Na podlagi Statuta Regionalne razvojne agencije Posavje, direktor javnega zavoda RRA Posavje izdajam

PRAVILNIK
o zavarovanju osebnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v Regionalni razvojni agenciji Posavje (v nadaljevanju RRA Posavje), 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, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z zakonom, ki ureja varstvo osebnih podatkov, Splošno uredbo EU o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Uredba), s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. člen

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

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je RRA Posavje, se vodi v evidenci dejavnosti obdelave (opisu zbirk osebnih podatkov), ki se vodi v skladu z določbami 30. člena Uredbe. Evidenca se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

Zaposleni, ki obdelujejo osebne podatke, morejo biti seznanjeni z evidenco dejavnosti obdelave, vpogled vanjo pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

Oseba, ki jo za to pooblasti direktor, je dolžna voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov. V seznam se vpisujejo naslednji podatki: naziv zbirke osebnih podatkov, osebno ime in / ali delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov ter osebno ime in / ali delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov, po potrebi pa tudi omejitve dostopa.

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

Prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in / ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja vodje (direktorja).

Obdelava osebnih podatkov je dovoljena le v prostorih RRA Posavje. Nosilcev osebnih podatkov ni dovoljeno iznašati iz prostorov RRA Posavje brez izrecnega dovoljenja nadrejenega.

Posredovanje tretjim osebam je na podlagi ustrezne pravne podlage mogoče samo z dovoljenjem vodstva, o čemer se takšno posredovanje zabeleži v knjigo evidenc o manipulaciji z osebnimi podatki.

Nosilci osebnih podatkov, ki so hranjeni izven delovnih prostorov, morajo biti zaklenjeni v ognjevarni in protivlomni omari. Na enak način morajo biti nosilci shranjeni tudi izven delovnega časa.

Ključi varovanih prostorov se uporabljajo in hranijo v skladu z navodili direktorja. Ključi se ne puščajo v ključavnici v vratih od zunanje strani ali na drugačen način, ki bi omogočal dostop nepooblaščenih oseb do njih.

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

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.

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.

Dostop do varovanih prostorov (tajništvo, pisarna kadrovika, likvidatura plač, pasivni arhivi in podobno) imajo samo zaposleni, ki so za to pooblaščeni s strani direktorja. Osebe, ki niso pooblaščene, lahko v te prostore vstopijo zgolj z dovoljenjem in v spremstvu pooblaščene osebe. Delavec mora v času prisotnosti v varovanih prostorih, te nadzorovati in po odhodi iz njih prostor zakleniti.

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

Zaposleni lahko obdelujejo zgolj tiste osebne podatke, za obdelavo katerih jih zadolži pooblaščeni nadrejeni ali odgovorna oseba za posamezno zbirko osebnih podatkov.

5. člen

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

6. člen

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z RRA Posavje sklenjeno ustrezno pogodbo.

7. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v zavarovanih prostorih samo z vednostjo pooblaščene osebe. Zaposleni, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

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

8. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

9. člen

Pristojna oseba, zadolžena za informacijsko varnost, zagotovi naslednje:

- določi stopnje zaupnosti podatkov za vse osebne podatke, ki jih obdeluje RRA Posavje ;
- glede na naravo dela in potrebe posameznega zaposlenega ali pogodbenega obdelovalca ali uporabnika, vsakemu uporabniku informacijskega sistema dodeli ustrezne pravice samo v obsegu, ki je nujen za njegovo delo;
- vodi uporabniško dokumentacijo za vsakega posameznega uporabnika sistema, in sicer z vsemi potrebnimi podatki o dodelitvi pravic, gesel in drugimi podatki, potrebnimi za zagotavljanje varnega delovanja informacijskega sistema;
- pisno določi postopke dodeljevanja / spreminjanja / odvzemanja uporabniških pooblastil in te postopke tudi dosledno izvaja.

10. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, ki imajo z RRA Posavje sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

Pristojna oseba, zadolžena za informacijsko varnost, za vsak poseg vzdrževanja, nadgradnje in ostalih posegov v informacijski sistem vodi evidenco, iz katere je razvidno naslednje:

- datum in ura, kdaj je bilo opravilo izvedeno;
- kdo je posegel v informacijski sistem;
- kakšen je bil namen posega;
- kaj je bilo narejeno med posegom.

11. člen

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

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. O prehodu se izdela kratek zapisnik.

12. člen

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

13. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa se tega čimprej odpravi s pomočjo pooblaščene osebe, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu.

Ob vsakem sumu vdora v informacijski sistem RRA Posavje ali kakršenkoli drug varnostni incident, se mora začeti preiskovati takoj, ko se zanj izve. Pooblaščeni delavec RRA Posavje mora zagotoviti, da se vsak vdor v informacijski sistem takoj blokira, nato pa je treba incident preiskati, ugotoviti pomanjkljivosti v sistemu in v pisnem poročilu o incidentu navesti uveljavljene izboljšave.

Ob zaznavi incidenta morajo zaposleni ravnati v skladu s poglavjem 7 tega pravilnika.

Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo v RRA Posavje na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

14. člen

Zaposleni ne smejo namestiti programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz RRA Posavje brez odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema.

15. člen

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani (kar vključuje tudi vpogled) ter kdo je to storil. V sistemih, kjer je to možno, mora biti zagotovljen tudi podatek o tem, za kakšen namen se je določeni osebni podatek obdeloval.

Vsak administratorski dostop do informacijskega sistema RRA Posavje mora biti zabeležen na način, da spreminjanje podatkov v dnevniku dogodkov (žurnalu) ni mogoče. Takšni podatki morajo biti celoviti in avtentični.

Pooblaščena oseba določi režim dodeljevanja hranjenja in spreminjanja gesel.

Katerokoli geslo, ki je v uporabi v informacijskem sistemu RRA Posavje, 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 slovarja. Vsak zaposleni je dolžan geslo zamenjati vsaj enkrat na 3 mesece, pooblaščeni delavec pa na strežniškem sistemu omogoči samodejno opozarjanje na potrebno menjavo gesla. 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.

Vse delovne postaje, ki jih zaposleni uporabljajo pri svojem delu, morajo biti kriptirane.

16. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervizorska oz. nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnicah in se jih skrbno varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob resnično nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

17. člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki tam nahajajo.

Kopije iz prejšnjega odstavka se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena. Ta mesta morajo biti fizično ločena od lokacije RRA Posavje, fizični prenos med obema lokacijama pa lahko opravi samo pooblaščena oseba, ki jo določi direktor. V nobenem trenutku fizičnega prenosa takšna kopija ne sme ostati nenadzorovana.

Za potrebe evidentiranja in nadzora nad varnostnimi kopijami je zadolžena oseba, ki jo določi direktor.

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

18. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (obdelovalec), se sklene pisna pogodba, predvidena v tretjem odstavku 28. člena Uredbe. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo, če imajo te dostop do osebnih podatkov.

Zunanje pravne ali fizične osebe smejo opravljati storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil in določenega obsega vrste osebnih podatkov ter teh ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pravna ali fizična oseba, ki za RRA Posavje opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

Pooblaščeni delavec RRA Posavje vodi ažurno evidenco vseh sklenjenih pogodb o pogodbeni obdelavi osebnih podatkov.

V. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

19. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki neposredno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v RRA Posavje – prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drugo organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki.

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 položaja in šele nato naslov RRA Posavje.

20. člen

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

POSEBNE VRSTE osebnih podatkov se fizično pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali s povratnico.

Osebni podatki se pošiljajo priporočeno.

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.

21. člen

Obdelava posebnih vrst osebnih podatkov mora biti posebej označena in zavarovana. Vsak dokument, datoteka ali mapa, ki vsebuje posebne vrste osebnih podatkov, mora biti označen z napisom »Posebne vrste osebnih podatkov«.

Podatki iz prejšnjega odstavka 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.

22. člen

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

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona ali Uredbe, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

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

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

VI. BRISANJE PODATKOV

23. člen

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

Roki, po katerih se osebni podatki izbrišejo iz zbirke podatkov, so razvidni iz evidence dejavnosti obdelave.

24. člen

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

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

Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma 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.

Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje oseba, ki jo določi direktor in ki po uničenju sestavi kratek zapisnik o načinu in temeljitosti uničenja.

VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA IN OBVEŠČANJE

25. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščeno obdelavo osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj (najkasneje v roku 1 ure od zaznave morebitnega incidenta ali škodnega dogodka) obvestiti direktorja ali od direktorja pooblaščeno osebo, sami pa poskušajo takšno aktivnost preprečiti, ne da bi pri tem ogrožali svoje zdravje in življenje.

25.a člen
(Obveščanje Informacijskega pooblaščenca)

V primeru kršitve varstva osebnih podatkov mora pooblaščena oseba najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvestiti Informacijskega pooblaščenca Republike Slovenje, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov.

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 RRA Posavje sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

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

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 RRA Posavje sklene z obdelovalcem.

Pooblaščena 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 služba dolžna razkriti Informacijskemu pooblaščencu, če ta tako zahteva.

Vsi zaposleni, ki delajo na raziskavi incidenta ali so kakorkoli povezane z odpravljanjem posledic incidenta, morajo pooblaščeno obveščati takoj o vseh informacijah, povezanih z incidentom.

25.b člen
(Obveščanje posameznika)

Če pooblaščena oseba oceni, da je verjetno, da je kršitev varstva osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, mora najkasneje v roku 24 ur sporočiti posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

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

Sporočilo posamezniku iz prvega odstavka ni potrebno v naslednjih primerih:

- pristojna služba RRA Posavje 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 RRA Posavje 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.

Vsi zaposleni, ki delajo na raziskavi incidenta ali so kakorkoli povezani z odpravljanjem posledic incidenta, morajo pooblaščeno osebo obveščati takoj o vseh informacijah, povezanih z incidentom.

VIII. POOBLAŠČENA OSEBA

26. člen
Pooblaščena oseba je oseba, ki jo določi direktor.

IX. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

27. člen
Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov direktor določi odgovorne osebe za posamezno zbirko osebnih podatkov.

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

Pred nastopom dela na delovno mesto, kjer se osebni podatki obdelujejo, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov – vzorec izjave je Priloga 1 tega pravilnika in je njegov sestavni del. Enako izjavo morajo podpisati pogodbeni obdelovalci RRA Posavje.

29. člen

Za kršitev določil tega pravilnika so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

X. KONČNE DOLOČBE:

30. člen

Ta pravilnik prične veljati dne 17.12.2018

Ime in priimek,
direktor Martin Bratanič

RRA POSAVJE
Regionalna razvojna agencija Posavje
RRA POSAVJE, CKŽ 2, 8270 KRŠKO

V Krškem, dne 17.12.2018

Priloga 1

Izjava delavca o varnosti osebnih podatkov

Spodaj podpisani _____ potrjujem, da sem prebral Pravilnik o zavarovanju osebnih podatkov RRA Posavje, ga razumem in se zavezujem k njegovemu izrecnemu uveljavljanju ves čas mojega dela za družbo, kakor tudi po prenehanju mojega dela.

Podpis: _____ Datum in kraj: _____