



X0107255

Na podlagi 25. člena Zakona o varstvu osebnih podatkov (Ur.l. RS 94/07 s spr. in dop.), 15. člena Zakona o knjižničarstvu (Ur.l. RS 87/01 s spr. in dop.) in v skladu z 41. členom Statuta Centralne tehniške knjižnice Univerze v Ljubljani je direktor CTK dne 24. 9. 2021 sprejel

PRAVILNIK O VAROVANJU ZAUPNIH IN OSEBNIH PODATKOV TER O VAROVANJU DOKUMENTARNEGA GRADIVA

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski in logično tehnični postopki in ukrepi za varovanje zaupnih in osebnih podatkov ter drugih podatkov potrebnih za delovanje CTK (v nadaljevanju: podatki), s katerimi upravlja Centralna tehniška knjižnica Univerze v Ljubljani (v nadaljevanju: CTK) ter prostorov, računalniške opreme in komunikacijskih omrežij CTK, v katerih se ti podatki nahajajo oziroma preko katerih poteka prenos teh podatkov, z namenom, da se nepooblaščenim osebam prepreči dostop, obdelava, uporaba, uničenje, spreminjanje in posredovanje zaupnih in osebnih podatkov ter drugih podatkov potrebnih za delovanje CTK.

2. člen

Izrazi, uporabljeni v tem pravilniku, imajo naslednji pomen:

ZAUPEN PODATEK je podatek, ki je razglašen za tajnost, ker je tako pomemben, da bi z njegovim razkritjem nastale škodljive posledice za delovanje ali interese CTK.

OSEBNI PODATEK je katerikoli podatek, ki se nanaša na posameznika ne glede na obliko, v kateri je izrazen.

PODATEK je skupno ime za zaupne in osebne podatke, opredeljene v prejšnjih dveh alinejah.

POSAMEZNIK je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek, če se lahko identificira na način, ki ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

ZBIRKA PODATKOV je zbirka, ki vsebuje zaupne ali osebne podatke (npr. evidence, register, baza podatkov), ki se vodi s sredstvi za avtomatsko obdelavo podatkov ali s klasičnimi sredstvi in je namenjena izvajanju nalog CTK.

OBDELAVA OSEBNIH IN ZAUPNIH PODATKOV je kakršnokoli delovanje v zvezi z osebnimi podatki, zlasti postopki in procesi zbiranja, shranjevanja, spreminjanja, združevanja, uporabe, brisanja in posredovanja podatkov.

DOKUMENTI so vsi pisni, tiskani, risani in posneti podatki ali podatki v elektronski oziroma drugi ustrezni obliki.

NOSILCI PODATKOV so vse vrste sredstev, na katerih so zapisani ali posneti podatki.

VAROVANI PROSTORI: vsi prostori, v katerih so nosilci zaupnih ali osebnih podatkov ali drugih podatkov potrebnih za delovanje CTK ter prostori, v katerih je oprema, s katero je mogoč dostop do teh podatkov.

II. KATALOG PODATKOV

3. člen

Upravljevec vodi katalog podatkov v skladu z zakonom. V katalogu morajo biti opisane vse zbirke osebnih podatkov, ki jih vodi. Katalog podatkov se redno dopolnjuje ob vsaki spremembi podatkov, ki jih ta vsebuje. Zaposleni, ki obravnavajo osebne podatke, morajo biti seznanjeni z vsebino kataloga podatkov.

III. STOPNJE TAJNOSTI IN VRSTE ZAUPNIH PODATKOV V CTK

4. člen

Stopnje tajnosti zaupnih podatkov v CTK so:

ZAUPNO so podatki, katerih razkritje nepoklicani osebi bi lahko škodovalo interesom CTK. Stopnjo tajnosti zaupno določita direktor oziroma oseba, ki ga nadomešča.

INTERNO so: strokovna navodila za opravljanje delovnih nalog, delovni materiali za interne predpise, analitična, statistična in druga gradiva o delu oddelkov in služb CTK, interno informiranje, interni imeniki in vsa druga interna gradiva CTK. Razkritje teh podatkov nepoklicani osebi bi lahko škodovalo delovanju in izvajanju nalog CTK. Izjeme od stopnje tajnosti interno, ki so namenjene javni objavi, določi vodja organizacijske enote oz. druga pooblaščenca oseba s soglasjem direktorja.

JAVNO so podatki, ki niso opredeljeni niti kot zaupno, niti kot interno in zajema vse ostale neoznačene dokumente.

Vrste zaupnih podatkov v CTK so:

TAJNI PODATKI z oznako stopnje »zaupno« ali »interno«.

OSEBNI PODATKI, ki se lahko obdelujejo samo v skladu z zakonom ali na podlagi pisne privolitve posameznika.

Z osebnimi podatki se glede na njihovo vsebino ravna kot s podatki stopnje »zaupno« ali »interno« (npr. interni telefonski imenik, osebne mape...). Stopnjo zaupnosti zbirk osebnih podatkov določi direktor oziroma oseba, ki ga nadomešča. Direktor lahko za posamezne zbirke osebnih podatkov pooblasti druge zaposlene, da določajo stopnjo tajnosti.

IV. VAROVANJE PROSTOROV, STROJNE, SISTEMSKE IN PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO S TO OPREMO

5. člen

Prostori v katerih so nosilci zaupnih ali osebnih podatkov ali drugih podatkov potrebnih za delovanje CTK ter prostori, v katerih je oprema, s katero je mogoč dostop do teh podatkov (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov. Način varovanja je podrobneje opredeljen v Varnostni politiki CTK, ki je priloga tega pravilnika.

6. člen

Dostop do strežnikov, osebnih računalnikov ter aplikacij za obdelovanje osebnih in zaupnih podatkov ter drugih podatkov, potrebnih za delovanje CTK (tako spletnih, strežniških, kot tudi lokalno nameščenih na osebnih računalnikih) se varuje s sistemom gesel za identifikacijo in avtorizacijo fizičnih uporabnikov in avtomatiziranih procesov.

Za delo s posameznimi aplikacijami in dostop do različnih vrst podatkov imajo delavci CTK različne pravice in pooblastila glede na zahteve svojega dela. Podeljevanje, spremembe in ukinitve pooblasti, pravic in dostopov ter nalogi za njihovo izvajanje morajo biti v pisni obliki. Kot pisna oblika se šteje tudi elektronska pošta poslana iz službenih e-naslovov pooblastiteljev na službene e-naslove pooblaščenecv.

Tako pooblastitelji, kot pooblaščenca vodijo lastno evidenco izdanih oziroma prejetih pooblastil. Evidenca pooblastil poslanih ali prejetih po elektronski pošti je lahko v obliki mape v poštnem predalu zaposlenega, v kateri hrani poslana oziroma prejeta pooblastila.

Pooblastila privilegiranim uporabnikom morajo biti v papirni obliki in se hranijo v tajništvu.

Politika gesel, pooblastil in pravic ter nadzor nad delom pooblaščenih oseb je podrobneje opredeljena v Varnostni politiki CTK, ki je priloga tega pravilnika.

7. člen

S šampiljkami in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati kot z zaupnimi podatki.

V. SPREJEM IN POSREDOVANJE ZAUPNIH IN OSEBNIH PODATKOV

8. člen

Zaupne in osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo spreminjanje, prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino. Ti postopki in ukrepi so podrobneje opredeljeni v Varnostni politiki CTK, ki je priloga tega pravilnika.

Zaposleni, ki je zadolžen za sprejem in evidenco pošte, mora proti podpisu izročiti poštno pošiljko z osebni oz. zaupni podatki direktno posamezniku ali oddelku oziroma službi, na katero je ta pošiljka naslovljena. Opravi se tudi vnos v program - evidenco prejete pošte.

Zbirajo in obdelujejo se lahko samo tisti osebni podatki, ki imajo ustrezno zakonsko osnovo. Za zbiranje in obdelavo vseh ostalih osebnih podatkov si je potrebno pridobiti pisno privolitev posameznika, na katerega se podatki nanašajo. Predhodno je potrebno posameznika pisno ali na drug ustrezen način seznanimi o upravljalcu in njegovem zastopniku (osebno ime, naziv oziroma firma in sedež) in z namenom obdelave. Prav tako pa je potrebno posameznika seznanimi z njegovimi pravicami v zvezi z zbiranjem in obdelavo osebnih podatkov. Pred vnosom v zbirko osebnih podatkov se lahko zahteva od posameznika na vpogled osebni dokument ali druga javna listina, da se preveri istovetnost in točnost vnosa.

Podatki se smejo uporabljati samo za namene določene v zakonu ali za namene, razvidne iz pisne privolitve posameznika.

Osebni podatki, vodeni v zbirkah se lahko posredujejo drugim uporabnikom na podlagi pisne zahteve ter samo, če so za njihovo pridobitev in uporabo pooblaščen z zakonom ali na podlagi pisne zahteve oz. privolitve osebe, na katero se nanašajo.

Vsako obdelovanje in posredovanje se beleži v evidenco obdelave in posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili obdelani oziroma posredovani, kdo je to storil, kdaj je to storil oziroma komu ter na kakšni podlagi, razen če to že omogočajo sredstva informacijske tehnologije oziroma je s temi sredstvi mogoče ugotoviti čas obdelave in kdo je to storil za obdobje zakonskega varstva.

Nikoli se ne posredujejo originali dokumentov.

VI. VIDEONADZOR

9. člen

Videonadzor se izvaja skladno z določili zakona, ki ureja varstvo osebnih podatkov. Pisno odločitev o tem sprejme direktor. V odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora. O tem se pisno obvesti vse zaposlene v nadzorovanem prostoru. Videonadzor izvajajo pooblaščen delavci.

Obvestilo o tem, da se izvaja videonadzor, mora biti vidno in razločno nameščeno na način, ki omogoča posamezniku, da se seznani z njim najpozneje v trenutku, ko se nad njim začne izvajati videonadzor (pri vходу v knjižnico) in vsebuje naslednje informacije:

da se izvaja videonadzor,

naziv izvajalca videonadzora,

telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki.

Video nadzorni sistem mora biti zavarovan pred dostopom nepooblaščenih oseb. Varovanje in pooblastila za delo z video nadzornim sistemom so podrobneje opredeljena v Varnostni politiki CTK, ki je priloga tega pravilnika.

VII. PRAVICE POSAMEZNIKA

10. člen

Vse pravice lahko posameznik uveljavlja s pisno zahtevo, ki jo vloži osebno v tajništvu CTK, jo odpošlje preko priporočene pošte na sedež CTK, Trg republike 3, Ljubljana oziroma jo pošlje v elektronski obliki na elektronski naslov post@ctk.uni-lj.si.

Zahteva za uveljavljanje pravic mora vsebovati čim bolj podroben opis želenih dejanj, zahtevanih osebnih podatkov, informacij oziroma dokumentov. V nasprotnem primeru bo CTK posameznika pozval k dopolnitvi zahteve, saj brez konkretizacije ne bo mogel ugotoviti katera dejanja, osebni podatki, informacije oziroma dokumenti v zvezi z obdelavo podatkov so predmet zahteve posameznika.

Za potrebe zanesljive identifikacije v primeru uveljavljanja pravic v zvezi z osebnimi podatki lahko CTK od posameznika zahteva dodatne podatke, kar predstavlja varnostni ukrep, ki zagotavlja, da se osebni podatki ne razkrijejo nepooblaščenim osebam.

CTK lahko zavrne ukrepanje v zvezi z zadevo v primerih, ko dokaže, da posameznika ne more zanesljivo identificirati, oziroma če niso izpolnjeni osnovni pogoji za seznanitev, če je zahteva očitno neutemeljena ali pretirana ali če so v relevantnih predpisih določene posebne izjeme.

Uveljavljanje pravic posameznika in posredovanje zahtevanih podatkov se posamezniku zagotovi brezplačno. CTK lahko zaračunava dejansko porabljen čas po ceniku CTK, če je zahteva posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljena ali pretirana, zlasti če se ponavlja.

CTK bo o zahtevi odločil najkasneje v enem (1) mesecu od prejema popolne zahteve. Rok se lahko ob upoštevanju števila in kompleksnosti zadev po potrebi podaljša za dva (2) meseca, pri čemer bo CTK posameznika, na katerega se nanašajo podatki, o vsakem takem podaljšanju obvestil v roku enega (1) meseca od prejema zahteve skupaj z razlogi za zamudo.

VIII. BRISANJE PODATKOV

11. člen

Po izpolnitvi namena, zaradi katerega so bili zbrani, se osebni podatki, v skladu z zakonom, brišejo iz zbirke, razen tistih, ki so po zakonu, ki ureja arhivsko gradivo in arhive opredeljeni kot arhivsko gradivo oziroma, če tako določa drug zakon.

12. člen

Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

Podatki na klasičnih medijih (listine, kartoteke, register, seznam in podobno) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov.

Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise, ipd.). Odpadnih nosilcev podatkov ni dovoljeno odmetavati v koše za smeti.

Postopek uničevanja nosilcev osebnih podatkov določi Strokovna komisija za nadzor nad brisanjem osebnih podatkov v CTK.

IX. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

13. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščen uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti direktorja ali pooblaščenca za varstvo osebnih podatkov v CTK, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.

V primeru kakršnegakoli potrjenega dejanja iz prejšnjega odstavka je o tem potrebno nemudoma obvestiti informacijskega pooblaščenca, v primeru suma kaznivega dejanja tudi policijo. Glede na posebnosti zgoraj opisanega dejanja je potrebno:

- V primeru vdora v računalniški sistem iz omrežja izklopiti in zavarovati strežnike z osebnimi podatki in o vdoru obvestiti SI.CERT,
- V primeru nepooblaščenega dostopa do zbirk osebnih podatkov v fizični obliki je potrebno prostor zavarovati in preprečiti nadaljnji dostop do osebnih podatkov,
- V primeru nepooblaščenega dostopa do osebnih podatkov s strani zaposlenih zaposlenemu nemudoma preprečiti dostop do vseh zbirk osebnih podatkov v fizični in elektronski obliki, o tem obvestiti pooblaščenca o sebo za varstvo osebnih podatkov v CTK in direktorja, ki mora ukrepati skladno s pooblastili.

X. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

14. člen

Za izvajanje postopkov in ukrepov za varovanje zaupnih in osebnih podatkov so odgovorni direktor in vodje organizacijskih enot.

Pooblaščen osebe odgovorne za posamezno zbirko osebnih podatkov so določene v katalogu zbirk osebnih podatkov.

Vsaka kršitev ali nespoštovanje določil tega pravilnika ali veljavne zakonodaje se šteje kot kršitev delovnih obveznosti in pogodbe o zaposlitvi. V primeru takih kršitev se izvedejo disciplinski ukrepi v skladu z zakonodajo.

15. člen

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

Pred nastopom dela na delovnem mestu, kjer se obdelujejo podatki s stopnjo tajnosti, ki je enaka »zaupno«, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju poklicne skrivnosti in vsebuje pouk o posledicah kršitve.

Za objavljanje osebnih podatkov, ki niso neposredno povezani z opravljanjem javne funkcije oziroma delovnim mestom posameznega delavca, je potrebna predhodna osebna pisna privolitev posameznika.

16. člen

Za kršitev določil prejšnjega člena oziroma določil tega pravilnika so zaposleni disciplinsko odgovorni, ostali pa so odgovorni skladno s pogodbo.

XI. PREHODNE IN KONČNE DOLOČBE

17. člen

Z dnem, ko začne veljati ta pravilnik preneha veljati pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva z dne 24. 9. 2021.

18. člen

O vsebini tega pravilnika morajo biti delavci seznanjeni, kar potrdijo s podpisom izjave o seznaitvi.

19. člen

Ta pravilnik začne veljati v osmih dneh od dneva objave na oglasni deski knjižnice.

V Ljubljani, dne 23. 8. 2028



mag. Miro Pušnik

direktor

URADNI ZAZNAMEK

Pravilnik je bil objavljen na oglasnih deskah 24. 8. 2022

Pravilnik je začel veljati dne: 24. 8. 2022

Priloge:

1. Izjava o varovanju podatkov
2. Varnostna politika CTK

Dunja Kovač

Na podlagi 15. člena **Pravilnika o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva** v Centralni tehniški knjižnici Univerze v Ljubljani, ki ga je sprejel direktor mag. Miro Pušnik dne 3. 9. 2021

IZJAVLJAM

da bom kot tajne varoval osebne podatke delavcev, uporabnikov, strank in drugih oseb ter druge zaupne podatke v CTK in z njimi vestno ravnal na način in po postopkih, ki jih določa Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva v Centralni tehniški knjižnici Univerze v Ljubljani, z določbami katerega sem seznanjen.

Izjavljam, da sem seznanjen s posledicami kršitev določil o varovanju podatkov ter s tem povezano odgovornostjo po zakonu.

Datum:

Delavec:

