Na podlagi 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 ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba) in na podlagi Zakona o varstvu osebnih podatkov – ZVOP-2 (Uradni list RS, št. 163/2022) izdaja direktor mag. Matjaž Eržen naslednji

PRAVILNIK
o varstvu osebnih podatkov v Knjižnici Ivana Tavčarja Škofja Loka

I. SPLOŠNE DOLOČBE

1. člen
(namen pravilnika in dolžnost varovanja)

S tem pravilnikom se določajo organizacijski, tehnični in logistično-tehnični postopki ter ukrepi za varstvo osebnih podatkov v Knjižnici Ivana Tavčarja Škofja Loka (v nadaljevanju: knjižnica) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

Zaposleni in zunanji sodelavci knjižnice, ki pri svojem delu obdelujejo osebne podatke, morajo spoštovati predpise s področja varstva osebnih podatkov. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju zaposlitve, opravljanja del ali nalog oziroma opravljanja storitev pogodbene obdelave.

2. člen
(splošna načela)

Osebni podatki se v knjižnici obdelujejo v skladu s Splošno uredbo, veljavno zakonodajo, tem pravilnikom in naslednjimi splošnimi načeli:

- podatki morajo biti obdelani zakonito, pošteno in na pregleden način;
- zbirajo se za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni;
- podatki so ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo;
- podatki so točni in – kadar je to potrebno – posodobljeni;
- hranjeni so v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo;
- obdelujejo se na način, ki zagotavlja ustrezno varnost osebnih podatkov.

3. člen
(uporaba izrazov)

V pravilniku uporabljeni izrazi, ki se nanašajo na osebe in so zapisani v moški slovnični obliki, so uporabljeni kot nevtralni za ženski in moški spol.

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. *osebni podatek* je katerakoli informacija v zvezi z določenim ali določljivim posameznikom;

2. *posameznik* je 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;
3. *Zbirka osebnih podatkov* je vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
4. *obdelava osebnih podatkov* 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;
5. *upravljavec osebnih podatkov* je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo EU ali zakonodaja Republike Slovenije, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom EU ali nacionalno zakonodajo;
6. *posebne vrste osebni podatki* so podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, genetski podatki, biometrični podatki za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;
7. *uporabnik osebnih podatkov* je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
8. *nosilci podatkov* so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov ipd.);
9. *obdelovalec* je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca.

4. člen
(evidenca dejavnosti obdelave)

Popis zbirk osebnih podatkov, katerih upravljavec je knjižnica, se vodi v evidenci dejavnosti obdelave skladu z določbami 30. člena Splošne uredbe.

V evidenco dejavnosti obdelave se vpisujejo naslednji podatki: naziv ali ime in kontaktne podatke upravljavca ter pooblaščene osebe za varstvo podatkov; namene obdelave; opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov; kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki; kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo; predvideni roki za izbris različnih vrst podatkov; splošni opis tehničnih in organizacijskih varnostnih ukrepov.

V evidenci dejavnosti obdelave, ki se občasno in na dokumentiran način pregleduje ter po potrebi posodablja, je podrobneje opisan tudi način hrambe in varstva posameznih zbirk osebnih podatkov.

II. VAROVANJE PROSTOROV IN OPREME

5. člen
(varnost podatkov)

Zagotavljanje varnosti osebnih podatkov obsega organizacijske, tehnične in logistično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki v skladu s Splošno uredbo in nacionalno zakonodajo s področja varstva osebnih podatkov, s katerimi se:

- varujejo prostori, oprema in sistemska programska oprema,
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki,
- preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih,
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov,
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ki ga predpisuje zakon ali v katerem je mogoče zakonsko varstvo pravice posameznika zaradi nedopustne obdelave osebnih podatkov.

6. člen
(varovani prostori)

Prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema, sodijo v kategorijo varovanih prostorov in so varovani s fizičnimi ukrepi (zaklepanje, prisotnost delavcev knjižnice) in tehničnimi ukrepi (alarm), ki zmanjšujejo tveganje za vstop nepooblaščenih oseb in njihov dostop do podatkov.

V knjižnici se med varovane prostore uvrščajo: pisarna direktorja, prostor tajništva in računovodstva, pisarne zaposlenih v knjižnici ter arhiv (v nadaljevanju: varovani prostori).

Varovani prostori so varovani s fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov, in zanje velja naslednji režim:

1. Dostop v varovane prostore je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja direktorja ali od njega pooblaščene osebe.
2. Dostop osebam, ki niso zaposlene v varovanih prostorih, je dovoljen le ob prisotnosti zaposlenih v teh prostorih.
3. Delavci, zaposleni v varovanih prostorih, morajo prostore vestno in skrbno nadzorovati in ob vsaki odsotnosti zakleniti.
4. Nosilcev osebnih podatkov ni dovoljeno izpostavljati nevarnosti nenadzorovanega vpogleda ali iznosa.
5. Osebni podatki se hranijo le v varovanih prostorih.
6. 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. Delavec, ki pri svojem delu obdeluje osebne podatke, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalni mizi ali jih drugače izpostavljati vpogledu vanje nepooblaščenim osebam.
8. V prostorih, v katere imajo vstop osebe, ki v knjižnici niso zaposlene, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je tretjim osebam onemogočen vpogled vanje.

Ključe varovanih prostorov je prepovedano puščati v ključavnici v vratih z zunanje strani. Za varovanje ključev posameznega varovanega prostora je odgovorna oseba, ki v posameznem prostoru opravlja delo.

Izven delovnega časa morajo biti pisarne z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

7. člen
(iznašanje podatkov)

Obdelovanje osebnih podatkov iz zbirk osebnih podatkov je dovoljeno le v prostorih knjižnice. Nosilcev osebnih podatkov delavci praviloma ne smejo odnašati izven knjižnice brez dovoljenja direktorja oziroma z njegove strani pooblaščene osebe.

Če je zaradi potreb delovnega procesa v knjižnici neizogibno potrebno, da zaposleni podatke na računalnikih ali drugih nosilcih podatkov zaradi opravljanja nalog iz delovnega razmerja iznašajo tudi izven prostorov knjižnice, morajo zaposleni pri tem spoštovati vsa načela in pravila varstva podatkov, da se podatki ustrezno varujejo in da ne pride do izgube ali obdelave s strani nepooblaščene osebe. Zaposleni, ki iznaša podatke, s tem del odgovornosti za ustrezno ravnanje prevzema nase, saj zbirke ne sme izgubiti, pozabiti ali na drug način ogroziti varnosti podatkov, zato mora z njimi ravnati odgovorno in predvsem paziti, da podatkov ne izgubi, da se ne odtujijo, da jih ne pozabi izven delovnega okolja in da ne pride do vpogleda v podatke s strani nepooblaščenih oseb.

8. člen
(posredovanje podatkov in vodenje evidence)

Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo pravno podlago za pridobitev osebnih podatkov, dovoli direktor ali od njega pooblaščena oseba. O zahtevi vlagatelja je treba odločiti najpozneje v roku 15 dni od prejema popolne zahteve.

Pri posredovanju podatkov tretjim osebam knjižnica za vsako posredovanje osebnih podatkov zagotovi možnost poznejše ugotovitve, kateri osebni podatki so bili posredovani, komu, kdaj in na kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka. S tem namenom se vodi evidenca posredovanj osebnih podatkov.

9. člen
(vzdrževanje in popravila opreme)

Vzdrževanje in popravilo strojne računalniške in druge opreme je dovoljeno samo z vednostjo pooblaščenih oseb upravljavca, izvajajo pa ga lahko samo za to usposobljeni servisi in vzdrževalci, ki imajo s knjižnico sklenjeno pogodbo o servisiranju in vzdrževanju računalniške oziroma strojne opreme.

10. člen
(zadrževanje v prostorih izven delovnega časa)

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji in druge osebe se smejo gibati v varovanih prostorih samo ob prisotnosti osebe, zaposlene v knjižnici. Delavci, kot so čistilke in tehnično-vzdrževalni delavci, se smejo izven delovnega časa v prostorih knjižnice zadrževati le z dovoljenjem direktorja ali od njega pooblaščene osebe.

III. VAROVANJE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

11. člen
(pooblaščene osebe)

Dostop do programske opreme mora biti varovan na način, ki omogoča dostop samo določenim za to vnaprej pooblaščenim osebam, ki v skladu s pogodbo opravljajo naloge, pri katerih je potrebna obdelava določenih osebnih podatkov.

12. člen
(popravljanje in spreminjanje programske opreme)

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorja ali od njega pooblaščene osebe, izvajajo pa ga lahko samo za to usposobljeni servisi in organizacije ter posamezniki, ki imajo s knjižnico sklenjeno ustrezno pisno pogodbo. Izvajalci morajo narejene spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

Zaposleni ne morejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema, saj nimajo podeljenih administratorskih pravic. Računalniki se enkrat letno tudi fizično pregledajo s strani pooblaščenega podjetja. Prav tako zaposleni ne smejo odnašati programske opreme iz prostorov knjižnice brez odobritve s strani direktorja ali z njegove strani pooblaščene osebe.

13. člen
(uničenje kopij)

Delavci, pooblaščeni za obdelavo osebnih podatkov na računalniku, morajo skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske oziroma aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji le-ta uniči, enako tudi drugi za lažje delo pripravljeni delovni pripomočki (npr. Excel tabele z uvoženimi osebni podatki iz zbirke).

14. člen
(antivirusni pregledi)

Vsebina mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se vsakodnevno samodejno preverja glede na možno prisotnost računalniških virusov z nameščenim antivirusnim programom, ki preverja promet in datoteke. Ob pojavu računalniškega virusa se ga odpravi s pomočjo pooblaščenega podjetja, s katerim je podpisana pogodba o podpori in vzdrževanju informacijskega sistema, ter se ugotovi vzrok pojava virusa.

Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo v knjižnico na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov in se zato pred vsako uporabo samodejno programsko preverijo.

Za vzpostavitev in zagotavljanje sistema rednih samodejnih preverjanj prisotnosti virusov in samodejno preverjanje nosilcev za prenos podatkov oziroma vhodnih podatkov je pristojen zunanji izvajalec storitev, s katerim ima knjižnica sklenjeno ustrezno pogodbo.

15. člen
(gesla)

Dostop do podatkov preko aplikativne programske opreme je varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Gesla je treba zamenjati vsake tri mesece, o čemer zaposlene avtomatično obvesti sistem v računalniku. Geslo za dostopanje do podatkov izbere vsak zaposleni sam, oziroma pooblaščeno podjetje pa mu dodeli uporabniško ime. Za vzpostavitev sistemske rešitve v skladu s tem členom pravilnika in za nadzor nad izvajanjem je pristojno pooblaščeno podjetje, ki mora v primeru težav nemudoma obvestiti direktorja.

16. člen
(varnostne kopije)

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se redno izdelujejo kopije zbirk osebnih podatkov. Kopije vsebin na računalnikih se izdelujejo samodejno s sistemsko rešitvijo, ki jo vzpostavi pooblaščeno podjetje. Kopije se praviloma hranijo s pomočjo oblačnih storitev, lahko pa tudi fizično na medijih, za hrambo katerih je pristojen izvajalec storitev.

Če se kopije hranijo na kompaktnih diskih ali drugih medijih, mora pristojna oseba poskrbeti, da se hranijo v varovanih prostorih v zaklenjenih omarah.

IV. VARSTVO OSEBNIH PODATKOV ZAPOSLENIH

17. člen
(sprejemanje pošte)

Delavec v knjižnici, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v knjižnico (prinesejo jih zaposleni, drugi ali kurirji), razen pošiljk iz drugega in tretjega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpre pošiljke, ki je naslovljena na drug organ ali organizacijo in je pomotoma dostavljena v knjižnico.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpreti pošiljke, naslovljene osebno na zaposlenega, na kateri je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime zaposlenega, brez označbe njegovega uradnega položaja, in šele nato naslov knjižnice.

18. člen
(vpogled v delovno sredstvo ali e-pošto delavca)

Elektronska pošta, računalnik, tablice, mobilni telefon in druge elektronske naprave, ki jih delavcu za potrebe opravljanja dela dodeli delodajalec, se s strani zaposlenih uporabljajo v službene namene. V omejenem obsegu in razumnih mejah se lahko elektronska pošta in računalnik uporabljata tudi v zasebne namene delavcev, pri čemer so se uporabniki na strani knjižnice dolžni v smislu skrbi za ugled knjižnice izogibati pošiljanju elektronskih sporočil z neprimerno in žaljivo vsebino.

V računalnik (delovno postajo), drugo tehnično sredstvo (npr. mobilni telefon), dano v uporabo s strani knjižnice, ali v elektronsko pošto delavca, ki je angažiran bodisi na podlagi pogodbe o zaposlitvi bodisi na drugem pogodbenem temelju (v nadaljevanju: uporabnik

opreme), sme knjižnica poseči le v izjemnih primerih, opredeljenih v tem pravilniku, in sicer v primeru nepričakovane, nenadne in dalj časa trajajoče ali trajne odsotnosti uporabnika opreme, na primer v primeru odpovedi delovnega razmerja s strani zaposlenega brez odpovednega roka, v primeru odpovedi delovnega razmerja iz krivdnih razlogov zaradi neopravičene odsotnosti, v primeru, da zaradi svojega zdravstvenega stanja uporabnik ni sposoben izraziti svoje volje, pa takšno stanje traja dlje časa ali se upravičeno domneva, da bo trajalo dlje časa, smrti uporabnika in podobnih izredni primerih, kadar:

- je to nujno potrebno za izpolnitev zakonskih obveznosti knjižnice;
- je to nujno in neogibno potrebno za izpolnitev pogodbenih obveznosti knjižnice, katerih neizpolnitev ali izpolnitev z zamudo bi za knjižnico pomenila izgubo ugleda ali nastanek premoženjske škode.

Uporabnika opreme se pred posegom v njegov računalnik (delovno postajo), drugo tehnično sredstvo ali elektronsko pošto pozove k prostovoljni predložitvi gesel in/ali potrebnih dokumentov ter se mu za izpolnitev zahteve postavi primeren rok. Tako v primeru prostovoljnega posredovanja dostopnih gesel kot v primeru, da se uporabnik na poziv knjižnice ne odzove ali ga zavrne, se vstop v računalnik (delovno postajo), drugo tehnično sredstvo ali elektronsko pošto opravi s strani tričlanske komisije, ki jo vsakokrat imenuje direktor, delavcu/uporabniku pa se omogoči, da dejanju osebno prisostvuje, tako da se ga obvesti o kraju in času dejanja, razen če to iz objektivnih razlogov ni mogoče ali če zaposleni s svojim ravnanjem očitno onemogoča dostop do podatkov.

O vsakem vstopu v računalnik, drugo tehnično sredstvo oziroma elektronsko pošto po tem členu se vodi dokumentacija, ki vsebuje najmanj:

- obrazložen razlog za dopustnost vstopa,
- zapisnik o vstopu v računalnik ali elektronsko pošto z morebitnimi pripombami delavca, če je ta navzoč,
- navedbo prisotnih oseb,
- seznam oziroma izpis pridobljenih podatkov.

Pri postopanju po tem členu se osebni podatki obdelujejo izključno za namene po tem členu, pri čemer se mora vedno spoštovati načelo najmanjšega obsega podatkov, kar pomeni, da se obdelujejo zgolj tisti podatki, ki so nujno potrebni za dosego namena, za katerega se obdelujejo.

Šteje se, da je o namenu uporabe elektronske pošte in ostale programske opreme, ki jo uporabniku za namene opravljanja dela nudi knjižnica, ter o možnostih nadzora po določbah tega pravilnika uporabnik predhodno obveščen, ko mu knjižnica izroči izvod tega pravilnika ali mu ga pošlje na e-naslov, ki ga delavcu/uporabniku zagotavlja delodajalec, ali ga za namen komunikacije s knjižnico posreduje uporabnik sam. Kot primerno obvestilo šteje tudi objava tega pravilnika na oglasni deski ali internem strežniku knjižnice.

19. člen

(izbris podatkov ob prenehanju delovnega razmerja)

Ob prenehanju delovnega razmerja je delavec knjižnice dolžan vrniti službeni računalnik, službeni mobilni telefon oziroma drugo tehnično sredstvo, ki ga je uporabljal v službene namene, pri čemer mora pred vrnitvijo delavec sam poskrbeti, da so s službenih naprav izbrisane vse njegove zasebne vsebine, službene pa ohranjene v celoti.

Delavec lahko za namene opravljanja dela poleg službene opreme in naprav v lasti knjižnice uporablja svoje zasebne računalnike in/ali mobilne telefone in druge tehnične naprave, če takšno uporabo odobri direktor ali od njega pooblaščena oseba. V primeru prenehanja delovnega razmerja je delavec dolžan z zasebnih računalnikov in/ali mobilnih telefonov ali drugih naprav (tudi USB ključev ipd.), ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni s službenega omrežja, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

V. SNEMANJE IN FOTOGRAFIRANJE DOGODKOV

20. člen
(pravna podlaga za snemanje in fotografiranje)

Za namene obveščanja javnosti o delu knjižnice se lahko dogodki v lastni organizaciji ali soorganizaciji delno ali v celoti snemajo oziroma fotografirajo. Tako pridobljeni osebni podatki se smejo obdelovati, vključno z objavo, kadar gre za dogodke, ki jih organizira knjižnica v okviru svojih nalog, pristojnosti ali dejavnosti, če posameznik te obdelave ni prepovedal.

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

21. člen
(obdelovalci)

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov za knjižnico in je registrirana za opravljanje takšne dejavnosti (obdelovalec), se sklene pisna pogodba, predvidena v 28. členu Splošne uredbe. V takšni pogodbi morajo biti določeni tudi pogoji in ukrepi za zagotovitev varnosti osebnih podatkov, zagotavljanje njihove celovitosti in avtentičnosti ves čas obdelave.

Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil s strani knjižnice in osebnih podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pooblaščena pravna ali fizična oseba, ki za knjižnico opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način zagotavljanja varnosti osebnih podatkov, kakor ga določa ta pravilnik.

VII. VARSTVO PODATKOV PRI NJIHOVEM POSREDOVANU

22. člen
(posredovanje podatkov)

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

Posebne vrste osebni podatki se pošiljajo naslovnikom s posebej skrbnimi, dodatnimi ukrepi za zagotavljanje varnosti (v zaprtih kuvertah, priporočeno, da je pošiljanje sledljivo, po elektronski poti pa zavarovano na način, da je med pošiljanjem kriptirano ali zavarovano z geslom).

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da 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.

VIII. BRISANJE PODATKOV

23. člen
(rok brisanja podatkov)

Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Osebni podatki, ki so del pogodb, se izbrišejo iz zbirke podatkov po izteku absolutnih zastaralnih rokov, ki so določeni v zvezi s posamezno obveznostjo ali upravičenjem.

Osebni podatki, ki se obdelujejo na podlagi privolitve, se izbrišejo po prejemu preklica.

24. člen
(način brisanja podatkov)

Za brisanje podatkov z nosilcev podatkov se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

Podatki na klasičnih medijih (listine, kartoteke, registri, seznami itd.) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov (npr. z rezalnikom papirja). Na enak način se uničuje pomožno gradivo (npr. izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).

Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v pisarniške koše za smeti na način, da je mogoča nepooblaščena obdelava podatkov.

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno varnost osebnih podatkov tudi v času prenosa/prevoza.

IX. UPRAVLJANJE VARNOSTNIH INCIDENTOV

25. člen
(izvajanje ukrepov)

Delavci knjižnice 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. Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem, nepooblaščenim dostopom ali uničenjem podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti direktorja, sami pa poskušajo takšno aktivnost preprečiti.

26. člen
(zloraba osebnih podatkov)

Knjižnica mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov, ustrezno ukrepati. Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu s predhodno določenimi nameni zbiranja.

27. člen
(postopek upravljanja varnostnih incidentov)

Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov ipd.) ali do vdora v zbirko osebnih podatkov, mora o tem nemudoma oziroma najkasneje v roku 24 ur obvestiti direktorja.

Direktor ob prejemu obvestila o kršitvi varnosti osebnih podatkov v roku 24 ur določi enega izmed delavcev knjižnice, ki bo preučil incident in glede na resnost kršitve bodisi napravil uradni zaznamek o kršitvi bodisi obvestil informacijskega pooblaščenca. Če je verjetno, da bo nastalo tveganje za pravice in svoboščine posameznikov, se vedno obvesti informacijskega pooblaščenca. O kršitvi varnosti se v vsakem primeru nemudoma obvesti pooblaščeno osebo knjižnice za varstvo podatkov.

Obvestilo informacijskemu pooblaščencu o kršitvi mora vsebovati vsaj naslednje informacije:

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov;
- kontaktne podatke pooblaščene osebe za varstvo podatkov;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih je knjižnica sprejela, ali pa predvidenih ukrepov za ublažitev tveganj za kršitve.

Vse osebe, ki obravnavajo varnostni incident, morajo postopati hitro in skrbno, informacijski pooblaščenec pa mora biti o incidentu – kadar je to potrebno – obveščen najkasneje v roku 72 ur.

X. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

28. člen
(odgovornost in nadzor)

Za izvajanje postopkov in ukrepov za varstvo osebnih podatkov so odgovorni vsi zaposleni v knjižnici in tudi zunanji izvajalci, ki imajo s knjižnico podpisan dogovor o sodelovanju.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja direktor knjižnice ali od njega pooblaščena oseba. Direktor ali od njega pooblaščena oseba opravlja nadzor periodično, in sicer načeloma enkrat letno, v primeru težav ali prejema obvestila o nespoštovanju določb tega pravilnika pa takoj po prejemu takšne informacije.

Splošni letni nadzor se izvede glede vseh ali posameznih določb tega pravilnika, predvsem glede zaklepanja prostorov, iznašanja podatkov izven prostorov knjižnice, posodabljanja evidence dejavnosti obdelave, preverjanja pogodb z zunanjimi obdelovalci, politike gesel, hrambe podatkov v varovanih prostorih, izdelovanja kopij podatkov ipd. V primeru težav ali prejema obvestila o kršitvi direktor ali od njega pooblaščena oseba izvede nadzor v zvezi s konkretno kršitvijo.

O izvedenem nadzoru oziroma pregledu se sestavi zapisnik, ki se hrani skupaj z ostalo dokumentacijo s področja varstva podatkov.

29. člen
(izjava delavca)

Pred nastopom dela delavca na delovnem mestu, na katerem se obdelujejo osebni podatki, mora delavec podpisati pisno izjavo, s katero se zaveže k varstvu osebnih podatkov ves čas trajanja delovnega razmerja, pri čemer se delavca opozori, da obveznost varovanja osebnih podatkov ne preneha s prenehanjem delovnega razmerja in da bo kršitev te obveznosti šteta tudi kot kršitev njegovih zavez iz pogodbe o zaposlitvi.

XI. POOBLAŠČENA OSEBA ZA VARSTVO PODATKOV

30. člen
(imenovanje pooblaščene osebe)

V skladu s prvim odstavkom 37. člena Splošne uredbe direktor imenuje pooblaščeno osebo za varstvo podatkov, katere naloge med drugim obsegajo:

- obveščanje direktorja in zaposlenih v knjižnici o varstvu podatkov ter svetovanje pri obdelavi podatkov;
- spremljanje skladnosti delovanja knjižnice z uredbo in drugimi predpisi;
- svetovanje, kadar je to zahtevano, glede ocene učinka in spremljanje njegovega izvajanja;
- sodelovanje z informacijskim pooblaščencem, zlasti kot kontakt v zvezi z varstvom osebnih podatkov;
- druge naloge, povezane z varstvom podatkov.

V roku 8 dni od določitve pooblaščene osebe se njeni podatki vpišejo v evidenco dejavnosti obdelav v knjižnici, njeni kontaktni podatki pa se objavijo na spletnih straneh knjižnice. V istem roku se kontaktne podatke pooblaščene osebe sporoči informacijskemu pooblaščencu.

XII. KONČNA DOLOČBA

31. člen
(neposredna uporaba in začetek veljavnosti)

Za vprašanja, ki jih ta pravilnik ne ureja, se neposredno uporabljajo določbe Splošne uredbe in veljavne zakonodaje s področja varstva osebnih podatkov.

Ta pravilnik začne veljati naslednji dan po objavi na internem strežniku knjižnice.

Direktor:
Mag. Matjaž Eržen

Številka: 013-RAZ-017/2023-1

Škofja Loka, 15. 03. 2023