Na podlagi 64. člena Statuta Univerze v Ljubljani (Uradni list RS, št. 4/17, s spremembami in dopolnitvami), ter na podlagi člena 32 (in dalje) 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 (OJ L 119, 4.5.2016, p. 1–88, v nadaljevanju: Uredba) je Upravni odbor Univerze v Ljubljani na seji dne 2. 4. 2020 sprejel naslednji

P R A V I L N I K
o varnosti obdelave osebnih podatkov na Univerzi v Ljubljani

I. poglavje
SPLOŠNE DOLOČBE

1. člen
(Obseg pravilnika)

(1) Univerza v Ljubljani (v nadaljevanju: UL) prek svojih članic izvaja izobraževalno, raziskovalno, razvojno in umetniško dejavnost ter temeljno, razvojno in uporabno raziskovalno delo. V vseh teh primerih nastopa UL kot upravljavec osebnih podatkov.

(2) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za varnost osebnih podatkov na Rektoratu in organih Univerze v Ljubljani (v nadaljevanju: UL) in posameznih članicah UL (v nadaljevanju: članica) z namenom, da se prepreči slučajno ali namerno nepooblaščeno obdelavo osebnih podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop ali izguba dostopa.

(3) Zaposleni in zunanji sodelavci (npr. znanstveni, strokovni in tehnični delavci in sodelavci in člani organov univerze in članic), ki pri svojem delu obdelujejo osebne podatke, morajo biti seznanjeni z Uredbo, zakonom, ki ureja varstvo osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. člen
(Pomen izrazov)

(1) V tem pravilniku uporabljeni izrazi imajo enake pomene, kot jih določa 4. člen Uredbe.

(2) »Nosilci osebnih podatkov« so papirni ali elektronski dokumenti, trdi diski, elektronske prenosne spominske naprave (npr. USB, prenosne podatkovne enote), programska oprema in drugi mediji, na katere je mogoče zapisati in shraniti osebne podatke.

(3) »Delovna postaja« je računalnik, prenosnik, tablica ali druga podobna naprava, ki poleg zapisa in shranjevanja omogoča tudi drugo obdelavo osebnih podatkov (npr. prikazovanje).

(4) Geslo je niz znakov, ki ga sestavljajo črke, številke in drugi znaki ter temelji na tajnosti, ki jo pozna uporabnik.

(5) Zunanji izvajalec (pogodbeni izvajalec) pomeni posameznika ali družbo, ki je odgovor-en/na in zadolžen/a za dodeljevanje in omejevanje dostopnih pravic do aplikacij in podatkov upravljalca osebnih podatkov ter drugih informacijskih sistemov.

II. poglavje
POOBLAŠČENA OSEBA ZA VARSTVO PODATKOV

3. člen
(Imenovanje DPO)

(1) Na predlog glavnega tajnika UL rektor imenuje Pooblaščeno osebo za varstvo podatkov UL (v nadaljevanju: DPO UL).

(2) Članice UL lahko imenujejo svojega DPO, v kolikor obdelujejo večje količine osebnih podatkov ali posebne vrste osebnih podatkov ali če na podlagi ocene tveganja presodijo, da ga potrebujejo. V tem primeru dekan članice imenuje osebo, pooblaščeno za neposredno sodelovanje z DPO UL (*DPO članice*).

(3) Če članica nima svojega DPO, mora določiti kontaktno osebo, ki bo koordinirala aktivnosti v zvezi z varstvom osebnih podatkov in sodelovala z DPO UL *(koordinator varstva osebnih podatkov)*.

(4) Za DPO UL ali DPO članice je lahko imenovana oseba, ki izpolnjuje pogoje iz Uredbe in zakona, ki ureja varstvo osebnih podatkov, zlasti pa mora imeti izkušnje na področju varstva osebnih podatkov, priporočljivo pa tudi na področju varnosti informacijskih sistemov.

(5) Če je za DPO UL imenovana zunanja fizična ali pravna oseba, mora ta zagotoviti, da naloge DPO UL neposredno

opravljajo tiste fizične osebe, ki izpolnjujejo pogoje iz 4. odstavka tega člena.

4. člen

(Naloge in položaj DPO)

(1) DPO UL izvaja za UL (rektorat);

- naloge, ki jih določata Uredba in zakon, ki ureja varstvo osebnih podatkov,
- koordinira delo in skrbi za enotno prakso DPO članic, zlasti tako, da svetuje, izobražuje in nadzoruje delo DPO članic,
- na podlagi ocene tveganja pripravi letni načrt dela in ga predloži rektorju,
- letno poroča o svojem delu rektorju.

(2) DPO članice izvaja naloge, ki jih določajo Uredba in zakon, ki ureja varstvo osebnih podatkov ter notranja pravila, za dekanat članice in organe članice, za katero je imenovan, zlasti pa tudi:

- svetuje znanstveno-raziskovalnemu in strokovno-tehničnemu osebju članice glede vprašanj, v zvezi s katerimi je vzpostavljena enotna praksa DPO članic;
- spremlja skladnost ravnanja na področju varstva osebnih podatkov pri članici in o tem poroča DPO UL;
- izvaja naloge, za katere jo pooblasti DPO UL;
- se udeležuje kolegijev DPO UL.

(3) Koordinator varstva osebnih podatkov na članici sodeluje z DPO UL, izvaja ukrepe na podlagi predlogov DPO UL, organizira izobraževanja zaposlenih in obveščanje zaposlenih o ravnanju z osebnimi podatki, posreduje DPO UL informacije o zaznanih kršitvah.

(4) DPO UL in DPO članice ne smeta biti razrešena ali kaznovana zaradi opravljanja svojih nalog.

(5) DPO UL mora biti zagotovljen dostop do osebnih podatkov in dejanj obdelave, ki jih izvaja Univerza v Ljubljani in članica UL. DPO članice mora biti zagotovljen dostop do osebnih podatkov in dejanj obdelave, ki jih izvaja članica, za katero je imenovana. Za vsak dostop ali za več teh se v skladu s tem odstavkom na podlagi namena obdelave in v skladu s politiko informacijske varnosti ter na podlagi pravne podlage podeli pooblastilo za vpogled.

5. člen

(kontaktni podatki DPO)

(1) Rektorat sporoči Informacijskemu pooblaščencu Republike Slovenije podatke o DPO UL, ki jih zahteva Uredba in zakon, ki ureja varstvo osebnih podatkov.

(2) Rektorat na spletni strani UL objavi ime, priimek in kontaktne podatke DPO UL ter kontaktne podatke vseh DPO članice. Dekanat članice na spletni strani članice objavi ime, priimek in kontaktne podatke DPO UL ter kontaktne podatke DPO članice, ki je imenovan zanjo.

II. poglavje
VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

6. člen

(Varovanje prostorov)

(1) Prostori, kjer se nahajajo nosilci varovanih osebnih podatkov, in strojna ter programska oprema (v nadaljevanju besedila: varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

(2) V varovane prostore (tajništvo, pisarna kadrovske službe, pisarna svetovalne službe, likvidatura plač, pasivni arhivi ipd.) nezaposlene osebe ne smejo vstopati brez spremstva ali prisotnosti zaposlenega delavca. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor.

(3) Vzdrževalci prostorov in druge opreme v varovanih prostorih, poslovni partnerji in drugi obiskovalci, se smejo gibati

v varovanih prostorih le ob prisotnosti delavca zavoda.

(4) 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, delovne postaje pa zaklenjene, na način, ki ga določa ta pravilnik za čas izven delovnega časa.

(5) Dostop v prostore iz 1. odstavka tega člena je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja glavnega tajnika v Upravi in tajnika članice na članici.

(6) 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.

(7) Ključi varovanih prostorov se hranijo v prostorih, ki so določeni s hišnim redom UL in hišnimi redi članic, neuporabni ključi se komisijsko uničijo. Ključi se ne puščajo v ključavnici v vratih z zunanje strani.

(8) Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

7. člen

(Ravnanje z nosilci podatkov)

(1) Izven delovnega časa morajo biti nosilci osebnih podatkov shranjeni v varovanih delovnih prostorih.

(2) Računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, mora biti izven delovnega časa izklopljena in fizično ali programsko zaklenjena, dostop do osebnih podatkov hranjenih na delovnih postajah pa kodiran.

(3) Računalniki, ki morajo biti zaradi stalnega dostopa ves čas priklopljeni, morajo biti varovani v smislu prvega odstavka 6. člena.

(4) Zaposleni ne smejo puščati nosilcev osebnih podatkov (vključujoč dokumente) na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje (npr. stranke). Vsakokrat, ko zaposleni zapusti svoje delovno mesto, mora zagotoviti, da se na mizi ali drugi delovni površini ne nahajajo osebni podatki (politika »čiste mize«), vključujoč nosilce zbirk osebnih podatkov, delovna postaja (računalnik) pa programsko zaklenjen ali izklopljen (politika "praznega zaslona").

(5) V prostorih, v katere imajo vstop stranke oziroma osebe, ki niso zaposlene v zavodu, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je strankam onemogočen vpogled vanje.

(6) Nosilci podatkov, ki vsebujejo posebne vrste osebnih podatkov, morajo biti posebej označeni in zavarovani.

8. člen

(Prostor obdelave)

(1) Obdelava osebnih podatkov iz zbirk osebnih podatkov je dovoljena le v prostorih zavoda. Nosilcev osebnih podatkov delavci zavoda ne smejo odnašati izven zavoda.

(2) Izjema od določila prvega odstavka tega člena je dovoljena, če iznos nosilca in/ali obdelavo osebnih podatkov izven zavoda vnaprej in izrecno dovoli glavni tajnik univerze oziroma tajnik članice za podatke, ki se vodijo na članicah. Ko zaposleni nosilce podatkov iznaša izven varovanih prostorov in/ali izven prostorov obdeluje osebne podatke, mora zagotoviti varnost osebnih podatkov v skladu s tem pravilnikom in mednarodnimi standardi informacijske varnosti.

(3) Glavni tajnik univerze oziroma tajnik članice lahko dovoli iznos nosilcev osebnih podatkov iz zavoda, ko predhodno delavec vpiše namen in razlog za iznos podatkov iz zavoda v knjigo evidenc o ravnanju z osebnimi podatki.

(4) Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, za namene Univerze v Ljubljani dovoli glavni tajnik univerze, na fakulteti pa tajnik fakultete.

(5) Posredovanje osebnih podatkov iz predhodnega odstavka tega člena se vpiše v knjigo evidenc o ravnanju z osebnimi podatki ali samodejno v revizijsko sled.

9. člen

(Vzdrževanja in popravila)

(1) Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo glavnega tajnika univerze oziroma tajnika članice ali od njih pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in njihovi vzdrževalci, ki imajo z zavodom sklenjeno ustrezno pogodbo o obdelavi osebnih podatkov.

III. poglavje
VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

10. člen

(Dostop in spreminjanje programske opreme)

(1) Dostop do računalniške programske opreme mora biti varovan na način, ki omogoča dostop samo določenim pooblaščenim delavcem in delavcem, ki za UL ali članico po pogodbi o obdelavi osebnih podatkov opravljajo servisiranje računalniške in programske opreme.

(2) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi splošne ali individualne odobritve glavnega tajnika oziroma tajnika članice oziroma od njih pooblaščene osebe in upoštevajoč obstoječe varnostne politike UL, izvajajo pa ga lahko samo pooblaščeni izvajalci oziroma njihovi delavci, ki imajo z UL ali članico sklenjeno ustrezno pogodbo o obdelavi osebnih podatkov.

(3) Izvajalci morajo spremembe sistemske in aplikativne programske opreme ustrezno dokumentirati v sorazmerju z velikostjo sprememb in sorazmerno s tveganji za varnost osebnih podatkov.

11. člen

(Razvojna in testna okolja)

(1) Razvojna in testna okolja ne smejo vsebovati osebnih podatkov, pač pa anonimizirane ali izmišljene podatke.

(2) Prehod iz testnega v produkcijsko okolje mora biti skrbno dokumentiran. Pri tem je treba skrbno nadzorovati vključitev osebnih podatkov v produkcijsko okolje. Osebni podatki v nobenem trenutku ne smejo ostati nenadzorovani oz. se jih ne sme obdelovati, dokler produkcijsko okolje ne zagotavlja vseh varnostnih zahtev, določenih v tem pravilniku. Prehodi morajo biti primerno in sledljivo dokumentirani.

12. člen

(Lokacija shranjevanja)

(1) Osebni podatki UL in članic se lahko hranijo le na strežniku UL ali članice. Na delovnih postajah (računalnikih) se osebni podatki lahko hranijo samo, če je to nujno potrebno za opravljanje dela.

(2) Ne glede na prvi odstavek tega člena se lahko osebni podatki hranijo tudi izven strežnika UL oz. članice, če ponudnik storitve zagotavlja vsaj take ukrepe varnosti obdelave, kot jih določajo ta pravilnik in varnostne politike UL in je za takšno hrambo podatkov sklenjena ustrezna pogodba ali obstaja druga pravna podlaga zanjo.

(3) Vse delovne postaje, na katerih so shranjeni osebni podatki, morajo biti kriptirane. Pristojne osebe so v primeru nabave nove programske opreme dolžne kupiti opremo, ki je v skladu z določilom tega odstavka. Za vso obstoječo programsko opremo, ki ni v skladu z zahtevo iz tega odstavka, mora pristojna oseba oceniti tveganje informacijske varnosti in pripraviti oceno učinkov za varstvo osebnih podatkov.

13. člen

(Vzdrževanje delovnih postaj)

(1) Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale osebne podatke in nosilce, na katerih se nahajajo, iz tega pravilnika.

(2) Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora skrbeti, da se v primeru morebitnega kopiranja osebnih podatkov pred servisiranjem, popravilom, spreminjanjem ali dopolnjevanjem sistemske ali aplikativne programske opreme o po prenehanju potrebe po kopiji, kopija uniči.

(3) 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.

(4) V primeru, če se pokaže potreba po popravilu računalnika, na čigar disku se nahajajo osebni podatki, izven zavoda in brez kontrole pooblaščenega delavca zavoda, se morajo podatki iz diska računalnika izbrisati na način, ki onemogoča restavracijo. Če tak izbris ni mogoč, se mora popravilo opraviti v poslovnih prostorih zavoda v prisotnosti pooblaščenega delavca.

14. člen

(Zaščita delovnih postaj)

(1) Vsebina diskov omrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se preverja glede na prisotnost računalniških virusov ter zlonamerne programske opreme v skladu z načrtom preverjanja.

(2) Ob pojavu računalniškega virusa ali zlonamerne programske opreme je potrebno storiti vse v skladu s smernicami, pravili članic in UL ter mednarodnimi smernicami o varovanju informacijske varnosti, da se s pomočjo strokovnjakov virus odpravi in da se ugotovi vzrok pojava virusa.

(3) Vsi podatki in programska oprema, ki so namenjeni uporabi na računalnikih zavoda in v računalniškem informacijskem sistemu zavoda in prispejo v zavod na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kanalov in so oz. bodo vključeni v obdelavo osebnih podatkov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

15. člen

(Prepoved manipulacij programske opreme)

(1) Zaposleni delavci ne smejo brez izrecnega dovoljenja glavnega tajnika oziroma tajnika članice nameščati programske opreme ali obstoječe spreminjati izven običajne dopustne rabe.

16. člen

(Gesla)

(1) Dostop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom osebnih gesel ali z drugim odobrenim načinom za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel oz. dostopov mora zagotavljati podatek o tem, kdo in kdaj je posamezni osebni podatek obdeloval, v sistemih, kjer je to mogoče, pa tudi podatek o namenu obdelave. Podatek o obdelavi mora biti zabeležen na način, da spreminjanje podatkov v dnevniku dogodkov (žurnalu, *log file*) ni mogoče. Takšni podatki morajo biti celoviti in avtentični.

(2) Glavni tajnik na predlog Informacijske službe UL določi režim dodeljevanja, hranjenja in spreminjanja gesel za vse informacijske sisteme, ki so v upravljanju UL.

(3) Osnovna pravila so:

Katerokoli geslo, ki je v uporabi v informacijskem sistemu UL ali članice, mora biti dolgo vsaj 8 znakov, nujno pa mora vsebovati vsaj eno malo in veliko črko, vsaj eno številko in vsaj en poseben znak (npr. »#%&'()«). Geslo ne sme vsebovati imen, priimkov, znanih dejstev ali besed iz kateregakoli jezika. Čas za periodično menjavo gesel se določi skladno s prepoznanimi tveganji. Novo geslo ne sme biti enako, kot je bilo zadnjih pet gesel uporabnika. Geslo si določi vsak uporabnik sam in ga ne sme razkrivati nikomur, vključno ne svojim nadrejenim ali nadzornikom sistema. Enakega gesla uporabniki ne smejo uporabljati zunaj informacijskih sistemov UL.

(4) Pri dodeljevanju in omejevanju dostopov do aplikacij in podatkov se mora upoštevati naslednje omejitve:

- uporabniki imajo dostop le do tistih aplikacij in podatkov, ki jih potrebujejo za opravljanje svojih del in nalog;
- uporabniki ne smejo imeti dostopa do aplikacij in podatkov, za katere nimajo dodeljenih pravic dostopa;
- uporabniki ne smejo imeti dostopa do podatkov/informacij, ki so označeni s stopnjo zaupnosti, za katero nimajo pooblastila.

Dostopi do aplikacij in podatkov, ki jih uporabnik ne potrebuje za opravljanje svojih del in nalog, niso dovoljeni, tudi če uporabniku ti dostopi niso omejeni.

Uporabniki so odgovorni za vse aktivnosti, ki se izvedejo z njihovo identifikacijo uporabnika in geslom ali kvalificiranim digitalnim potrdilom.

17. člen

(Sistemska gesla)

(1) Vsa sistemska gesla in postopki, ki se uporabljajo za dostop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo v zapečatenih ovojnicah v ognjevarni omari ali sefu na rektoratu UL oziroma dekanatu članice, če gre za sistem, ki ni del sistema UL.

(2) Varovana gesla, hranjena v zapečatenih ovojnicah, se smejo uporabiti v izjemnih in nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira.

(3) Po uporabi zapečatenih gesel iz ovojnic glavni tajnik oziroma tajnik članice določi na predlog informacijske službe

UL nova gesla.

18. člen

(Varnostne kopije)

(1) Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlogov mora ustrezna služba ali delavec, ki ga za UL imenuje glavni tajnik, za članico pa tajnik članice, redno izdelovati kopije zbirk osebnih podatkov in izdelavo kopij ustrezno dokumentirati.

(2) Kopije iz prejšnjega odstavka se hranijo v za to določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena s protivlomnimi sredstvi. Ta mesta morajo biti fizično ločena od lokacije UL oz. fakultete, fizični prenos med obema lokacijama pa lahko opravi samo pooblaščena oseba, ki jo za UL določi glavni tajnik, za članico pa tajnik članice. V nobenem trenutku fizičnega prenosa takšna kopija ne sme ostati nenadzorovana.

19. člen

(Varovanje arhivov)

(1) Prostori, v katerih se nahaja arhivsko gradivo, ki vsebuje osebne podatke, morajo ustrezati veljavnim mednarodno priznanim standardom varovanja arhivskega gradiva.

(2) Ne glede na prejšnji odstavek morajo biti prostori, v katerih se nahaja arhivsko gradivo z nosilci osebnih podatkov (vključno s fizičnimi dokumenti), vsaj protipožarno in protivlomno zaščiteni ter fizično ustrezni na način, da se prepreči uničenje osebnih podatkov zaradi poplav, razlitja vode ali drugih nesreč in vplivov okolja.

IV. poglavje
STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

20. člen

(Obveznost podpisa pogodbe o obdelavi osebnih podatkov)

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo (torej tudi z vpogledom) osebnih podatkov (obdelovalec) in ima ta vsaj možnost dostopa do osebnih podatkov, se sklene pisna pogodba o obdelavi osebnih podatkov. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varnosti obdelave osebnih podatkov ali pa se obdelovalca zaveže k spoštovanju tega pravilnika. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

(2) Zunanje pravne ali fizične osebe smejo opravljati samo storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

(3) Pooblaščena pravna ali fizična oseba, ki za Univerzo v Ljubljani ali njeno članico opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

V. poglavje
SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

21. člen

(Vhodna pošta)

(1) Delavec, 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.

(2) Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo na Upravo UL ali članico (prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena).

(3) Delavec, 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. V primeru, ko je pošiljka naslovljena na drug organ ali organizacijo in je pomotoma dostavljena na UL ali članico, jo delavec, ki je zadolžen za sprejem in evidenco pošte, brez odlašanja pošlje naslovnemu organu ali organizaciji, ob smiselni uporabi določili zakona, ki ureja splošni upravni postopek.

(4) Delavec, 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 uradnega položaja in šele nato naslov univerze ali članice.

22. člen

(Prenos osebnih podatkov)

(1) Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo nepooblaščeno obdelavo ali seznanjenje z vsebino.

(2) Osebni podatki v fizični obliki se pošiljajo priporočeno.

(3) Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

(4) Posebne vrste osebnih podatkov (prej občutljivi osebni podatki) v fizični obliki se pošiljajo naslovnikom v zaprtih ovojnicah preko kurirja ali z vročilnico. Takšni podatki morajo biti pri obdelavi posebej označeni in varovani tako, da se nepooblaščenim osebam prepreči dostop do njih.

(5) Posebne vrste osebnih podatkov v elektronski obliki se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

23. člen

(Ravnanje ob posredovanju osebnih podatkov)

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

(2) Za vsako posredovanje osebnih podatkov mora zunanji uporabnik vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo.

(3) Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kateri pravni podlagi.

(4) Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

(5) Pregledovanje in prepisovanje (kopiranje) upravnih spisov in dajanje obvestil o poteku postopka se opravlja v skladu z določbami zakona, ki ureja splošni upravni postopek.

VI. poglavje
BRISANJE PODATKOV

24. člen

(Način brisanja)

(1) Po izteku roka hrambe ali poteku namena, se osebni podatki zbrišejo oziroma nepovratno uničijo nosilci podatkov.

(2) Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov.

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

(4) Uničevanje in brisanje osebnih podatkov se opravi komisijsko. Glavni tajnik oziroma tajnik članice imenuje tričlansko

komisijo s trajnim mandatom, ki prisostvuje in protokolira vsak izbris in uničenje nosilcev osebnih podatkov z zapisnikom.

25. člen

(Brisanje pomožne dokumentacije)

(1) Z vso vestnostjo in skrbnostjo, določeno s tem pravilnikom, se mora brisati in uničevati tudi pomožna dokumentacija, osnutki, računalniški produkti ali polizdelki in predloge, ki vsebujejo posamezne osebne podatke.

(2) Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

VII. poglavje
UKREPANJE OB UGOTOVITVI ZLORABE OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

26. člen

(Obveza sporočanja in preprečevanja nadaljnje škode)

(1) Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščeno obdelavo osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj po zaznavi morebitnega incidenta ali škodnega dogodka) obvestiti DPO UL in / ali ustrezno službo UL ali članice, ki jo za UL določi glavni tajnik, za članice pa tajnik članice, sami pa skušajo takšno aktivnost preprečiti. Pri tem zaposleni ne smejo tvegati svojega življenja ali zdravja.

27. člen

(Obveščanje Informacijskega pooblaščenca)

(1) V primeru kršitve varstva osebnih podatkov se rektorat pred obveščanjem posvetuje z DPO UL, dekanat pa s svojim DPO članice. Rektorat ali dekanat mora najpozneje v 72 urah po seznanitvi s kršitvijo o njej obvestiti Informacijskega pooblaščenca Republike Slovenije, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Pri obveščanju se uporabi zadnji objavljen obrazec Informacijskega pooblaščenca RS oz. obrazec, ki ga predpiše DPO UL.

(2) Obvestilo iz prejšnjega odstavka mora vsebovati:

- opis vrste kršitve varstva osebnih podatkov, 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 pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih UL ali članica sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

(3) V primeru, ko informacij iz prejšnjega odstavki ni mogoče sporočiti v celoti, se te sporočajo postopoma, in sicer takoj, ko se zanje izve.

(4) V primeru, da je do kršitve varstva osebnih podatkov prišlo pri obdelovalcu, je ta dolžan najkasneje v roku 24 ur obvestiti upravljavca. Takšno določilo mora biti zapisano v vsaki pogodbi o pogodbeni obdelavi, ki jo UL ali članica sklene z obdelovalcem.

(5) Oseba, ki raziskuje incident oz. odpravlja morebitne posledice incidenta mora dokumentirati vsako kršitev varstva osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe. To dokumentacijo je UL ali članica dolžna razkriti Informacijskemu pooblaščencu Republike Slovenije, če ta tako zahteva.

28. člen

(Obveščanje posameznika)

(1) Če DPO UL ali DPO članice oceni, da je verjetno, da je kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, mora rektorat ali dekanat najkasneje v roku 24 ur sporočiti posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

(2) Sporočilo iz prejšnjega odstavka mora biti napisano v jasnem in preprostem jeziku in mora vsebovati naslednje informacije:

- sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov UL ali članice oz. druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih UL ali članica sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

(3) Sporočilo posamezniku iz prvega odstavka ni potrebno v naslednjih primerih:

- pristojna služba UL ali članice 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;
- pristojna služba UL ali članice je sprejela naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz prvega odstavka verjetno ne bo več udejanjilo;
- v primerih, ko bi takšno obveščanje 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.

VIII. poglavje
ODGOVORNOST ZA IZVAJANJE UKREPOV ZA VARNOST OSEBNIH PODATKOV

29. člen
(Podpis izjave o seznanjenosti s pravilnikom)

1. Pred nastopom dela delavca ali začetka drugačnega sodelovanja z UL ali članico mora biti delavec oz. pogodbenik (tudi študent na študentskem delu, ali člani organov UL in delovnih teles Senata UL) seznanjen s tem pravilnikom, o čemer praviloma podpiše tudi izjavo o seznanjenosti. Obveznost spoštovanja tega pravilnika velja tudi v primeru, da posameznik podpis izjave odkloni. O odklonitvi podpisa izjave strokovni delavec rektorata ali članice naredi zaznamek.
2. Obveza varovanja osebnih podatkov velja trajno, tudi po koncu zaposlitve oziroma sodelovanja.

30. člen
(Ravnanje v primeru suma prekrška ali kaznivega dejanja)

(1) V primeru, da v konkretnem primeru obstaja sum prekrška, rektorat ali dekanat o tem obvesti Informacijskega pooblaščenca Republike Slovenije.

(2) V primeru, da v konkretnem primeru obstaja sum storitve kaznivega dejanja, glavni tajnik ali tajnik članice o tem obvesti Policijo ali pristojno tožilstvo.

IX. poglavje
VODENJE EVIDENC

31. člen
(Evidenca dejavnosti obdelave)

(1) UL in članice so dolžne voditi Evidenco dejavnosti obdelave osebnih podatkov, v skladu z določilom 30. člena Uredbe. Evidenca se ažurira sproti, obvezno pa enkrat letno.

X. poglavje
POSEBNE UREDITVE

32. člen
(Posebna ureditev za specifične dejavnosti)

(1) Ta pravilnik velja za UL in vse članice v celotnem obsegu njihovega poslovanja.

(2) V primeru, da posamezna članica, njen DPO članice ali DPO UL oceni, da bi v določenem delu poslovanja ali izvajanja nalog morala članica varnost obdelave urediti podrobneje, kot določa ta pravilnik, to lahko stori samo ob pogoju, da posebna ureditev dosega vsaj enake standarde varnosti, kot so določeni v tem pravilniku. Pred sprejemom posebnega pravilnika mora pridobiti soglasje DPO UL.

XI. poglavje
PREHODNE IN KONČNE DOLOČBE

33. člen

(Uskladitev evidence dejavnosti obdelave)

(1) UL in članice morajo v svoji evidenci dejavnosti obdelave v roku 3 mesecev od sprejema tega pravilnika določiti odgovorne osebe za posamezne zbirke osebnih podatkov ali procese obdelave.

(2) UL in članice morajo za vsako delovno mesto, ki sme zaradi narave svojega dela obdelovati osebne podatke, v roku 3 mesecev od sprejema tega pravilnika določiti dostopne pravice tako za fizične, kot tudi elektronske oblike zbirk ali procesov.

34. člen

(Uskladitev pogodb o obdelavi osebnih podatkov)

(1) UL in članice morajo v roku 3 mesecev od sprejema tega pravilnika uskladiti pogodbe o obdelavi podatkov, izjave, evidenco dejavnosti obdelav in druge morebitne akte, ki jih ureja ta pravilnik.

(2) Vse pogodbe o obdelavi osebnih podatkov, ki so bile sklenjene pred 25. 5. 2018, morajo UL in članice nadomestiti s pogodbami o obdelavi z vsemi sestavinami, kot jih določa člen 28 Uredbe.

35. člen

UL in članice morajo v roku 1 meseca dni od objave tega pravilnika o tem seznaniti vse zaposlene in zunanje izvajalce, ki izvajajo dejavnosti obdelave osebnih podatkov (vključno s študenti, ki opravljajo delo preko študentske napotnice).

36. člen

(1) Ta pravilnik začne veljati petnajsti dan po dnevu objave na spletnih straneh Univerze v Ljubljani.

(2) Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o varovanju osebnih in zaupnih podatkov na Univerzi v Ljubljani z dne 9. 10. 2006.

(3) Ta pravilnik se objavi na intranetu in oglasni deski (kjer ta obstaja) UL in vseh članic.

V Ljubljani, dne 2. 4. 2020

Upravni odbor Univerze v Ljubljani:
prof. dr. Borut Božič, predsednik

PRILOGE:

Priloga 1

Izjava delavca oz. pogodbenika o varnosti osebnih podatkov

Spodaj podpisani _____ potrjujem, da sem prebral Pravilnik o varnosti obdelave osebnih podatkov na Univerzi v Ljubljani, ga razumem in se zavezujem k njegovemu izrecnemu uveljavljanju ves čas mojega dela za Univerzo v Ljubljani oz. fakulteto, kakor tudi po prenehanju mojega dela.

Prav tako potrjujem, da sem seznanjen z določbami zakona, ki ureja področje varstva osebnih podatkov, in Splošno uredbo EU o varstvu osebnih podatkov (GDPR), ter s posledicami morebitnega neupoštevanja prej navedenega pravilnika oziroma zakona ali uredbe (kršitev pogodbe o zaposlitvi). Seznanjen sem tudi, da bom regresno odgovoren v primeru, da bo Univerza v Ljubljani ali fakulteta, kjer sem zaposlen, morala izplačati globo, kazen ali odškodnino zaradi protipravnih posegov v varstvo osebnih podatkov, ki jih bom s svojim ravnanjem povzročil namenoma ali iz hude malomarnosti.

Podpis: _____ Datum in kraj: _____

Priloga 2

Izjava zunanjega izvajalca o varnosti osebnih podatkov

Spodaj podpisani _____ potrjujem, da sem prebral Pravilnik o varnosti obdelave osebnih podatkov na Univerzi v Ljubljani, ga razumem in se zavezujem k njegovemu izrecnemu uveljavljanju ves čas mojega dela za Univerzo v Ljubljani oz. fakulteto, kakor tudi po prenehanju mojega dela.

Prav tako potrjujem, da sem seznanjen z določbami zakona, ki ureja področje varstva osebnih podatkov, in Splošno uredbo EU o varstvu osebnih podatkov (GDPR), ter s posledicami morebitnega neupoštevanja prej navedenega pravilnika oziroma zakona ali uredbe (kršitev pogodbe). Seznanjen sem tudi, da bom regresno odgovoren v primeru, da bo Univerza v Ljubljani ali fakulteta, kjer sem zaposlen, morala izplačati globo, kazen ali odškodnino zaradi protipravnih posegov v varstvo osebnih podatkov, ki jih bom s svojim ravnanjem povzročil namenoma ali iz hude malomarnosti.

Podpis: _____ Datum in kraj: _____

Priloga 3

VZORCI POSREDOVANJ OSEBNIH PODATKOV

Naziv članice/univerze Naslov

_____

_____

_____

V Ljubljani, dne_____

Opr. št.: _____

1. EVIDENCA IZNOSA NOSILCEV OSEBNIH PODATKOV IZ POSLOVNIH PROSTOROV

Datum iznosa	Razlog iznosa	Odobritev	Datum vračila	OPOMBE

2. EVIDENCA POSREDOVANJ OSEBNIH PODATKOV TRETJIM OSEBAM (neobvezno, če obstaja drugačna oblika sledljivosti)

Datum posredovanja	Razlog (pravna podlaga)	Odobritev	OPOMBE

3. EVIDENCA IZDELAVE KOPIJ VSEBIN ZBIRK OSEBNIH PODATKOV (neobvezno, če obstaja druga oblika sledljivosti)

Datum izdelave kopij	Vrsta kopirane zbirke	Namen, za katerega so rabljene kopije	Kraj hranjenja kopij	Datum uničenja kopije	OPOMBE

4. EVIDENCA URESNIČEVANJA PRAVIC POSAMEZNIKOV (neobvezno)

Datum zahteve	Vrsta pravice	Odločitev	Datum odločitve	OPOMBE

5. EVIDENCA SPREMEMB IN DOPOLNITEV SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME

Datum posega v programsko opremo	Vrsta posega v opremo	Ime in priimek osebe, ki je izvedla poseg	Namen posega	Podpis osebe	OPOMBE

Priloga 4

Seznam varnostnih politik UL / članice, ki se nanašajo na varnost obdelave osebnih podatkov oz. varovanja informacij:

a. (navedba varnostne politike)
b. (navedba varnostne politike)
c. …