti, podatek o prejšnjih delovnih razmerjih, delovno dobi, pokojninski dobi, podatki o dokončno ugotovljeni disciplinski in odškodninski odgovornosti, podatki o dokončni ugotovitvi nesposobnosti, podatki opravljenih preventivnih zdravstvenih pregledih, podatki o telesni okvari ali invalidnosti, podatki o delni upokojitvi, identifikacijski podatki o otrocih, mlajših od 10 ali 15 let oziroma družinskih članih, za katere zaposleni uveljavlja davčno olajšavo, podatki o prenehanju delovnega razmerja – razlog in datum prenehanja, kratek življenjepis, če s tem zaposleni soglaša.

2. Študenti: ime in priimek, datum rojstva, naslov stalnega prebivališča, naslov začasnega prebivališča, e-mail naslov, telefonska številka, EMŠO, davčna številka, številka transakcijskega računa, podatki o vrsti in ravni dosežene izobrazbe, funkcionalnem in specialnem znanju, udeležbi na različnih oblikah izpopolnjevanja in usposabljanja in o opravljenih strokovnih izpitih in preizkusih znanja, zdravstveni podatki, ki vplivajo na izvajanje študija, ostali osebni podatki, pridobljeni na podlagi spremljanja študenta skozi študijski proces.

3. Klienti ambulante: spol, ime in priimek, naslov stalnega prebivališča, naslov začasnega prebivališča, e-mail naslov, telefonska številka, datum rojstva, kraj rojstva, najvišja do sedaj dosežena stopnja izobrazbe, psevdonimizirani zapisi, avdio in video snemanja, opazovanje psihološkega svetovanja s strani študentov.

4. Zunanji sodelavci: ime in priimek, naslov stalnega prebivališča, naslov začasnega prebivališča, e-mail naslov, telefonska številka, EMŠO, davčna številka, številka transakcijskega računa, podatek o sedanjem delovnem mestu in prejšnjih delovnih mestih, podatki o vrsti in ravni izobrazbe, funkcionalnem in specialnem znanju, udeležbi na različnih oblikah izpopolnjevanja in usposabljanja in o opravljenih strokovnih izpitih in preizkusih znanja ter drugi podatki o strokovni usposobljenosti, kratek življenjepis, če s tem zaposleni soglaša.

III. VARSTVO IN VAROVANJE OSEBNIH PODATKOV

5. člen

[I] Varstvo in varovanje osebnih podatkov obsega administrativne, organizacijske in tehnične postopke ter ukrepe, s katerimi se na podlagi tega Pravilnika, GDPR in ZVOP-2 izvaja:

- varstvo posebnih vrst osebnih podatkov;

- varstvo fizičnega in omrežnega dostop do prostorov, kjer se obdelujejo osebni podatki in varstvo nosilcev osebnih podatkov (notranji in zunanji računalniški diski, storitve v oblaku, ostali podatkovni nosilci);

- varstvo sistemske in programske opreme za obdelavo osebnih podatkov;

- varstvo prenosov (sprejem in oddaja) osebnih podatkov;

- varstvo v primeru obdelave osebnih podatkov s strani zunanjih obdelovalcev ter

- varstvo pri brisanju oziroma uničenju osebnih podatkov.

[II] Varstvo in varovanje osebnih podatkov se nanaša tudi na ravnanja v primeru ugotovitve zlorab ali fizičnih ali kibernetskih vdorov v informacijski sistem SFU LJUBLJANA (Protokol v primeru varnostnih dogodkov).

[III] Cilj ukrepov je zmanjševanje verjetnosti zlorabe osebnih podatkov in kršitev s področja varstva osebnih podatkov.

Varstvo posebnih vrst osebnih podatkov

6. člen

[I] Posebne vrste osebnih podatkov se, v kolikor je smiselno vodijo, ločeno od ostalih osebnih podatkov in omogočati obdelavo samo odgovornemu strokovnjaku, za katerega velja obveznost varovanja poklicne skrivnosti (v nadaljevanju: odgovorni strokovnjak).

[II] Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovana s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena neberljivost podatkov med njihovim prenosom, njihov prejemnik pa je strokovnjak, za katerega velja obveznost varovanja poklicne skrivnosti.

[III] V kolikor je učinkovita obdelava osebnih podatkov možna že tako, da se podatki anonimizirajo, se ti posredujejo v anonimizirani obliki.

[IV] Posebne vrste osebnih podatkov se lahko v izvirniku dajo na vpogled samo strokovnjaku, za katerega velja obveznost varovanja poklicne skrivnosti, pod nadzorstvom odgovornega strokovnjaka.

[V] Posebne vrste osebnih podatkov v papirnati obliki se morajo po obdelavi shranjevati v ognjevarnih in zaklenjenih omarah.

[VI] Posebne vrste osebnih podatkov se v elektronski obliki lahko nahajajo samo na mestu izvirnika. Po obdelavi posebne vrste osebnih podatkov v elektronski obliki se morajo na ostalih elektronskih mestih izbrisati, razen v primeru redundantne lokacije.

Dostopi

7. člen

[I] Prostori, kjer se nahajajo osebni podatki ali nosilci osebnih podatkov, sodijo v kategorijo ''Varovanih prostorov''. Na SFU LJUBLJANA so to prostori, kjer se nahaja: vodstvo, tajništvo, referat za študijske in študentske zadeve, finančno računovodska služba, ambulanta in arhiv. Ti prostori morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov in za katere velja naslednji režim:

1. Dostop v varovane prostore je mogoč samo za zaposlene in posebej pooblaščene osebe.
2. Dostop osebam, ki niso zaposlene v varovanih prostorih, je dovoljen le v prisotnosti zaposlenega delavca v teh prostorih ali v slučaju višje sile (požar, izlitje vode, nujna vzdrževalna dela) ob prisotnosti varnostnika.
3. Delavci v varovanih prostorih morajo prostor vestno in skrbno nadzorovati in ob vsaki odsotnosti zakleniti.
4. Nosilcev osebnih podatkov ne smejo izpostavljati nevarnosti nenadzorovanega vpogleda ali iznosa.
5. Osebni podatki, ki se hranijo izven varovanih prostorov, morajo biti shranjeni v zaklenjeni ognjevarni omari.
6. Vsi računalniki, na katerih se nahajajo osebni podatki, morajo biti v času vsake odsotnosti delavca zadolženega za delo z osebnimi podatki fizično ali programsko zaklenjeni.
7. Nosilci osebnih podatkov, hranjeni izven aktivnih delovnih prostorov oziroma izven varovanih prostorov (hodniki, skupni prostori, aktivni in pasivni arhivi ipd.), morajo biti stalno zaklenjeni v ognjevarni zaščiteni omari.
8. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor.
9. Delavec, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma delavcem.

10. V prostorih, v katere imajo vstop študenti ali osebe, ki niso zaposlene na SFU LJUBLJANA, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je strankam onemogočen vpogled vanje.

[II] Obdelovanje osebnih podatkov je dovoljeno le v prostorih SFU LJUBLJANA. Nosilcev osebnih podatkov delavci SFU LJUBLJANA ne smejo odnašati izven prostorov SFU LJUBLJANA brez izrecnega dovoljenja člana Sveta zavoda SFU LJUBLJANA ali osebe, ki jo ta pooblasti.

8. člen

[I] Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo člana Sveta zavoda ali od njega pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in njihovi vzdrževalci, ki imajo s SFU LJUBLJANA sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme.

[II] Osebe iz zgoraj navedenega odstavka morajo pri izvajanju opravil vzdrževati raven varstva osebnih podatkov, ki ustreza ravni varstva osebnih podatkov SFU LJUBLJANA.

9. člen

[I] Vzdrževalci prostorov in druge opreme v varovanih prostorih, poslovni partnerji, drugi obiskovalci in študenti, se smejo gibati v varovanih prostorih le ob prisotnosti delavca.

[II] Zaposleni, tehnično-vzdrževalni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti odgovornega delavca le, če so nosilci podatkov shranjeni v zaklenjenih omarah na način, ki ga določa ta Pravilnik za čas izven delovnega časa.

10. člen

Dostop do računalniške programske opreme mora biti varovan na način, ki omogoča dostop samo določenim pooblaščenim delavcem in delavcem, ki za SFU LJUBLJANA po pogodbi opravljajo servisiranje računalniške in programske opreme.

11. člen

[I] Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve člana Sveta zavoda oziroma od njega pooblaščene osebe, izvajajo

pa ga lahko samo pooblaščeni servis in organizacije oziroma njihovi delavci, ki imajo s SFU LJUBLJANA sklenjeno ustrezno pogodbo.

[II] Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati ter na zahtevo dati na vpogled in v kopiranje za to pristojnemu delavcu SFU LJUBLJANA. Tovrstna dokumentacija se vnese v Dnevnik obdelave.

12. člen

[I] Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz Pravilnika.

[II] Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske ali aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

[III] Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora biti v času servisiranja računalnika in programske opreme ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki. V kolikor delavec v času servisiranja ne more biti prisoten, mora za to določiti namestnika.

[IV] V primeru, da se pokaže potreba po popravilu računalnika, na čigar disku se nahajajo osebni podatki, izven SFU LJUBLJANA in brez kontrole pooblaščenega delavca, se morajo podatki iz diska računalnika na varen način prenesti na drug disk ter iz računalnika za popravilo izbrisati na način, ki onemogoča restavracijo. Če tak izbris ni mogoč, se mora popravilo opraviti v prostorih SFU LJUBLJANA v prisotnosti pooblaščenega delavca.

[V] Vsaka tovrstna sprememba se mora vnesti v Dnevnik obdelave.

Varstvo sistemske in programske opreme

13. člen

[I] Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se preverja glede na prisotnost škodljive programske opreme (v nadaljevanju: ŠPO) v skladu z Načrtom preverjanja. Ob pojavu ŠPO je potrebno storiti vse, da se s pomočjo strokovnjakov ta izbriše in da se ugotovi vzrok pojava ŠPO in v prihodnje odpravijo oziroma omejijo tveganja za pojavljanje.

[II] Vsi podatki in programska oprema, ki so namenjeni uporabi na računalnikih SFU LJUBLJANA in v računalniškem informacijskem sistemu SFU LJUBLJANA in prispejo na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

14. člen

Zaposleni delavci lahko programsko opremo namestijo samo z dovoljenjem člana Sveta zavoda ali od njega pooblaščene osebe.

15. člen

Dostop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Svet zavoda na predlog sodelujočega informatika določi režim dodeljevanja, hranjenja in spreminjanja gesel.

16. člen

[I] Vsa gesla in postopki, ki se uporabljajo za dostop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto, administriranje prek aplikativnih programov, spletna banke in gesla za dostope do osebnih računalnik se hranijo v posebej označenih ovojnicah in varujejo v ognjevarni omari v prostorih SFU LJUBLJANA.

[II] Varovana gesla, hranjena v posebej označenih ovojnicah, se smejo uporabiti za vnaprej določene namene.

[III] Svet zavoda na predlog informatika določi nova gesla.

17. člen

[I] Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov mora SFU LJUBLJANA redno izdelovati kopije vsebine zbirk osebnih podatkov.

[II] Računalniške kopije vsebin zbirk osebnih podatkov se po obdelavi hranijo v strežniškem sistemu in na redundantni lokaciji, ki jo s sklepom določi Svet zavoda.

[III] Strežniški (diskovni) sistem mora biti ustrezno varovan in zavarovan, tako da onemogoča neposreden fizični dostop nepooblaščenim osebam, nepooblaščeno kopiranje podatkov s strežnika. Prav tako mora biti strežniški sistem vzdrževan v primernih klimatskih in varnostnih razmerah.

Prenos (sprejem in oddaja) osebnih podatkov

18. člen

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli Svet zavoda in posredovanje vpiše v Dnevnik obdelave osebnih podatkov.

19. člen

[I] Osebni podatki zaposlenih in študentov iz 3. člena Pravilnika se posredujejo SFU Dunaj kot matični ustanovi SFU LJUBLJANA v notranje upravne namene, kot so vodenje kadrovskih in visokošolskih evidenc.

[II] SFU Dunaj mora zagotavljati najmanj raven varnosti osebnih podatkov, ki je za SFU LJUBLJANA predvidena v tem Pravilniku, ob upoštevanju GDPR in ostale zakonodaje na področju varovanja osebnih podatkov.

[III] Za uresničevanje nalog iz tega člena Pravilnika se DPO SFU LJUBLJANA in DPO SFU Dunaj redno obveščata in sodelujeta.

20. člen

[I] Zaposleni, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

[II] Zaposleni, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo na SFU LJUBLJANA.

[III] Zaposleni, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis.

[IV] Zaposleni, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega položaja in šele nato naslov SFU LJUBLJANA.

21. člen

Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in podobnimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

22. člen

[I] Za pošiljanje osebnih podatkov po elektronski poti je potrebno zagotoviti:

- uporabo varne elektronske pošte, ki omogoča šifriranje sporočila in priloge;

- avtentikacijo prejemnika z zahtevanjem preverjanja identitete prejemnika ali z uporabo drugih varnostnih ukrepov, kot so na primer gesla ali šifre za dostop do zaščitenega območja ter

- omejitev uporabe osebnih podatkov (ali so podatki potrebni za namen, za katerega jih pošiljate, ter ali so ustrezno zaščiteni).

[II] V primeru pošiljanja posebnih vrste osebnih podatkov je potrebno uporabiti dodatne varnostne ukrepe, kot je na primer dvojna avtentikacija ali dodatni varnostni protokoli.

[III] Osebni podatki morajo biti med pošiljanjem ves čas varovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

23. člen

Za pošiljanje osebnih podatkov po pošti, kurirju ali kurirski službi je potrebno zagotoviti, da:

- se pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi z vročilnico ali priporočeno;
- je ovojnica, v kateri se posredujejo osebni podatki, izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice, pri čemer mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice;
- je obdelava občutljivih osebnih podatkov posebej označena in zavarovana.

24. člen

[I] Osebni podatki se lahko posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

[II] Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

[III] Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

[IV] Vsak prenos osebnih podatkov je potrebno zabeležiti v Dnevnik obdelave osebnih podatkov.

Obdelava osebnih podatkov s strani pogodbenega obdelovalca

25. člen

[I] Z vsako zunanjo osebo (pravno ali fizično), ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov SFU LJUBLJANA in je registrirana za opravljanje takšne dejavnosti, se sklene pogodba. V pogodbi se skladno s Pravilnikom, GDPR in

ZVOP-2 določijo tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in namestijo novo strojno ali programsko opremo.

[II] Pogodbeni obdelovalci smejo opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil SFU LJUBLJANA in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

[III] Pogodbeni obdelovalec, ki opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti v skladu z GDPR in ZVOP-2 vsaj enako strog način varstva osebnih podatkov, kot ga določa Pravilnik.

[IV] SFU LJUBLJANA lahko od pogodbenega obdelovalca zahteva, da izkaže način varstva osebnih podatkov iz zgornjega odstavka.

Brisanje in uničenje osebnih podatkov

26. člen

[I] Osebni podatki se lahko hranijo le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo oziroma dokler za to obstaja veljavna pravna podlaga.

[II] Po prenehanju potrebe po vodenju osebnih podatkov, se podatki zbrišejo oziroma uničijo nosilci podatkov.

27. člen

[I] Brisanje osebnih podatkov na elektronskih medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov.

[II] Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (pokurijo, razrežejo) v prostorih univerze ali pod nadzorom pooblaščenega delavca SFU LJUBLJANA pri organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije.

[III] Izbris ali uničenje se vnese v Dnevnik obdelave osebnih podatkov, v katerega se prav tako vpiše izbris in uničenje osebnih podatkov.

28. člen

[I] Z vso vestnostjo in skrbnostjo, določeno s Pravilnikom, se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

[II] Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

[III] Izbris ali uničenje pomožne dokumentacije ali računalniških produktov ali predlog se vnese v Dnevnik obdelave osebnih podatkov, v katerega se prav tako vpiše izbris in uničenje osebnih podatkov.

IV. PROTOKOL V PRIMERU VARNOSTNIH DOGODKOV

29. člen

[I] Vsi zaposleni in zunanji sodelavci 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, GDPR in ZVOP-2.

[II] Zaposleni ali zunanji sodelavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov (skupno v nadaljevanju: kršitve VOP), mora takoj in najkasneje v 12 urah o tem obvestiti osebo, pooblaščeno za varstvo osebnih podatkov (v nadaljevanju: DPO) ali člana Sveta zavoda, ti pa naprej o varnostnem dogodku obvestijo pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je vdrlo.

[III] SFU LJUBLJANA o kršitvah VOP najkasneje v 72 urah obvesti Informacijskega pooblaščenca (nadzorni organ), razen če ni verjetno, da bi bile s kršitvijo VOP ogrožene pravice in svoboščine posameznikov.

[IV] Uradno obvestilo o kršitvi mora vsebovati:

- opis vrste kršitve VOP, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
- sporočilo o imenu in kontaktnih podatkih DPO ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve VOP ter
- opis ukrepov, ki jih SFU LJUBLJANA sprejme ali katerih sprejetje predlaga za obravnavanje kršitve VOP, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

[V] Kadar in kolikor informacij ni mogoče zagotoviti istočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja. SFU LJUBLJANA dokumentira vsako kršitev VOP, vključno z dejstvi v zvezi s kršitvijo VOP, njene učinke in sprejete popravne ukrepe. Ta dokumentacija nadzornemu organu omogoči, da preveri skladnost s tem členom.

[V] SFU LJUBLJANA o kršitvah VOP obvesti tudi SFU Dunaj zlasti in nemudoma, če je sklepati, da je do vdora v informacijski sistem SFU LJUBLJANA prišlo preko informacijskega sistema SFU Dunaj, če bi

lahko vdor na SFU Ljubljana vplival na varnost informacijskega sistema SFU Dunaj ali v primeru, da so zaradi vdora ogrožene evidence študentov in zaposlenih.

30. člen

[I] Kadar je verjetno, da kršitev VOP povzroči veliko tveganje za pravice in svoboščine posameznikov, SFU LJUBLJANA brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve VOP. Sporočilo mora vsebovati jasno navedbo obsega kršitve, kontaktne osebe za dodatne informacije oziroma DPO ter opis verjetnih posledic.

[II] Sporočilo posamezniku ni potrebno, če je izpolnjen kateri od naslednjih pogojev:

- SFU LJUBLJANA je izvedla ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot je šifriranje;

- SFU LJUBLJANA je sprejela naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz odstavka I verjetno ne bo več udejanjilo;

- to bi zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

31. člen

[I] Če obstaja sum pri vdoru v zbirko osebnih podatkov, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani, ali če je do zlorabe osebnih podatkov že prišlo, mora Svet zavoda poleg uvedbe disciplinskega postopka zoper storilca ali poleg izreka opomina pred redno odpovedjo pogodbe o zaposlitvi ali poleg redne odpovedi pogodbe o zaposlitvi iz krivdnih razlogov ali poleg izredne odpovedi pogodbe o zaposlitvi, če je zlorabil ali poskusil zlorabiti osebne podatke delavec fakultete, vdor ali zlorabo oziroma poskus zlorabe, prijaviti organom pregona.

(II) Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v zakonu, na podlagi katerega se zbirajo ali nameni določenimi v katalogu zbirk osebnih podatkov. Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene.

32. člen

Zaposleni SFU LJUBLJANA in zunanji sodelavci so dolžni poskrbeti za ustrezno zavarovanje in hrambo podatkov in dokazov kršitve VOP, na podlagi katerih bi se dalo ugotoviti dejstva v zvezi z dogodkom.

33. člen

O kršitvi VOP usposobljeni zaposleni ali DPO sestavi Poročilo o varnostnem dogodku. Poročilo se vnese v Dnevnik obdelave podatkov.

V. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

34. člen

[I] Pred nastopom dela zaposlenega na delovnem mestu, kjer se obdelujejo osebni podatki, mora zaposleni podpisati Izjavo, ki ga zavezuje k varovanju osebnih podatkov.

[II] Pred nastopom funkcije (članstva) v organih SFU LJUBLJANA, na katerih se obravnavajo tudi osebni podatki zaposlenih in študentov, mora član organa podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov in ki ga opozarjajo na posledice kršitve zaveze.

[III] Obveza varovanja osebnih podatkov, s katerimi se zaposleni seznani pri svojem delu na SFU LJUBLJANA, traja tudi po prenehanju delovnega razmerja.

[IV] Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega Pravilnika ter ureditvijo na področju varstva osebnih podatkov (GDPR in ZVOP-2), izjava pa mora vsebovati tudi pouk o posledicah kršitve.

[V] Za kršitev določil iz prejšnjega odstavka so zaposleni disciplinsko odgovorni, zunanji obdelovalci pa na podlagi pogodbenih obveznosti.

[VI] Disciplinska, delovnopravna ali pogodbena odgovornost ne izključuje morebitne odškodninske in kazenske odgovornosti kršitelja, ki povzroči ali omogoči kršitev VOP.

[VII] Ureditev iz tega člena se smiselno uporablja tudi za zunanjega sodelavca.

35. člen

Zaposleni v zvezi z varstvom osebnih podatkov stori kršitev delovne dolžnosti, če:

1. opusti vestno in skrbno nadzorovanje varovanih prostorov;

2. opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov;

3. ne uniči kopije osebnih podatkov v za to določenih primerih;

4. ni ves čas servisiranja računalnika in programske opreme prisoten;

5. ne izvaja preventive v zvezi z računalniškimi virusi;
6. ne vpisuje obdelav osebnih podatkov v Dnevnik obdelav osebnih podatkov;
7. ne obvesti Sveta zavoda, DPO-ja ali pooblaščenega delavca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov.

36. člen

Zaposleni stori hujšo kršitev delovne dolžnosti, če:

1. sporoča osebne podatke, s katerimi se je seznanil pri svojem delu, sodelavcem ali drugim osebam;
2. opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam;
3. nepooblaščeno izdela kopije nosilcev osebnih podatkov;
4. brez izrecnega dovoljenja odnaša iz SFU LJUBLJANA nosilce osebnih podatkov;
5. če posreduje osebne podatke brez potrebnega dovoljenja;
6. če posredovanje osebnega podatka ne vpiše v Dnevnik obdelav osebnih podatkov;
7. če brez potrebnega dovoljenja popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo;
8. če namesti ali odnese programsko opremo iz SFU LJUBLJANA brez izrecnega dovoljenja člana Sveta zavoda ali od njega pooblaščene osebe;
9. če ne hrani računalniških kopij vsebin zbirk osebnih podatkov v zavarovanih zaklenjenih omarah.

VI. ODGORNOST IN NALOGE

37. člen

Za vzpostavitev, vodenje in ažuriranje normativne ureditve varstvo osebnih podatkov na SFU LJUBLJANA je na splošni ravni odgovoren Svet zavoda, ob sodelovanju z DPO in z ostalimi pooblaščenimi zaposlenimi ali zunanjimi sodelavci.

38. člen

[I] Za posamezne primere iz ureditve na področju varstva osebnih podatkov je na SFU LJUBLJANA odgovoren DPO.

[II] DPO določi Svet zavoda, pri čemer upošteva njeno seznanjenost z delovnimi, pedagoškimi in organizacijskimi procesi znotraj SFU LJUBLJANA ter njena znanja in praktične izkušnje s področja varstva osebnih podatkov.

[II] Naloge DPO obsegajo:

- obveščanje upravljavca ali obdelovalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu z GDPR, ZVOP-2 in drugimi področno povezanimi zakoni s področja varstva osebnih podatkov;
- spremljanje skladnosti politik upravljavca in obdelovalca osebnih podatkov z GDPR, ZVOP-2 in drugimi področno povezanimi zakoni s področja varstva osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;
- svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja;
- sodelovanje z Informacijskih pooblaščencem (nadzorni organ);
- delovanje kot kontaktna točka za Informacijskega pooblaščenca (nadzorni organ) pri vprašanjih v zvezi z obdelavo osebnih podatkov na SFU LJUBLJANA.

39. člen

SFU LJUBLJANA osebne podatke obdeluje na podlagi zakonite obdelave, ki vključuje obdelave, ki jih nalaga zakonska ureditev in privolitev posameznikov, na katere se ti podatki nanašajo.

40. člen

[I] Pred začetkom obdelave osebnih podatkov SFU LJUBLJANA od posameznikov pridobi pisno soglasje, ki mora vsebovati:

- jasno opredeljeno voljo;
- navedbo podatkov, ki se zbirajo;
- opredeljen namen zbiranja podatkov;
- čas shranjevanja podatkov ter
- seznanitev s pravico zahtevati dostop do lastnih osebnih podatkov, pravico zahtevati popravek, izbris ali omejitev uporabe osebnih podatkov, pravico do ugovora obdelavi, pravico do prenosljivosti podatkov, pravico, da v primeru kršitev varstva osebnih podatkov o tem seznani DPO-ja o tem s pritožbo obvesti Informacijskega pooblaščenca.

[II] SFU LJUBLJANA od posameznikov zbira podatke, navedene v 3. členu, z natančneje določenim rokovanjem v Evidenci dejavnosti obdelave.

[III] SFU LJUBLJANA lahko zaradi lažjega dostopa in preverbe vodi elektronsko Evidenco privolitev posameznikov. Do elektronske evidence privolitev lahko dostopajo samo osebe, ki so sicer upravičene, da od posameznikov pridobijo privolitve, ali od njih pooblaščene osebe znotraj SFU LJUBLJANA.

VII. HRAMBA IN ROKI HRAMBE OSEBNIH PODATKOV

41. člen

[I] Vpisni listi z osebnimi podatki o študentih, vpisanih na SFU LJUBLJANA, se hranijo v referatu SFU LJUBLJANA. Arhiv mora biti zaklenjen, s ključem lahko razpolagajo le pooblaščeni zaposleni.

[II] Kadrovske evidence z osebnimi podatki zaposlenih se hranijo v zaklenjeni ognjevarni omari v prostorih SFU LJUBLJANA. S ključem lahko razpolagajo le pooblaščeni zaposleni.

[III] Osebni podatki posameznikov, povezani z računovodskimi in knjigovodskimi podatki, se z namenom finančne obdelave hranijo v računovodsko-knjigovodski pisarni.

42. člen

[I] SFU LJUBLJANA osebne podatke posameznikov na podlagi privolitve in glede na pravno ureditev hrani za čas trajanja pogodbenega razmerja, kolikor je potrebno za namene obdelave in kolikor je potrebno za izpolnjevanje zakonskih obveznosti oziroma do preklica, v kolikor preklic ni v nasprotju z zakonsko določenimi načini in roki hrambe.

[II] SFU LJUBLJANA lahko osebne podatke shrani za daljše obdobje, če bodo obdelani zgolj za namene arhiviranja v javnem interesu, za znanstvenoraziskovalne namene ali statistične namene, pri čemer se izvedejo ustrezni tehnični in organizacijski ukrepi, da se zaščitijo pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo.

VIII. OSEBNI PODATKI NA SPLETU

43. člen

Obiskovalci spletne strani SFU LJUBLJANA se ob uporabi Zakona o elektronskih komunikacijah seznanijo s Politiko zasebnosti, piškotki in pogoji uporabe spletne strani ter se morajo za pričetek uporabe spletne strani strinjati s spletno obdelavo osebnih podatkov.

IX. PREHODNE IN KONČNE DOLOČBE

44. člen

Za vsa področja, ki jih Pravilnik ne ureja, se uporabljajo določbe GDRP in ZVOP-2 ter področna zakonodaja Republike Slovenije in EU.

45. člen

Z določbami tega Pravilnika morajo biti seznanjeni vsi zaposleni in pogodbeni obdelovalci SFU LJUBLJANA.

46. člen

Ta pravilnik začne veljati in se uporablja naslednji dan po dnevu objave na spletni strani SFU LJUBLJANA.

V Ljubljani, dne 4. 4. 2023

Predsednik Sveta zavoda SFU LJUBLJANA

Mag. Miran Možina