Na podlagi Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22 s spremembami, v nadaljevanju: ZVOP-2) ter 24., 25. in 32. člena 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 o varstvu podatkov/ GDPR) in 13. člena Statuta Rudolfovo – Znanstveno in tehnološko središče Novo mesto, je Upravni odbor Rudolfovega na 27. seji dne 18. 10. 2024 sprejel naslednji

PRAVILNIK
O RAVNANJU Z OSEBNIMI PODATKI

I. Splošne določbe

1. člen

S tem Pravilnikom o ravnanju z osebnimi podatki (v nadaljevanju: Pravilnik) se določajo tehnični, organizacijski postopki in ukrepi ter kadrovski ukrepi za ravnanje z osebnimi podatki, z namenom, da se izpolnijo zakonske zahteve glede obdelave in varovanja osebnih podatkov in zaščitijo pravice posameznikov, na katere se osebni podatki nanašajo.

2. člen

Pri obdelavi osebnih podatkov zaposleni upoštevajo splošna načela v zvezi z obdelavo osebnih podatkov in obdelujejo le tiste osebne podatke, za katere obstaja zakonska podlaga na podlagi določb ZVOP-2 in GDPR.

3. člen

Ta Pravilnik velja za vse osebe, ki pri delodajalcu opravljajo delo, ne glede na to, ali so z njim v delovnem razmerju (v nadaljevanju zaposleni).

Delodajalec je Rudolfovo.

4. člen

Izrazi, ki se uporabljajo v tem Pravilniku, imajo pomene, kot izhajajo iz veljavnega ZVOP-2 ter GDPR.

II. Seznam evidenc dejavnosti obdelave osebnih podatkov

5. člen

Sestavni del tega pravilnika je Seznam evidenc dejavnosti obdelave osebnih podatkov (v nadaljevanju: Seznam evidenc). Seznam evidenc je objavljen v dokumentnemu sistemu delodajalca.

Direktor imenuje osebo, odgovorno za vodenje Seznama evidenc (v nadaljevanju odgovorna oseba).

Podatke v Seznam evidenc vnašajo zaposleni ali odgovorna oseba. Zaposleni sproti vnašajo spremembe v Seznam evidenc. V koledarskem letu odgovorna oseba z zaposlenimi vsaj enkrat preveri veljavnost podatkov v Seznamu evidenc.

III. Kadrovski ukrepi

6. člen

Zaposleni, ki obdeluje osebne podatke, je dolžan podatke obdelovati v skladu z GDPR, ZVOP-2, s tem pravilnikom in krovno politiko informacijske varnosti.

Zaposleni sme osebne podatke, do katerih dostopa uporabljati samo za zakoniti namen, za katerega so bili zbrani.

Za kršitev določil iz tega člena so zaposleni disciplinsko, odškodninsko in kazensko odgovorni. Kršitev določil tega Pravilnika se šteje za hujšo kršitev pravic in obveznosti iz delovnega razmerja, kar lahko predstavlja podlago za odpoved pogodbe o zaposlitvi.

IV. Fizična varnost

7. člen

Zaposleni v svoji odsotnosti z delovnega mesta ali ob prisotnosti oseb, ki nimajo pravice vpogleda v osebne podatke, upoštevajo t. i. politiko čiste mize in politiko čistega ekrana in nosilcev osebnih podatkov ne puščajo na mizah, računalniške ekrane pa fizično ali programsko zaklepajo.

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

Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.

V. Varovanje integritete in zaupnosti podatkov ob sprejemu in prenosu

8. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte:

1) mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku ali enoti, na katero je pošiljka naslovljena,
2) odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo k upravljavcu, razen pošiljk iz tretje in četrte točke tega člena,
3) ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki,
4) ne sme odpirati pošiljk, naslovljenih na zaposlenega, na katerih 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 upravljavca.

9. člen

Osebni podatki, ki se pošiljajo fizično, se pošiljajo s priporočeno pošto ali osebno preko kurirja.

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

10.člen

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

V primeru elektronskega pošiljanja sporočil z osebnimi podatki se uporabi tehnične postopke, ki onemogočijo prestrezanje, kopiranje, spreminjanje, preusmerjanje ali uničenje prenesenih informacij.

11.člen

Obdelava posebnih vrst osebnih podatkov mora biti posebej označena in zavarovana.
Med posebne vrste osebnih podatkov sodijo podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

Posebne vrste osebnih podatkov se pošiljajo naslovnikom v zaprtih ovojnicah iz 2. odstavka 10. člena proti podpisu v dostavni knjigi ali z vročilnico.
Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij samo, če se zagotovi, da do podatkov ne bodo dostopale nepooblaščene oseb (npr. kriptografija, zaščita z geslom).

VI. Zagotavljanje zaupnosti, celovitosti in odpornosti sistemov in storitev za obdelavo podatkov

12.člen

Vsakemu uporabniku se dodeliti jasno (osebno) uporabniško ime (ID oznaka uporabnika). To velja tudi za privilegirane pravice do dostopa (npr. za administratorje).

Dostopne pravice se preverja in ažurira vsaj enkrat v koledarskem letu.

Če delavec zamenja delovno mesto, se pravice dostopa preveri in po potrebi prilagodi.

Ob prenehanju delovnega razmerja, se mora najpozneje ob koncu zadnjega delovnega dne odvzeti dostopne pravice.

13.člen

Zunanji dostopi, ki so namenjeni vzdrževanju, se aktivirajo le za čas trajanja vzdrževanja in če je možno po predhodno izvedenem formalnem in dokumentiranem zahtevku. Po prenehanju vzdrževalnih del se ti podeljeni dostopi za vzdrževanje deaktivirajo oz. onemogočijo.

Zunanjemu ponudniku storitev se najkasneje zadnji dan veljavnosti pogodbe odvzame dostopne pravice.

14.člen

Vsi osebni računalniki, na katerih je možen dostop do osebnih podatkov, so varovani z uporabniškim imenom in geslom.

VII. Zagotavljanje dostopnosti oz. razpoložljivosti podatkov

15.člen

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

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakonska podlaga, ki uporabnika pooblašča za

pridobitev osebnih podatkov, ali pa mora biti k vlogi priložena pisna zahteva oz. privolitev posameznika, na katerega se podatki nanašajo.

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

Znotraj delovnega procesa smejo osebne podatke obdelovati le zaposleni, ki imajo pravno podlago za obdelavo osebnih podatkov.

16. člen

Zaposleni morajo paziti na službeni računalnik, ki jim je dodeljen za opravljanje delovnih nalog in ga ne smejo dajati v uporabo drugim osebam. O odtujitvi ali nedovoljenemu dostopu mora zaposleni obvestiti delodajalca in pristojne organe pregona.

IX. Rok hrambe in brisanje podatkov

17. člen

V Seznamu evidenc je določen rok za izbris osebnih podatkov.

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

18. člen

Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov. Brisanje mora biti popolno in nepovratno. Poleg nosilca takih podatkov je potrebno uničiti tudi podatke v mapi »Izbrisano« ali »Koš« oz. drugi ustrezni mapi/direktoriju, tako da vsebine ni več moč obnoviti.

Podatki na klasičnih medijih (listine, kartoteke, register, seznam ipd.) 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 oz. neuspešne izpise ipd.).

Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

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

Ob prenehanju delovnega razmerja mora zaposleni odstraniti zasebne informacije iz elektronske pošte, računalnika in centralnega sistema in vrniti službeni računalnik, če ni dogovorjeno drugače.

Ob prenehanju delovnega razmerja in ob zamenjavah se računalnik informacijsko očisti. Elektronski naslov nekdanjega zaposlenega se deaktivira, hkrati nastavi avtomatsko obvestilo o neobstoju e-naslova in informacijo o morebitnem novem kontaktnem elektronskem naslovu. Delodajalec elektronsko pošto arhivira in do vsebine arhivirane elektronske pošte dostopa zaposleni po pooblastilu direktorja v primeru, ko informacij, potrebnih za poslovanje ni mogoče pridobiti iz drugih virov.

XI. Poročanje v primeru varnostnega incidenta

19. člen

Vsi zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, nedostopnosti, spreminjanju ali poškodovanju podatkov, takoj obvestiti odgovorno osebo ali osebo s področja informatike, sami pa poskušajo takšno aktivnost preprečiti.

Odgovorna oseba ali oseba s področja informatike v evidenco varnostnih incidentov beleži vsako kršitev varstva osebnih podatkov, iz katere morajo biti razvidna dejstva v zvezi s kršitvijo varstva osebnih podatkov, učinki take kršitve in sprejeti popravni ukrepi.

V evidenco varnostnih incidentov se po kronološkem vrstnem redu vpisujejo vsi varnostni incidenti, ne glede na stopnjo in vrsto tveganja za pravice in svoboščine posameznikov. Odgovorna oseba ali oseba s področja informatike zlasti beleži kršitve zaupnosti podatkov (npr. nepooblaščeno razkritje podatkov), kršitve v zvezi z možnostjo dostopa do podatkov in kršitve integritete podatkov (npr. nepooblaščena sprememba podatkov).

20. člen

Če obstaja nezanemarljivo tveganje, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, mora delodajalec nemudoma, najkasneje pa v roku 72 ur po seznanitvi s kršitvijo, o njej uradno obvestiti pristojni nadzorni organ, skladno s 33. členom Splošne uredbe o varstvu podatkov.

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikom, mora delodajalec, skladno z določbo 34. člena Splošne uredbe o varstvu podatkov, brez nepotrebnega odlašanja obvestiti tudi posameznike, na katere se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

XII. Končne določbe

21. člen

Vse spremembe in dopolnitve tega Pravilnika se sprejmejo na enak način kot Pravilnik in v pisni obliki.

22. člen

Zaposleni je bil predlog v razpravo poslan preko internega glasila dne 23. 9. 2024.

Pravilnik prične veljati naslednji dan, ko ga sprejme upravni odbor.

Veljavna verzija pravilnika je dostopna v dokumentnem sistemu Rudolfovega.

Rudolfovo – Znanstveno in tehnološko središče Novo mesto
predsednik upravnega odbora
dr. Tomaž Savšek

E-žig ustvarjen za:
Tomaž Savšek
tomaz.savsek@siol.net

Napredni e-žig s kvalificiranim potrdilom
Imetnik potrdila: PODPISOVANJE
Datum e-žiga: 18.10.2024
Potek veljavnosti potrdila: 29.11.2028