Na podlagi 32. člena Splošne 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 (GDPR), Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/2022) in 11. člena Sklepa o ustanovitvi Javne agencije Republike Slovenije za zdravila in medicinske pripomočke (Uradni list RS, št. 115/06 in 70/17) je Svet Javne agencije Republike Slovenije za zdravila in medicinske pripomočke na 7. redni seji, dne 23. 2. 2023, sprejel naslednji

PRAVILNIK
o varstvu osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen
(Vsebina in namen pravilnika)

(1) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za varnost osebnih podatkov pri Javni agenciji Republike Slovenije za zdravila in medicinske pripomočke (v nadaljevanju: JAZMP) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava osebnih podatkov.

(2) Zaposleni pri JAZMP in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z določbami nacionalne zakonodaje s področja varstva osebnih podatkov, GDPR, s področno zakonodajo, ki ureja posamezno področje njihovega dela, ter z vsebino tega pravilnika.

2. člen
(Pomen izrazov)

Izrazi, uporabljeni v tem pravilniku, pomenijo:

1. **Nosilec podatkov** so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov ipd.).

2. **Obdelava osebnih podatkov** je 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.

3. **Obdelovalec** je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca.

4. **Osebni podatek** je katerokoli informacija v zvezi z določenim ali določljivim posameznikom, na katerega se nanašajo osebni podatki; določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

5. **Posebna vrsta osebnih podatkov** so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem in filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, biometričnih in genetskih značilnosti ter podatki o vpisu ali izbrisu v ali iz kazenske ali prekrškovne evidence.

6. **Uporabnik osebnih podatkov** je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice in zaposleni na JAZMP ne štejejo za uporabnike.

7. **Upravljavec** je fizična ali pravna oseba, javni organ, agencija ali drugi subjekt, ki sam ali skupaj z drugimi določa namene in sredstva obdelave, oziroma oseba, določena z zakonom, ki določa tudi namen in sredstva obdelave.

8. **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.

II. OBDELAVA OSEBNIH PODATKOV

3. člen
(Vzpostavitev zbirke osebnih podatkov)

Posamezno zbirko osebnih podatkov na posameznem delovnem področju JAZMP vzpostavi odgovorna oseba za določeno zbirko osebnih podatkov (v nadaljevanju: odgovorna oseba), ki jo določi direktor. Odgovorna oseba pred vzpostavitvijo zbirke obvesti pooblaščeno osebo za varstvo osebnih podatkov.

4. člen
(Obdelava osebnih podatkov)

(1) V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno zakonsko podlago po določbah GDPR in nacionalne zakonodaje s področja varstva osebnih podatkov.

(2) Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.

(3) Posebne vrste osebnih podatkov morajo biti pri obdelavi posebej označene in varovane tako, da se nepooblaščenim osebam onemogoči dostop do njih.

(4) O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbo 13. in 14. člena GDPR.

(5) Odgovorne osebe ter osebe, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke (v nadaljevanju: pooblaščeni obdelovalci), morajo biti pred obdelavo osebnih podatkov seznanjene z določbami GDPR ter z vsebino tega pravilnika.

5. člen
(Evidentiranje dokumentov)

Za evidentiranje zadev, dosjejev in dokumentov, ki vsebujejo osebne podatke, se uporabljajo določbe predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.

6. člen
(Posredovanje osebnih podatkov)

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

(2) Osebni podatki se po uradni dolžnosti posredujejo samo tistim uporabnikom, ki imajo ustrezno zakonsko podlago.

(3) Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno. Zahteva za posredovanje osebnih podatkov vsebuje podatke o vlagatelju zahteve, podpis vlagatelja ali pooblaščene osebe, pravno podlago za pridobitev zahtevanih podatkov, namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve, predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni, ter navedbo organa ali drugega subjekta, ki obravnava zadevo, vrste osebnih podatkov, ki naj se mu posredujejo ter obliko in način pridobitve zahtevanih osebnih podatkov.

(4) Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom, oziroma v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče uporabiti brez vidne sledi odpiranja ovojnice.

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

(6) Posebne vrste osebnih podatkov je dovoljeno posredovati preko komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

(7) Originalni dokument, ki vsebuje osebne podatke, se lahko posreduje uporabniku samo na podlagi pisne odredbe sodišča, poziva pristojnega organa ali v drugih primerih, ki jih določa zakon. Posredovani originalni dokument mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

7. člen
(Evidenca posredovanj)

(1) Vsako posredovanje osebnih podatkov iz prejšnjega člena se zabeleži z navedbo naslednjih podatkov:

- kateri osebni podatki so bili posredovani,
- komu so bili posredovani osebni podatki, oziroma navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
- datum posredovanja osebnih podatkov,
- za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka ter
- pravna podlaga, na kateri so bili posredovani osebni podatki.

(2) Podatki iz prejšnjega odstavka so v pisni ali elektronski obliki kot del podatkov zadeve, o kateri se vodi postopek. Oblika zabeležbe je odvisna od nosilca podatkov, ki vsebuje posredovani osebni podatek (spis, informacijski sistem za podporo pisarniškemu poslovanju).

(3) Če osebni podatek, ki se posreduje, ni del podatkov zadeve, o kateri se vodi postopek, se zabeležba iz prvega odstavka tega člena v obliki iz prejšnjega odstavka evidentira neposredno v zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek.

(4) Zabeležbo iz prvega odstavka tega člena naredi odgovorna oseba ali pooblaščeni obdelovalec, ki je osebne podatke posredoval uporabniku.

8. člen
(Posredovanje osebnih podatkov znotraj JAZMP)

(1) Dokumenti, ki vsebujejo osebne podatke zaposlenega pri JAZMP, se zaposlenemu, na katerega se osebni podatki nanašajo, posredujejo v skladu s tretjim odstavkom 6. člena tega pravilnika.

(2) Osebni podatki zaposlenih pri JAZMP in ostalih oseb se lahko posredujejo znotraj JAZMP tudi tistim osebam, ki jih potrebujejo v okviru opravljanja svojih del in nalog.

(3) Oseba iz četrtega odstavka prejšnjega člena mora zaznamovati vsako posredovanje posebnih vrst osebnih podatkov znotraj JAZMP v skladu s prejšnjim členom.

9. člen
(Pregledovanje, prepisovanje in kopiranje osebnih podatkov s strani strank oziroma upravičencev)

(1) Za pregledovanje, prepisovanje in kopiranje dokumentov, ki vsebujejo osebne podatke, se uporabljajo določbe predpisov, ki urejajo splošni upravni postopek in upravno poslovanje z dokumentarnim gradivom.

(2) Pred pregledom, prepisovanjem ali kopiranjem dokumentov, ki vsebujejo osebne podatke, je treba preveriti identiteto stranke oziroma vsakega drugega, ki verjetno izkaže, da ima od pregledovanja, prepisovanja ali preslikavanja pravno korist (v nadaljevanju: upravičenec) z vpogledom v njegovo osebno izkaznico, potni list, vozniško dovoljenje ali drug dokument, ki nedvoumno izkazuje njegovo istovetnost.

(3) Pri vsakem posameznem pregledovanju, prepisovanju ali kopiranju dokumentov po tem členu, ki vsebujejo osebne podatke, se naredi uradni zaznamek, ki se vloži v spis. Iz uradnega zaznamka, ki ga mora podpisati tudi stranka oziroma upravičenec, mora biti razvidna številka spisa, datum pregleda, vrsta dokumenta, katerega kopija se je posredovala upravičencu, osebno ime stranke oziroma upravičenca, njegov naslov, številka in vrsta dokumenta, iz katerega je ugotovljena identiteta ter namen, zaradi katerega je bil opravljen pregled, prepis oziroma kopiranje dokumenta.

(4) Stranko oziroma upravičenca je pred pregledom, prepisovanjem in kopiranjem dokumentov, ki vsebujejo osebne podatke, treba opozoriti na dolžnost varovanja takšnih podatkov. Opozorilo mora biti sestavni del uradnega zaznamka iz prejšnjega odstavka.

10. člen

(kopiranje in tiskanje osebnih podatkov s strani zaposlenih)

Zaposleni pri JAZMP, ki pri izvajanju svojih delovnih nalog kopirajo ali na drug tehnični način razmnožujejo ali tiskajo dokumente, ki vsebujejo osebne podatke, na napravah, ki jih uporablja večje število zaposlenih, po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob napravah.

11. člen
(Hramba osebnih podatkov)

(1) Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe, kot je razviden iz evidence dejavnosti obdelave za posamezno zbirko osebnih podatkov.

(2) Po poteku roka hrambe se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma, če zakon za posamezne vrste osebnih podatkov ne določa drugače.

(3) Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča obnovitev vseh ali dela brisanih podatkov.

(4) Osebni podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja).

(5) Uničenje nosilcev podatkov in pomožnega gradiva se zagotovi v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.

(6) Prepovedano je odmetavati odpadne nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).

(7) Pri prenosu nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, na mesto uničenja, je treba zagotoviti ustrezno varnost tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov.

(8) Prenos nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, na mesto uničenja ter uničevanje takih nosilcev podatkov nadzoruje posebna tričlanska komisija, ki jo imenuje direktor JAZMP.

(9) Komisijo iz prejšnjega odstavka sestavljajo zaposleni na JAZMP, en član komisije je odgovorna oseba.

(10) O uničenju iz osmega odstavka tega člena komisija sestavi zapisnik.

12. člen
(Evidenca dejavnosti obdelave)

(1) Opis zbirke osebnih podatkov, katerih upravljavec je JAZMP, se vodi v evidenci dejavnosti obdelave za posamezne zbirke osebnih podatkov, ki se vodi v skladu z določbami 30. člena GDPR.

(2) Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni z evidencami dejavnosti obdelave za posamezne zbirke osebnih podatkov.

(3) JAZMP zagotovi, da je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba (osebno ime in delovno mesto) je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe (osebno ime in delovno mesto) lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov.

III. PODROČNE UREDITVE VARSTVA OSEBNIH PODATKOV

13. člen
(Evidentiranje obiskovalcev)

(1) JAZMP lahko vodi knjigo obiskovalcev, v katero za namene varovanja premoženja ali telesa posameznika ter reda v prostorih JAZMP lahko vpiše vsako osebo, ki namerava vstopiti ali izstopiti iz prostorov JAZMP, z izjemo zaposlenih pri JAZMP.

(2) V knjigo obiskovalcev se lahko vpisujejo naslednji podatki:

- datum vpisa,
- osebno ime osebe, ki namerava vstopiti,
- številka in vrsta njenega osebnega dokumenta,
- razlog vstopa ter
- uro vstopa in izstopa.

(3) Osebni podatki v knjigah obiskovalcev in same knjige obiskovalcev se varujejo v skladu z določbami tega pravilnika.

(4) Za uničenje knjig obiskovalcev velja ureditev iz osmega odstavka 11. člena tega pravilnika.

14. člen
(Elektronska pošta, telefonski priključki in uporaba druge programske opreme na računalniku)

(1) Zaposleni morajo uporabljati elektronsko pošto in drugo programsko opremo na računalniku v skladu s Pravilnikom o informacijski varnostni politiki JAZMP (v nadaljevanju: informacijska varnostna politika).

(2) Vpogled v telefonske prometne podatke priključkov, katerih lastnik je JAZMP, lahko direktor zahteva od operaterjev telekomunikacijskih storitev le takrat, kadar pride med JAZMP in zaposlenim do kakršnegakoli spora glede višine stroškov porabe konkretnega priključka.

(3) O možnosti nadzora iz drugega odstavka tega člena mora biti zaposleni pisno obveščen. Kot zadostno obvestilo se šteje objava na intranetni strani JAZMP.

15. člen
(Internet)

Zaposleni morajo uporabljati internet v skladu z informacijsko varnostno politiko.

IV. VAROVANJE PROSTOROV, NOSILCEV PODATKOV, STROJNE IN PROGRAMSKE OPREME

16. člen
(Varovanje prostorov)

(1) Prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke ter strojna in programska oprema (v nadaljevanju: varovani prostor) morajo biti varovani z organizacijskimi in/ali tehničnimi ukrepi iz tega pravilnika, informacijske varnostne politike in hišnega reda, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

(2) Dostop do varovanih prostorov je mogoč v skladu z določbami informacijske varnostne politike in hišnega reda.

(3) Vsak zaposleni ima službeno kartico, s katero lahko vstopa v vse skupne prostore. Prostori glavne pisarne, sistemske sobe in prostora IT so zaščiteni z elektronskim zaklepanjem vrat. V prostore glavne pisarne lahko vstopajo samo zaposleni v glavni pisarni, v prostore sistemske sobe in pisarne IT pa le zaposleni v IT. Ostali varovani prostori so zaklenjeni s cilindričnimi ključavnicami. Dostop do posameznega varovanega prostora je dovoljen zaposlenim, ki svoje delovne aktivnosti opravljajo v tem prostoru. Poleg zaposlenih lahko v varovane prostore za potrebe opravljanja nalog vstopajo osebe, ki opravljajo naloge varovanja in čiščenja.

(4) Varovani prostori ne smejo ostati nenadzorovani oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo. Ključi se ne smejo puščati v ključavnici v vratih.

(5) V varovanih prostorih morajo biti po zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke, zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni. Ključe hrani zaposleni, ki nadzoruje posamezen varovani prostor, na zavarovanem mestu v varovanem prostoru.

(6) Omare, mize in drugo pohištvo z nosilci podatkov, ki vsebujejo osebne podatke, ki se nahajajo na hodnikih in v drugih skupnih prostorih, mora biti stalno zaklenjeno. Ključe hrani zaposleni, ki nadzoruje posamezno omaro, mizo ali drugo pohištvo, na zavarovanem mestu v varovanem prostoru, ki ga nadzoruje.

(7) Osebe, ki niso zaposlene na JAZMP (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji) se smejo gibati v varovanih prostorih samo z vednostjo zaposlenega, ki nadzoruje varovani prostor, kjer se oseba giba.

(8) Posebne vrste osebnih podatkov se ne smejo hraniti izven varovanih prostorov.

17. člen
(Varovanje nosilcev podatkov, ki vsebujejo osebne podatke)

(1) Zaposleni ne smejo puščati nosilcev podatkov, ki vsebujejo osebne podatke, na vidnem mestu (npr. na mizah) v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

(2) Nosilci podatkov, ki vsebujejo posebne vrste osebnih podatkov, se ne smejo hraniti izven varovanih prostorov ali odnašati izven prostorov JAZMP.

(3) Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni odnašajo izven prostorov JAZMP samo za namen opravljanja delovnih nalog.

(4) Nosilce podatkov, ki vsebujejo posebne vrste osebnih podatkov, lahko zaposleni izjemoma odnašajo izven prostorov JAZMP, če je to nujno potrebno za opravljanje delovnih nalog.

(5) Če zaposleni odnašajo nosilce podatkov, ki vsebujejo osebne podatke, izven prostorov JAZMP, morajo zagotoviti, da ne pride do nepooblaščenega vpogleda v osebne podatke.

(6) V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov, ki vsebujejo osebne podatke, in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

18. člen
(Varovanje strojne in programske opreme)

(1) Vzdrževanje in popravila strojne in računalniške in druge opreme je dovoljeno samo z vednostjo osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni serviserji in vzdrževalci. Ob predaji opreme v servis morata oseba, ki predaja opremo in oseba, ki jo sprejema v popravilo, izpolniti primopredajni zapisnik.

(2) Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo zaposlenim, ki jih določi oseba, zadolžena za delovanje računalniškega informacijskega sistema, ali pravnim ali fizičnim osebam, ki opravljajo dogovorjene storitve.

(3) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije ter posamezniki, ki za JAZMP na podlagi dogovora opravljajo dogovorjene storitve. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

(4) Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega pravilnika.

(5) Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, je zaščitena z ustrezno programsko opremo. Ob pojavu zlonamerne programske kode na programski opremi se to čim prej odpravi in ugotovi vzrok pojava.

(6) Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo k JAZMP na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo preverjeni z vidika prisotnosti zlonamerne programske kode.

(7) Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom uporabniških imen za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem uporabniških imen mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatkih vneseni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil glede na tveganja.

(8) Režim dodeljevanja, hranjenja in spreminjanja gesel je določen v Informacijski varnostni politiki.

(9) Postopke varnostnega kopiranja in posodabljanja varnostnih mehanizmov ureja Informacijska varnostna politika.

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

19. člen
(Pogodbena obdelava)

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov v imenu in za račun JAZMP (v nadaljevanju: obdelovalec), JAZMP sklene pisno pogodbo v skladu z 28. členom GDPR.

(2) Pogodba iz prejšnjega odstavka mora obvezno vsebovati tudi postopke in ukrepe za zagotovitev varstva osebnih podatkov.

(3) Prejšnji odstavek velja tudi za obdelovalce, ki vzdržujejo obstoječo strojno in programsko opremo ter izdelujejo in inštalirajo novo strojno ali programsko opremo.

(4) Obdelovalci lahko opravljajo storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe iz prvega odstavka tega člena in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

(5) Obdelovalci, ki za JAZMP opravljajo pogodbeno dogovorjene storitve izven prostorov JAZMP, morajo imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

(6) Vodi se seznam zunanjih izvajalcev, ki vsebuje: naziv in sedež pravne osebe, ime in priimek oseb, ki izvajajo zunanje storitve ter kontaktne podatke teh oseb (naslov e-pošte in telefonska številka).

VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

20. člen
(Obveščanje)

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

VII. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA VARNOST OSEBNIH PODATKOV

21. člen
(Izvajanje postopkov in ukrepov)

Vsak, ki obdeluje osebne podatke, je dolžan izvajati s tem pravilnikom predpisane postopke in ukrepe za varnost osebnih podatkov in varovati osebne podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

22. člen
(Vodenje dnevnikov obdelav osebnih podatkov)

(1) Kadar se v avtomatiziranih sistemih obdelave osebnih podatkov izvajajo obsežne obdelave posebnih vrst osebnih podatkov, ali kadar gre za redno in sistematično spremljanje posameznikov, ali kadar je z oceno učinka ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave, ali če tako določa zakon, je treba voditi dnevnik obdelave osebnih podatkov.

(2) Dnevnik obdelave osebnih podatkov vključuje podatke o naslednjih obdelavah osebnih podatkov: zbiranje, spreminjanje, vpogled, razkritje, vključno s prenosi, izbris in druga dejanja obdelave, ki jih določa zakon.

(3) Dnevnik obdelave mora za dejanja obdelave iz prejšnjega odstavka vsebovati vrsto dejanja obdelave, datum in čas obdelave, identifikacijo osebe, ki je izvedla dejanje obdelave, ter identifikacijo uporabnikov osebnih podatkov, da je mogoče naknadno ugotoviti točno identiteto teh oseb. Ob upoštevanju ocene učinka se lahko določijo dodatne vsebine dnevnika obdelave.

(3) Dnevnik obdelave se uporablja le za izkazovanje zakonitosti obdelave ter izvajanje notranjega nadzora, izvajanje nadzorov ali drugih zakonsko določenih preverjanj s strani nadzornega organa ali drugih pristojnih organov, zagotavljanje celovitosti in varnosti osebnih podatkov ter za odpravljanje napak v delovanju informacijskega sistema ali obdelavi podatkov.

23. člen
(nadzor nad izvajanjem)

(1) Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja oseba pooblaščena za varstvo osebnih podatkov oziroma oseba, ki jo za to pooblasti direktor.

(2) Nadzor nad obdelavo osebnih podatkov se lahko izvaja preko nadzora dnevnikov obdelave osebnih podatkov. Pri pregledu dnevnikov je treba biti pozoren predvsem na skladnost obdelave z delovnimi nalogami odgovorne osebe ali pooblaščene osebe za obdelavo, skladnost časa obdelav z delovnim časom uporabnika (možnost, da je kdo drug uporabil pravice za dostop), izdelavo posameznih »občutljivih« izpisov in vpogled v podatke oseb, ki so v javnosti izpostavljene oziroma zanje velja večje tveganje.

24. člen
(Izjava)

(1) Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov in drugih zaupnih podatkov.

(2) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami zakonodaje s področja varstva osebnih podatkov, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega pravilnika in predmetne zakonodaje.

(3) Navedeno se smiselno uporablja tudi za druge oblike občasnega dela študentov ali drugih posameznikov, ki sklenejo z JAZMP pogodbo za opravljanje občasnih del, kar ne vključuje pogodbenih obdelovalcev.

25. člen
(Vodenje evidence kršitev osebnih podatkov ter sporočanje nadzornemu organu in posameznikom)

(1) Pooblaščena oseba za varstvo osebnih podatkov JAZMP ali druga oseba, ki jo za to pooblasti direktor JAZMP, vodi evidenco kršitev varstva osebnih podatkov. Evidenca vsebuje podatke o datumu in uri kršitve, vsebini kršitve, datumu in uri prijave kršitve pri nadzornem organu, vsebino učinkov na varstvo zasebnosti posameznikov in izvedene aktivnosti na podlagi kršitve (vključno z obveščanjem posameznikov).

(2) V primeru kršitve varstva osebnih podatkov, katerih posledice ogrožajo pravice in svoboščine posameznikov, pooblaščena oseba za varstvo osebnih podatkov o kršitvi obvesti nadzorni organ (Informacijski pooblaščenec) najkasneje v 72 urah. Prijava kršitve pri nadzornem organu vsebuje

podatke o nazivu upravljavca, vsebino narave kršitve, oceno učinkov na varstvo pravice posameznikov do zasebnosti, seznamu že izvedenih ukrepov za ustrezno zavarovanje in načrtovanih ukrepih in razlogih za morebitno zamudo pri prijavi. V primeru suma storitve kaznivega dejanja pooblaščena oseba za varstvo osebnih podatkov kršitev sporoči tudi policiji ali tožilstvu.

(3) Če kršitev pomeni veliko tveganje za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, pooblaščena oseba za varstvo osebnih podatkov brez nepotrebnega odlašanja o kršitvi obvesti posameznika, na katerega se nanašajo osebni podatki.

26. člen
(Odgovornost za kršitev)

(1) Kršitev določil tega pravilnika s strani zaposlenih pomeni kršenje obveznosti iz delovnega razmerja, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

(2) Odgovornost iz prejšnjega odstavka ne izključuje kazenske ali odškodninske odgovornosti.

VIII. KONČNE DOLOČBE

27. člen
(Začetek veljavnosti)

(1) Z dnem začetka uporabe tega pravilnika preneha veljati Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov na Javni agenciji Republike Slovenije za zdravila in medicinske pripomočke št. 05-3/2016-1, z dne 24.5.2016.

(2) Ta pravilnik začne veljati z dnem, ko ga sprejme svet JAZMP in je objavljen na oglasni deski oziroma intranetu JAZMP.

JAVNA AGENCIJA REPUBLIKE SLOVENIJE ZA ZDRAVILA IN MEDICINSKE PRIPOMOČKE
REPUBLIKA SLOVENIJA

Številka: 05-1/2023-1
Ljubljana, 23. 2. 2023

Predsednica sveta JAZMP
mag. Vlasta Mežek