

Na podlagi 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljnjem besedilu: ZVOP-1) in prvega odstavka 25. člena Akta o ustanovitvi Eko sklada, Slovenskega okoljskega javnega sklada (Uradni list RS, št. 112/09, 1/12, 98/12 in 20/13) direktor Eko sklada, Slovenskega okoljskega javnega sklada, sprejme naslednji

PRAVILNIK O VARSTVU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen

(1) Ta pravilnik določa splošne postopke in ukrepe za varovanje osebnih podatkov, vodenih v zbirkah osebnih podatkov, s katerimi upravlja Eko sklad, Slovenski okoljski javni sklad, Bleiweisova cesta 30, 1000 Ljubljana, matična številka: 5854067000 (v nadaljnjem besedilu: upravljavec osebnih podatkov). Pravilnik obsega splošne ukrepe za varovanje zbirk osebnih podatkov pri njihovem zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi. Konkretni postopki in ukrepi za varovanje osebnih podatkov so opisani v operacijskem predpisu o postopkih in ukrepih za varstvo zbirk osebnih podatkov (v nadaljnjem besedilu: operacijski predpis za varstvo osebnih podatkov), ki ga upravljavec osebnih podatkov sprejme na podlagi tega pravilnika.

(2) Namen tega pravilnika je zagotoviti skladnost delovanja upravljavca osebnih podatkov s predpisi s področja varstva osebnih podatkov.

2. člen

Izrazi, ki so uporabljeni v tem pravilniku, imajo naslednji pomen:

Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.

Posameznik je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

Obdelava osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).

Zbirka osebnih podatkov je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

Upravljavac osebnih podatkov je Eko sklad, Slovenski okoljski javni sklad, Bleiweisova cesta 30, 1000 Ljubljana, matična številka: 5854067000, ki sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov.

Pogodbeni obdelovalec je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov.

Uporabnik osebnih podatkov je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki.

Posredovanje osebnih podatkov je posredovanje ali razkritje osebnih podatkov.

Tretja država je država, ki ni država članica Evropske unije ali del Evropskega gospodarskega prostora.

Katalog zbirke osebnih podatkov je opis zbirke osebnih podatkov.

Osebna privolitev posameznika je prostovoljna izjava volje posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen, in je dana na podlagi informacij, ki mu jih mora zagotoviti upravljavac osebnih podatkov po ZVOP-1; osebna privolitev posameznika je lahko pisna, ustna ali druga ustrezna privolitev posameznika.

Občutljivi osebni podatki so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške; občutljivi osebni podatki so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

Pravilnik o varstvu osebnih podatkov določa splošne postopke in ukrepe za varovanje osebnih podatkov v zbirkah osebnih podatkov upravljavca osebnih podatkov.

Operacijski predpis o postopkih in ukrepih za varstvo zbirk osebnih podatkov vsebuje opis konkretnih postopkov in ukrepov za varovanje osebnih podatkov v zbirkah osebnih podatkov upravljavca osebnih podatkov.

II. ZBIRKE OSEBNIH PODATKOV

3. člen

Upravljavac osebnih podatkov v katalogu zbirke osebnih podatkov za vsako zbirko osebnih podatkov navede:

- naziv zbirke osebnih podatkov;
- podatke o upravljavcu osebnih podatkov (naziv oziroma firmo in naslov oziroma sedež upravljavca osebnih podatkov in matično številko);
- pravno podlago za obdelavo osebnih podatkov;
- kategorije posameznikov, na katere se nanašajo osebni podatki;
- vrste osebnih podatkov v zbirki osebnih podatkov;
- namen obdelave;

- rok hrambe osebnih podatkov;
- omejitve pravic posameznikov glede osebnih podatkov v zbirki osebnih podatkov in pravno podlago omejitev;
- uporabnike ali kategorije uporabnikov osebnih podatkov, vsebovanih v zbirki osebnih podatkov;
- dejstvo, ali se osebni podatki iznašajo v tretjo državo, kam, komu in pravno podlago iznosa;
- splošen opis zavarovanja osebnih podatkov;
- podatke o povezanih zbirkah osebnih podatkov iz uradnih evidenc ter javnih knjig;
- podatke o zastopniku iz tretjega odstavka 5. člena ZVOP-1, če ta obstaja oziroma navedbo, da ne obstaja.

4. člen

Posamezna zbirka osebnih podatkov je lahko sestavljena iz ene ali več fizičnih zbirk osebnih podatkov.

5. člen

Fizična zbirka lahko obstaja v:

- papirni obliki (knjiga, fascikel, datotečna omara itd.);
- elektronski obliki (magnetni diski, tračne enote, CD-ROMi in drugi nosilci elektronskih zapisov).

6. člen

Upravljalavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov popiše fizične zbirke podatkov, ki vsebujejo osebne podatke in jih razvrsti po evidencah oziroma katalogih.

7. člen

Varovanje osebnih podatkov zajema organizacijske, tehnične in ustrezne logično-tehnične postopke in ukrepe, s katerimi se preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba, izguba ali nepooblaščen obdelava, tako da se:

- varujejo prostori in strojna oprema, v katerih oziroma s pomočjo katere se obdelujejo osebni podatki;
- varuje aplikativna in sistemska programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk;
- omogoča naknadno ugotavljanje kdaj so bili posamezni podatki vneseni, uporabljeni ali preneseni v zbirko podatkov in kdo je to storil, in sicer za obdobje, za katero se posamezni podatki shranjujejo. Evidenca sledljivosti notranjih obdelovanj osebnih podatkov se vodi na obrazcu (Priloga A);
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov.

III. VAROVANJE PROSTOROV IN STROJNE OPREME

8. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov za vsako fizično zbirko osebnih podatkov določi, v katerem prostoru se zbirka nahaja oziroma v katerih prostorih je preko telekomunikacijskih sredstev možen dostop do te zbirke.

9. člen

Upravljavec osebnih podatkov za fizične zbirke, ki jih zanj vodijo pogodbeni obdelovalci osebnih podatkov, ne določi ukrepov varovanja v tem pravilniku, ampak v pogodbi s pogodbenim obdelovalcem, upoštevajoč zakon in ta pravilnik ter dobro poslovno prakso pri varovanju podatkov.

10. člen

Prostori, v katerih se nahajajo zbirke osebnih podatkov in strojna ter programska oprema, ki omogoča dostop do teh podatkov, so varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov (v nadaljnjem besedilu: varovani prostori).

11. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov popiše ukrepe za varovanje prostorov, v katerih se nahajajo fizične zbirke oziroma je možen dostop do njih.

12. člen

(1) Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov določi osebe na posameznem delovnem mestu, ki imajo pravico do vstopa v posamezen prostor v in izven delovnega časa, kjer se nahajajo zbirke osebnih podatkov. Dostop v varovane prostore je dovoljen le tistim osebam, katerih pravica do vstopa v posamezni prostor izhaja iz operacijskega predpisa za varstvo osebnih podatkov.

(2) Vstop v varovane prostore upravljavca osebnih podatkov je dovoljen tudi tistim pogodbenim sodelavcem, ki imajo z upravljavcem osebnih podatkov sklenjene ustrezne pogodbe o sodelovanju, ki vključujejo tudi dolžnost varovanja osebnih podatkov (pogodbeni obdelovalci osebnih podatkov).

(3) Pod pogoji, ki jih določa ta pravilnik je vstop v varovane prostore upravljavca osebnih podatkov dovoljen tudi nezaposlenim osebam, poslovnim partnerjem in drugim obiskovalcem (tretje osebe).

13. člen

Z namenom omejiti dostop v varovane prostore se pri upravljavcu osebnih podatkov izvajajo ukrepi kontrole dostopa kot so uporaba magnetnih kartic, ključev in drugi ukrepi.

14. člen

Delavcem je vstop v varovane prostore dopusten v delovnem času, izven delovnega časa pa le na podlagi izrecnega dovoljenja direktorja. Vsak vstop delavca v prostor in poseg v opremo izven delovnega časa se ustrezno zabeleži (datum, ura, oseba, razlog itd.).

15. člen

(1) Pogodbeni obdelovalci osebnih podatkov v varovane prostore upravljavca osebnih podatkov v delovnem času ne smejo vstopati ali se zadrževati brez prisotnosti odgovornega delavca, razen če jih veže dolžnost varovanja osebnih podatkov, ki je določena v pogodbi z upravljavcem osebnih podatkov.

(2) Oseba, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ga ob vsakem odhodu zakleniti.

(3) Pogodbeni obdelovalci osebnih podatkov se lahko gibljejo v varovanih prostorih upravljavca osebnih podatkov izven delovnega časa in brez prisotnosti odgovornega delavca le, če so nosilci podatkov shranjeni na način, ki ga določa ta pravilnik za čas izven delovnega časa.

16. člen

(1) Oseba, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje (pooblaščen osebna za obdelavo osebnih podatkov), ne sme med delovnim časom brez nadzora puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda s strani nepooblaščenih oseb.

(2) Če ima v varovane prostore pravico vstopiti oseba, ki ni zaposlena pri upravljavcu osebnih podatkov, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da tem osebam ni omogočen vpogled vanje.

17. člen

Tretje osebe v varovane prostore upravljavca osebnih podatkov, kjer se nahajajo osebni podatki, ki niso posebej zaščiteni, ne smejo vstopati ali se zadrževati brez prisotnosti odgovornega delavca.

18. člen

(1) Strojno opremo za zajemanje, obdelavo, izdelavo, kopiranje, prikazovanje, tiskanje, skeniranje, prenašanje in hranjenje podatkov se uporablja v skladu s tehničnimi navodili izdelovalca opreme, določili tega pravilnika ter standardi in navodili za posamezna področja dela.

(2) Strojna oprema se lahko nahaja in uporablja samo v prostorih, ki ustrezajo predpisanim pogojem za delo s to opremo.

(3) S strojno opremo lahko upravljajo samo pooblaščen delavci pri upravljavcu osebnih podatkov. Vsak delavec, ki ima pooblastilo za delo z opremo, je odgovoren za svoje geslo in odgovarja za vsak izveden postopek ali transakcijo.

(4) Omrežna gesla za prijavo v mrežo osebnih računalnikov podeljuje pooblaščenim osebam za obdelavo osebnih podatkov skrbnik mreže ali skrbnik sistema.

IV. VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME, PODATKOVNIH NOSILCEV TER PRENOS PO TELEKOMUNIKACIJSKIH SREDSTVIH

19. člen

Upravljavec osebnih podatkov v tem poglavju predpiše ukrepe in postopke za varovanje systemske in aplikativne programske opreme, postopke in ukrepe za varovanje podatkovnih nosilcev ter prenos po telekomunikacijskih omrežjih.

20. člen

Izven delovnega časa morajo biti računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, izklopljeni in fizično ali programsko zaklenjeni, dostop do osebnih podatkov, hranjenih na disku računalnika, pa mora biti zaščiten z geslom.

21. člen

(1) Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z odobritvijo direktorja ali od njega pooblaščen osebe, izvajajo pa ga lahko samo pooblaščen servisi in njihovi vzdrževalci, ki imajo z upravljavcem sklenjeno pogodbo o servisiranju računalniške oziroma strojne opreme.

(2) Vzdrževanje in popravila se morajo izvajati na lokaciji upravljavca osebnih podatkov in v prisotnosti osebe, pooblaščen za varstvo osebnih podatkov.

(3) Vsak delavec, ki na svojem računalniku (namiznem, prenosnem itd.) hrani osebne podatke, je dolžan v primeru servisiranja računalnika, pred predajo računalnika servisu osebne podatke na njem ustrezno zaščititi (anonimizirati, šifrirati ali trajno izbrisati). V primeru, da tega ne more izpeljati sam, se je dolžan pred predajo računalnika servisu obrniti na osebo, zadolženo za IT, ki izvede zaščito oziroma anonimiziranje podatkov.

VAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE OPREME

22. člen

(1) Dostop do systemske in aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo pooblaščenih oseb za obdelavo osebnih podatkov (posebej na ravni systemske programske opreme in aplikativne programske opreme), ki omogoča dostop samo osebam na določenih delovnih mestih in osebam, ki za upravljavca osebnih podatkov po pogodbi opravljajo servisiranje računalniške in programske opreme.

(2) Program oziroma aplikacija mora biti sestavljen tako, da je obdelava podatkov ponovljiva, ter da ob prekinitvi obdelav ne pride do izgube, uničenja ali sprememb podatkov.

(3) Vsak nov program ali spremembo pri obstoječih programih je treba pred redno uporabo testirati na testnem vzorcu. Razvojni programi in testne podatkovne zbirke morajo biti ločene od produkcijskega okolja.

23. člen

(1) Če je za servisiranje, popravilo, spreminjanje ali dopolnjevanje systemske ali aplikativne programske opreme potrebno kopiranje osebnih podatkov, mora oseba, ki je pooblaščen za obdelavo osebnih podatkov in manipulacijo z osebnimi podatki na računalniku po prenehanju potrebe po kopiji poskrbeti, da se le-ta uniči.

(2) Če pogodba o obdelovanju osebnih podatkov z upravljavcem osebnih podatkov ni sklenjena, se morajo podatki iz diska računalnika izbrisati na način, ki onemogoča restavrancijo.

24. člen

(1) Glede vsebine diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se preverja prisotnost računalniških virusov.

(2) Ob pojavu računalniškega virusa je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi in ugotovi vzrok pojava virusa.

(3) Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu pri upravljavcu osebnih podatkov in prispejo k upravljavcu osebnih podatkov na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

VAROVANJE STREŽNIKOV TER PODATKOVNIH NOSILCEV

25. člen

Nosilci osebnih podatkov, hranjeni izven varovanih prostorov (hodniki, skupni prostori ipd.), morajo biti vedno zaklenjeni v omarah.

26. člen

(1) Zaposlene osebe ne smejo odnašati nosilcev osebnih podatkov izven poslovnih prostorov upravljavca osebnih podatkov brez izrecnega dovoljenja direktorja oziroma od njega pooblaščenih oseb.

(2) Direktor oziroma od njega pooblaščen osebni lahko dovoli iznos nosilcev osebnih podatkov izven poslovnih prostorov upravljavca osebnih podatkov potem, ko je pooblaščen osebni za obdelavo osebnih podatkov predhodno vpisala namen in razlog za takšen iznos nosilcev podatkov v obrazec manipulacij z osebnimi podatki (Priloga A).

(3) Posredovanje osebnih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli direktor oziroma od njega pooblaščen osebni, izvršeno posredovanje pa se vpiše v obrazec manipulacij z osebnimi podatki (Priloga A).

27. člen

Strežniki, na katerih se nahajajo podatki, morajo biti fizično, organizacijsko in tehnično varovani. Neposreden dostop do podatkov v zbirkah podatkov na strežnikih mora biti zavarovan na enak način, kot je zavarovan aplikativni dostop do teh podatkov.

VAROVANJE PRI PRENOSU PO TELEKOMUNIKACIJSKIH OMREŽJIH

28. člen

Osebni podatki morajo biti pri prenosu po telekomunikacijskih sredstvih in omrežjih zaščiteni.

29. člen

Občutljivi osebni podatki morajo biti pri prenosu po telekomunikacijskih sredstvih in omrežjih zaščiteni z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost.

V. UKREPI ZA ZAGOTAVLJANJE INTEGRITETE, ZAUPNOSTI IN DOSTOPNOSTI DO OSEBNIH PODATKOV IN SLEDLJIVOSTI OPERACIJ NA NJIH

INTEGRITETA PODATKOV

30. člen

(1) Upravljavec osebnih podatkov mora zagotoviti integriteto obdelovanih podatkov.

(2) Integriteta (nespremenljivost podatkov) se zagotavlja z uporabo sistemov in aplikacij, ki onemogočajo spreminjanje zajetih podatkov ter z različnimi logično-tehničnimi postopki, kot so uporaba elektronskega podpisa, uporaba elektronskih prstnih odtisov itd..

(3) Organizacijsko se integriteta podatkov zagotavlja s tem, da imajo dostop do posameznega podatka le pooblaščen osebe za obdelavo osebnih podatkov v obsegu dodeljenih uporabniških pravic, veže pa jih dolžnost varovanja integritete podatkov.

(4) Integriteta podatkov se zagotavlja tudi s fizičnim varovanjem prostorov, programske opreme in podatkovnih nosilcev.

ZAUPNOST PODATKOV

31. člen

(1) Upravljavec osebnih podatkov mora zagotoviti zaupnost obdelovanih podatkov.

(2) Zaupnost podatkov se logično-tehnično zagotavlja z uporabniškimi imeni in gesli na ravni systemske in aplikativne programske opreme, s katero se obdelujejo podatki. Podatki so lahko kodirani ali šifrirani ali pa mora sistem za upravljanje s podatki zagotavljati, da do njih ne dostopajo nepooblaščen osebe. Zaupnost podatkov se lahko zagotavlja tudi s kriptografijo (šifriranjem) podatkov, kjer sam zapis podatkov onemogoča njihovo branje s strani nepooblaščenih oseb.

(3) Organizacijsko se zaupnost podatkov lahko zagotavlja v aktu o sistemizaciji delovnih mest, kjer se za vsako delovno mesto opredelijo pravice in pooblastila na posamezni podatkovni zbirki. Če to v sistemizaciji delovnih mest ni podrobneje opredeljeno, omenjene pravice in pooblastila izhajajo iz operacijskega predpisa o varstvu osebnih podatkov. Za vsako delovno mesto se v notranjih aktih upravljavca lahko opredeli tudi dolžnost varovanja zaupnosti osebnih podatkov.

(4) Zaupnost podatkov se zagotavlja tudi s fizičnim varovanjem prostorov, systemske in aplikativne programske opreme ter podatkovnih nosilcev.

32. člen

Dostop do podatkov prek aplikativne programske opreme je varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel vsakemu subjektu priredi skupino pravic in pooblastil na posamezni sistemski in aplikativni programski opremi.

33. člen

(1) Vsa gesla, ki se uporabljajo za vstop in za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov, se hranijo v zapečatenih ovojnica in varujejo v ognjevarni omari.

(2) Varovana gesla, hranjena v zapečatenih ovojnica, se smejo uporabiti samo v izjemnih in nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira.

(3) Po uporabi zapečatenih gesel iz ovojnic direktor oziroma od njega pooblaščen oseba določi nova gesla.

DOSTOPNOST

34. člen

(1) Upravljevec osebnih podatkov mora zagotoviti dostopnost obdelovanih podatkov.

(2) Dostopnost podatkov se zagotavlja z ukrepi, ki omogočajo neprekinjen in trajen (do izbrisa) dostop do podatkov: izdelava varnostnih kopij podatkov (back-up), arhiviranje podatkov, vzporedne evidence, izdelava izvedenih evidenc itd.. Varnostna kopija podatkov lahko obstaja v isti obliki kot izvorni podatki (npr. kopirani papirni arhiv), lahko je njihova varnostna kopija v drugem formatu (npr. skenirani dokumenti, shranjeni v sistemu za elektronsko upravljanje z dokumenti), lahko pa gre za povzetek podatkov v drugem formatu (npr. vpis podatkov iz papirnih vlog v elektronsko zbirko podatkov).

(3) Vsi postopki izdelovanja varnostnih kopij morajo biti ustrezno dokumentirani in morajo zagotavljati natančen zajem, transformacijo in shranjevanje podatkov.

35. člen

(1) Upravljevec osebnih podatkov mora za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlogov redno izdelovati kopije vsebine osebnih podatkov.

(2) Vse izdelane papirne kopije vsebin zbirk osebnih podatkov se morajo vpisati v obrazec manipulacij z osebnimi podatki (Priloga A) in se hranijo v zaklenjeni omari.

(3) Informacije o izdelavi elektronskih kopij vsebin zbirk osebnih podatkov se vodijo v dnevniških datotekah (log files) aplikacij za kopiranje.

SLEDLJIVOST OPERACIJ NA PODATKIH IN SLEDLJIVOST POSREDOVANJ PODATKOV

36. člen

Sledljivost operacij (vnos, uporaba, sprememba, posredovanje, brisanje) na osebnih podatkih se dosega z vodenjem evidenc o operacijah na podatkih oziroma zbirkah podatkov. Take evidence so lahko elektronske ali papirne, njihovo vodenje pa je lahko ročno ali avtomatsko. Vodenje je ročno, če se vsaka obdelava podatkov ročno zavede. Vodenje je avtomatsko, če se vsaka obdelava avtomatsko zavede. Primer avtomatskega vodenja je vodenje dnevnikov v posameznih aplikacijah (log files), iz katerih se da razbrati dejanja posameznih oseb v zvezi s posameznimi osebnimi podatki.

37. člen

Sledljivost posredovanj osebnih podatkov uporabnikom se dosega z vodenjem evidenc o posredovanju osebnih podatkov. Take evidence so lahko pisne (npr. obrazec posredovanj) ali elektronske (npr. preglednica ali zbirka podatkov o posredovanjih), njihovo vodenje pa je lahko ročno (ročni vpis v posamezno evidenco) ali pa avtomatsko (kjer je posredovanje izvršeno preko aplikacije, ki vodi dnevnik operacij). Omenjene evidence se vodijo na obrazcu manipulacij z osebnimi podatki (Priloga A).

38. člen

Upravljevec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov podrobneje določi načine zagotavljanja integritete, zaupnosti in dostopnosti podatkov ter sledljivosti operacij na njih.

VI. ORGANIZACIJA DELOVNIH PROCESOV

39. člen

Upravljevec zbirk osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov določi tipične pravice v zvezi z obdelavo osebnih podatkov (dostop, pregledovanje, spreminjanje, brisanje, posredovanje). Za vsako evidenco določi katere pravice na tej evidenci obstajajo in katera delovna mesta iz sistemizacije delovnih mest imajo te pravice pri posamezni evidenci.

40. člen

Upravljevec osebnih podatkov določi odgovorno osebo za vsako zbirko osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov.

41. člen

Vsi ostali delavci (pooblaščen osebe za obdelavo osebnih podatkov) morajo za obdelavo osebnih podatkov pridobiti ustrezno pooblastilo direktorja oziroma odgovorne osebe za posamezno zbirko osebnih podatkov iz prejšnjega člena tega pravilnika (Priloga B).

VII. MANIPULACIJA Z OSEBNIMI PODATKI IN ZBIRKAMI OSEBNIH PODATKOV

SPLOŠNE DOLOČBE

42. člen

Upravljavec osebnih podatkov za vsako operacijo na osebnih podatkih zagotovi možnost poznejšega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

43. člen

Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov podrobneje razčleni operacije v zvezi s posameznimi zbirkami osebnih podatkov.

ZBIRANJE OSEBNIH PODATKOV

44. člen

(1) Pravna podlaga za zbiranje osebnih podatkov je zakon, ki dovoljuje obdelovanje določene vrste osebnih podatkov ali osebna privolitev posameznika, če zakon za obdelovanje osebnih podatkov določi, da se nekateri podatki lahko obdelujejo le na podlagi posameznikovega privoljenja (drugi odstavek 9. člena ZVOP-1). Osebna privolitev posameznika je praviloma pisna, še posebej ko se obdelujejo občutljivi osebni podatki. Pisna privolitev posameznika je praviloma v obliki podpisane izjave posameznika (Priloga C ali D).

(2) Izjemoma se lahko obdelujejo tudi osebni podatki, za katere ni eksplicitnega zakonskega pooblastila ali privolitve posameznika, če gre za osebne podatke posameznikov, ki so z upravljavcem osebnih podatkov sklenili pogodbo ali pa so z njim v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna za izvedbo pogajanj ali izpolnitev pogodbe (tretji odstavek 9. člena ZVOP-1). Ne glede na prejšnji odstavek pa se lahko osebni podatki obdelujejo tudi, če je to nujno zaradi izvrševanja zakonitih pristojnosti, nalog ali obveznosti javnega sektorja oziroma zakonitih interesov upravljavca osebnih podatkov in ti interesi očitno prevladajo nad interesi posameznika, na katerega se nanašajo (četrti odstavek 9. člena ZVOP-1).

45. člen

(1) Upravljavec osebnih podatkov mora zagotoviti, da je posameznik, katerega osebni podatki se vnašajo v zbirko osebnih podatkov obveščen o obdelavi njegovih osebnih podatkov in da je podana osebna privolitev posameznika v skladu z veljavno zakonodajo s področja varstva osebnih podatkov.

(2) Če se osebni podatki zbirajo neposredno od posameznika, upravljavec osebnih podatkov posamezniku sporoči naslednje informacije, če z njimi posameznik še ni seznanjen:

- podatke o upravljavcu osebnih podatkov (firma in sedež) ter
- namen obdelave osebnih podatkov.

(3) Če osebni podatki niso bili zbrani neposredno od posameznika, na katerega se nanašajo, pa upravljavec osebnih podatkov sporoči informacije, navedene v drugem odstavku tega člena, posamezniku najpozneje ob vpisu ali posredovanju osebnih podatkov.

(4) Če je glede na posebne okoliščine zbiranja teh osebnih podatkov potrebno, da se zagotovi zakonita in poštena obdelava osebnih podatkov posameznika, upravljavec osebnih podatkov sporoči tudi dodatne informacije, če posameznik z njimi še ni seznanjen, zlasti:

- navedbo uporabnika ali vrste uporabnikov njegovih osebnih podatkov;
- navedbo, ali je zbiranje osebnih podatkov obvezno ali prostovoljno, ter možne posledice, če ne bo prostovoljno podal podatkov;
- informacijo o pravici do vpogleda, prepisa, kopiranja, dopolnitve, popravka, blokiranja in izbrisa osebnih podatkov, ki se nanašajo nanj.

(5) Teh informacij ni potrebno zagotoviti le, če bi bilo to zaradi obdelave osebnih podatkov za zgodovinsko, statistično ali znanstveno-raziskovalne namene nemogoče ali bi povzročilo velike stroške, nesorazmerno velik napor ali zahtevalo veliko časa ali če je z zakonom izrecno določen vpis ali posredovanje osebnih podatkov.

VZPOSTAVITEV IN DOPOLNITEV ZBIRKE OSEBNIH PODATKOV

46. člen

Osebni podatki se vpisujejo v zbirke osebnih podatkov samo na podlagi ustrezne pravne podlage iz 44. člena tega pravilnika.

47. člen

(1) Katalog zbirke osebnih podatkov vsebuje naslednje podatke:

- naziv zbirke osebnih podatkov;
- podatke o upravljavcu osebnih podatkov (firmo, sedež in matično številko družbe);
- pravno podlago za obdelavo osebnih podatkov;
- kategorije posameznikov, na katere se nanašajo osebni podatki;
- vrste osebnih podatkov v zbirki osebnih podatkov;
- namen obdelave;
- rok hrambe osebnih podatkov;
- omejitve pravic posameznikov glede osebnih podatkov v zbirki osebnih podatkov in pravno podlago omejitev;
- uporabnike ali kategorije uporabnikov osebnih podatkov, vsebovanih v zbirki osebnih podatkov;
- dejstvo, ali se osebni podatki iznašajo v tretjo državo, kam, komu in pravno podlago iznosa;
- splošen opis zavarovanja osebnih podatkov;
- podatke o povezanih zbirkah osebnih podatkov iz uradnih evidenc ter javnih knjig;
- podatke o zastopniku iz tretjega odstavka 5. člena ZVOP-1.

(2) Upravljavec osebnih podatkov mora podatke iz 1., 2., 4., 5., 6., 9., 10., 11., 12. in 13. alineje prejšnjega odstavka posredovati pristojnemu organu za varstvo osebnih podatkov v roku najmanj 15 (petnajstih) dni pred vzpostavitvijo zbirke osebnih podatkov ali pred vnosom nove vrste osebnih podatkov.

(3) Upravljavec osebnih podatkov mora skrbeti za točnost in ažurnost vsebine posameznega kataloga zbirke osebnih podatkov.

(4) Podatki, navedeni v tem členu, se posredujejo pristojnemu organu za varstvo osebnih podatkov na obrazcu (Priloga E).

SPREMEMBE ZBIRKE OSEBNIH PODATKOV

48. člen

Upravljavec osebnih podatkov posreduje spremembe podatkov pristojnemu organu za varstvo osebnih podatkov najkasneje v 8 (osmih) dneh od dneva spremembe.

POSREDOVANJE

49. člen

Osebni podatki, vodeni v zbirki osebnih podatkov pri upravljavcu osebnih podatkov, se lahko posredujejo drugim uporabnikom samo, če so za njihovo pridobitev in uporabo pooblaščen z zakonom ali na podlagi pisne zahteve ali privolitve osebe, na katero se osebni podatki nanašajo.

50. člen

Upravljavec osebnih podatkov za vsako posredovanje osebnih podatkov zagotovi, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.

BRISANJE

51. člen

Upravljavec osebnih podatkov shranjuje osebne podatke le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Rok hrambe osebnih podatkov je opredeljen v posameznem katalogu zbirke osebnih podatkov. Po izpolnitvi tega namena obdelave se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, 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.

52. člen

(1) Brisanje osebnih podatkov na računalniških medijih se opravi na način, ki onemogoča restavriranje brisanih podatkov, kar lahko vključuje tudi uničenje računalniških medijev na način opredeljen v drugem odstavku tega člena.

(2) Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam), se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (zažgejo, razrežejo) v prostorih upravljavca osebnih podatkov, lahko pa tudi pri drugi organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije, v obeh primerih pa mora postopek potekati pod nadzorom pooblaščenega delavca upravljavca osebnih podatkov.

53. člen

(1) Z vestnostjo in skrbnostjo, določeno s tem pravilnikom, za uničevanje osebnih podatkov, vodenih v zbirkah oziroma na posameznih nosilcih podatkov, se mora brisati in uničevati tudi

pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

(2) Uničevanje osebnih podatkov na nosilcih iz prejšnjega odstavka se mora izvajati tekoče in ažurno.

VIII. POGODBENI OBDELOVALCI OSEBNIH PODATKOV

54. člen

(1) Upravljavec osebnih podatkov lahko poveri posamezna opravila v zvezi z obdelavo osebnih podatkov pogodbenemu obdelovalcu osebnih podatkov, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe za varovanje osebnih podatkov.

(2) Upravljavec osebnih podatkov v operacijskem predpisu za varstvo osebnih podatkov določi seznam pogodbenih obdelovalcev osebnih podatkov za posamezno zbirko osebnih podatkov.

55. člen

Za vsakega pogodbenega obdelovalca osebnih podatkov določi upravljavec osebnih podatkov v pogodbi o obdelovanju osebnih podatkov do katerih zbirk oziroma do katerih vrst osebnih podatkov v posamezni zbirki osebnih podatkov ima pogodbeni obdelovalec osebnih podatkov dostop, kakšna pooblastila ima pogodbeni obdelovalec osebnih podatkov na teh zbirkah oziroma vrstah podatkov (dostop, pregledovanje, spreminjanje, brisanje, posredovanje) ter kakšne ukrepe in postopke mora pogodbeni obdelovalec osebnih podatkov sprejeti oziroma izvajati za varstvo teh podatkov.

56. člen

Upravljavec osebnih podatkov v pogodbi o obdelovanju osebnih podatkov evidentira, do katerih zbirk oziroma do katerih vrst osebnih podatkov znotraj posamezne zbirke osebnih podatkov imajo pogodbeni obdelovalci osebnih podatkov dostop in kakšna so njihova pooblastila za obdelavo teh podatkov.

57. člen

Pogodbeni obdelovalec osebnih podatkov sme opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru pooblastil upravljavca osebnih podatkov in osebnih podatkov ne sme obdelovati za drug namen.

58. člen

V primeru spora med upravljavcem osebnih podatkov in pogodbenim obdelovalcem osebnih podatkov je dolžan pogodbeni obdelovalec osebnih podatkov na podlagi zahteve upravljavca osebnih podatkov osebne podatke, ki jih je pogodbeno obdeloval, nemudoma vrniti upravljavcu osebnih podatkov. Morebitne kopije teh podatkov mora takoj uničiti ali jih posredovati državnemu organu, ki je v skladu z zakonom pristojen za odkrivanje ali pregon kaznivih dejanj, sodišču ali drugemu državnemu organu, če tako določa zakon.

59. člen

V primeru prenehanja pogodbenega obdelovalca osebnih podatkov se osebni podatki brez nepotrebnega odlašanja vrnejo upravljavcu osebnih podatkov.

IX. IZNOS OSEBNIH PODATKOV V TRETJE DRŽAVE

60. člen

(1) Posredovanje osebnih podatkov, ki se obdelujejo ali se bodo obdelovali šele po opravljenem posredovanju v tretjo državo, je dopustno v skladu z ZVOP-1 in pod pogojem, da pristojni organ za varstvo osebnih podatkov izda odločbo, da država, v katero se iznašajo, zagotavlja ustrezno raven varstva osebnih podatkov.

(2) Odločba iz prejšnjega odstavka ni potrebna, če je tretja država na seznamu tistih držav, za katere je pristojni organ za varstvo osebnih podatkov ugotovil, da v celoti zagotavlja ustrezno raven varstva osebnih podatkov.

(3) Odločba iz prvega odstavka tega člena ni potrebna, če je tretja država na seznamu tistih držav, za katere je pristojni organ za varstvo osebnih podatkov ugotovil, da delno zagotavlja ustrezno raven varstva osebnih podatkov, če se posredujejo tisti osebni podatki in za tiste namene, za katere je ugotovljena ustrezna raven varstva.

61. člen

Ne glede na določbe prvega odstavka prejšnjega člena se lahko iznesejo osebni podatki in posredujejo v tretjo državo, če:

- tako določa zakon ali obvezujoča mednarodna pogodba;
- je podana osebna privolitev posameznika, na katerega se nanašajo osebni podatki in je ta seznanjen s posledicami takšnega posredovanja, predvsem s tem, da v tretji državi lahko ne bo deležen iste ravni pravnega varstva osebnih podatkov kot v Republiki Sloveniji;
- je iznos potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov ali za izvršitev predpogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki;
- je iznos potreben za sklenitev ali izvršitev pogodbe, ki je v korist posameznika, na katerega se nanašajo osebni podatki, sklenjene med upravljavcem osebnih podatkov in tretjo stranko;
- je iznos potreben, da se pred hujšim ogrožanjem zavaruje življenje ali telo posameznika, na katerega se nanašajo osebni podatki;
- se iznos opravi iz registrov, javnih knjig ali uradnih evidenc, ki so po zakonu namenjene zagotavljanju informacij javnosti in so na voljo za vpogled javnosti na splošno ali katerikoli osebi, ki lahko izkaže pravni interes, da so v posameznem primeru izpolnjeni pogoji, ki jih za vpogled določa zakon;
- upravljavec osebnih podatkov zagotovi ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov in navede možnosti njihovega uresničevanja ali varstva, predvsem v določbah pogodb ali v splošnih pogojih poslovanja. V primeru iznosa osebnih podatkov v skladu s to alinejo je potrebno pridobiti posebno odločbo pristojnega organa za varstvo osebnih podatkov, ki dovoljuje iznos osebnih podatkov. Osebnosti se sme iznesti šele po prejemu navedene odločbe, s katero je iznos dovoljen.

62. člen

Seznam izdanih odločb iz 60. člena tega pravilnika vodi pristojni organ za varstvo osebnih podatkov, glavni državni nadzornik pa ga objavi v Uradnem listu Republike Slovenije.

63. člen

Iznos osebnih podatkov v tretjo državo je potrebno evidentirati skladno z določbami desete alineje prvega odstavka 47. člena tega pravilnika.

X. VIDEONADZOR

64. člen

(1) Upravljavec osebnih podatkov mora o izvajanju videonadzora objaviti obvestilo. Obvestilo mora biti vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznaní z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor.

(2) Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije:

- da se izvaja videonadzor;
- naziv upravljavca osebnih podatkov ter
- telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema.

(3) Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan pred dostopom nepooblaščenih oseb.

65. člen

(1) Videonadzor dostopa v uradne službene oziroma poslovne prostore se lahko izvaja, če je to potrebno za varnost ljudi in premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja delavcev.

(2) Odločitev o uvedbi videonadzora dostopa v uradne službene oziroma poslovne prostore sprejme direktor. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora.

(3) O izvajanju videonadzora je potrebno pisno obvestiti vse delavce, ki opravljajo delo v nadzorovanem prostoru.

(4) Zbirka osebnih podatkov po tem členu vsebuje posnetek posameznika (slika oziroma glas), datum in čas vstopa in izstopa iz prostora, lahko pa tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo poleg ali s posnetkom videonadzornega sistema.

66. člen

(1) Videonadzor znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi in premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

(2) Videonadzor se lahko izvaja le glede tistih delovnih prostorov, kjer je potrebno varovati interese iz prejšnjega odstavka.

(3) Prepovedano je izvajati videonadzor v delovnih prostorih izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih.

(4) Delavci morajo biti pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obveščeni o njegovem izvajanju.

(5) Pred uvedbo videonadzora se mora upravljavec osebnih podatkov posvetovati z reprezentativnim sindikatom pri upravljavcu osebnih podatkov.

XI. EVIDENCA VSTOPOV IN IZSTOPOV IZ PROSTOROV

67. člen

(1) Upravljavec osebnih podatkov lahko za namene varovanja premoženja, življenja ali telesa posameznika ter reda v njegovih prostorih od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva, da navede vse ali nekatere osebne podatke iz drugega odstavka tega člena ter razlog vstopa ali izstopa. Po potrebi lahko osebne podatke preveri tudi z vpogledom v osebni dokument.

(2) V evidenci vstopov in izstopov se lahko o posamezniku vodijo samo naslednji osebni podatki: osebno ime, številka in vrsta osebnega dokumenta, naslov stalnega ali začasnega prebivališča, zaposlitev ter datum, ura in razlog vstopa ali izstopa v ali iz poslovnih prostorov.

XII. PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

68. člen

Upravljavec osebnih podatkov mora posamezniku na njegovo zahtevo:

- omogočiti vpogled v katalog zbirke osebnih podatkov;
- potrditi, ali se podatki v zvezi z njim obdelujejo ali ne in mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje;
- dopolniti, popraviti, blokirati ali izbrisati osebne podatke, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom.

69. člen

Upravljavec osebnih podatkov mora posamezniku omogočiti vpogled, prepis, kopiranje oziroma izdati potrdilo o tem, ali se podatki v zvezi z njim obdelujejo ali ne najkasneje v 15 (petnajstih) dneh od dneva, ko je prejel zahtevo, ali ga v istem roku pisno obvestiti o razlogih, zaradi katerih vpogleda, prepisa, kopiranja ali izdaje potrdila ne bo omogočil. V istem roku mora upravljavec osebnih podatkov opraviti dopolnitev, popravo, blokiranje ali izbris osebnih podatkov oziroma ga obvestiti o razlogih, zaradi katerih tega ne bo storil.

70. člen

Upravljavec osebnih podatkov mora posamezniku na njegovo zahtevo tudi:

- posredovati izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj;
- posredovati seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšen namen;
- dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave;
- dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem;
- pojasniti tehnične oziroma logično-tehnične postopke odločanja, če izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika.

71. člen

Upravljevec osebnih podatkov posreduje posamezniku izpis, seznam, informacije ter pojasnilo v 30 (tridesetih) dneh od dneva, ko je prejel zahtevo, ali ga v istem roku pisno obvestiti o razlogih, zaradi katerih mu izpisa, seznama, informacij ali pojasnila ne bo posredoval.

72. člen

Posredovanje osebnih podatkov iz zbirk osebnih podatkov, ki jih vodi upravljevec, drugim upravičencem se vpiše v obrazec manipulacij z osebnimi podatki (Priloga A). Na zahtevo osebe, o kateri so bili posredovani osebni podatki, mora delavec, ki je osebne podatke posredoval, izročiti osebi seznam upravičencev, katerim so bili v določenem obdobju posredovani podatki, ki so vsebovani v zbirki podatkov upravljavca osebnih podatkov in se nanašajo nanjo.

73. člen

Posameznik lahko kadarkoli pisno ali na drug dogovorjen način zahteva, da upravljevec osebnih podatkov trajno ali začasno preneha uporabljati njegove osebne podatke za namen neposrednega trženja. Upravljevec osebnih podatkov je dolžan v 15 (petnajstih) dneh ustrezno preprečiti uporabo osebnih podatkov za namen neposrednega trženja ter o tem v nadaljnjih 5 (petih) dneh pisno ali na drug dogovorjen način obvestiti posameznika, ki je to zahteval.

74. člen

Interne postopke v zvezi s pravicami posameznika vodi direktor.

XIII. UKREPANJE OB UGOTOVITVI ZLORABE OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

75. člen

(1) Delavci upravljavca osebnih podatkov, ki pridejo v stik z osebnimi podatki, 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 določata ta pravilnik in operacijski predpis.

(2) Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (razkritje osebnih podatkov, nepooblaščen uničenje, nepooblaščen spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora o tem takoj

obvestiti direktorja in pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je nepooblaščen posegel.

76. člen

(1) Upravljavec lahko zoper tistega, za katerega obstaja sum, da je zlorabil osebne podatke ali je nepooblaščen posegel v zbirko osebnih podatkov, ukrepa v skladu z zakonodajo.

(2) Če pri nepooblaščenem posegu v zbirko osebnih podatkov obstaja sum, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani ali če je do zlorabe osebnih podatkov že prišlo, lahko upravljavec osebnih podatkov poleg uvedbe disciplinskega postopka oziroma postopka odpovedi pogodbe zoper storilca, če je ta delavec upravljavca, nepooblaščen poseg ali drugo zlorabo prijavi organom pregona.

(3) Za zlorabo osebnih podatkov se šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v zakonu, na podlagi katerega se zbirajo ali nameni, določenimi v katalogu zbirke osebnih podatkov.

XIV. ODGOVORNOST DELAVCEV ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

77. člen

(1) Pred nastopom dela delavca na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora delavec podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in v kateri je opozorjen na posledice kršitve te dolžnosti (Priloga F).

(2) Dolžnost varovanja osebnih podatkov, s katerimi se je delavec seznanil pri svojem delu, velja tudi po prenehanju delovnega razmerja pri upravljavcu osebnih podatkov.

78. člen

Pooblaščen delavec stori disciplinsko kršitev:

- če razkriva osebne podatke, s katerimi se je seznanil pri svojem delu, sodelavcem, ki niso pooblaščen za delo z osebnimi podatki ali tretjim osebam;
- če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov oziroma če opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam oziroma če brez dovoljenja odnaša nosilce osebnih podatkov izven prostorov upravljavca osebnih podatkov;
- če opusti izvajanje postopkov in ukrepov za zagotavljanje integritete, zaupnosti in razpoložljivosti osebnih podatkov, ki jih določa ta pravilnik ter če opusti izvajanje postopkov in ukrepov za evidentiranje vseh obdelovanj osebnih podatkov;
- če ne obvesti pooblaščenega delavca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov;
- če opusti vestno in skrbno nadzorovanje varovanih prostorov ali
- če kako drugače krši določbe tega pravilnika.

79. člen

O zlorabi ali sumu zlorabe osebnih podatkov, vodenih v zbirkah osebnih podatkov podjetja s strani oseb, ki niso delavci podjetja se obvesti organe, pooblaščne za pregon.

XV. PREHODNE IN KONČNE DOLOČBE

80. člen

Spremembe in dopolnitve tega pravilnika sprejme direktor po postopku in na način kot velja za sprejem tega pravilnika.

81. člen

Direktor v roku 1 (enega) meseca po sprejetju tega pravilnika sprejme operacijski predpis o varstvu osebnih podatkov, v katerem konkretizira postopke in ukrepe za varstvo zbirk osebnih podatkov iz tega pravilnika.

82. člen

(1) Z določbami tega pravilnika morajo biti seznanjeni vsi delavci pri upravljavcu osebnih podatkov, ki pridejo v stik z osebnimi podatki.

(2) Izvod pravilnika je dostopen na elektronski oglasni deski vsem delavcem, v katerih delovne obveznosti sodi zbiranje, urejanje, obdelava, spreminjanje, shranjevanje, posredovanje ali uporaba osebnih podatkov ali nosilcev osebnih podatkov.

83. člen

Vsi zaposleni pri upravljavcu morajo podpisati izjavo iz 77. člena tega pravilnika v roku 30 (trideset) dni od dneva sprejema tega pravilnika.

84. člen

Z uveljavitvijo tega pravilnika preneha veljati Pravilnik o zavarovanju osebnih podatkov, št. 071-1/2006 z dne 7. 4. 2006.

85. člen

Ta pravilnik začne veljati naslednji dan po objavi na e-oglasni deski na intranetu Eko sklada, Slovenskega okoljskega javnega sklada.

Številka: 0141-5/2017-4

Datum: 9. 11. 2017