V skladu s 24. in 40. členom Statuta javnega zavoda Inštitut za varovanje zdravja Republike Slovenije na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (ZVOP-1, Uradni list RS, 86/04 in nasl.) direktorica Inštituta za varovanje zdravja Republike Slovenije Marija Seljak izdaja

PRAVILNIK

o varstvu osebnih podatkov na IVZ

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov na Inštitutu za varovanje zdravja Republike Slovenije (v nadaljnjem besedilu IVZ) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava osebnih podatkov.

Zaposleni na IVZ in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. ZVOP-1 – Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/04 in nasl.);
2. Osebni podatek – je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
3. Posameznik – je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njegovo fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov ali ne zahteva veliko časa;
4. 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;
5. 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);
6. Upravljavec osebnih podatkov – je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave;

7. Občutljivi osebni podatki – so podatki o rasnem narodnem ali narodnostnem poreklu, političnem, verskem filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti;
8. Uporabnik osebnih podatkov – je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
9. Nosilec podatkov – so vse vrste sredstev, na katerih so zapisani ali posneti osebni podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);
10. Anonimiziranje – je takšna sprememba oblike osebnih podatkov, da jih ni več mogoče povezati s posameznikom ali je to mogoče le s nesorazmerno velikimi napori, stroški ali porabo časa;
11. Odgovorna oseba za zbirko osebnih podatkov (odgovorna oseba) – s strani direktorja imenovana oseba, ki skrbi in odgovarja, da delovanje posamezne zbirke osebnih podatkov (obdelava osebnih podatkov) in zavarovanje osebnih podatkov v zbirki poteka v skladu s postopki in ukrepi za zavarovanje osebnih podatkov, določenimi s tem pravilnikom, ZVOP-1 in drugimi veljavnimi predpisi v Republiki Sloveniji;
12. Osebe, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke (pooblaščeni obdelovalci) – osebe, ki pri svojem delu v IVZ obdelujejo osebne podatke v posamezni zbirki osebnih podatkov in jih poimensko pisno določi odgovorna oseba za zbirko osebnih podatkov;
13. Oseba, odgovorna za delovnaje informacijskega sistema – če ni drugače določeno, gre za osebo, ki vodi notranjo organizacijsko enoto oziroma oddelek za informacijsko-komunikacijsko tehnologijo.
14. Križanje zbirk osebnih podatkov – enkratna, začasna združitev dveh zbirk osebnih podatkov, ki jo za statistični ali drug dovoljen namen izvede s strani direktorja za konkretni primer pisno imenovana oseba, ki zbirki združi z uporabo istega povezovalnega znaka, ki ga vsebujeta obe zbirki osebnih podatkov (na primer: EMŠO), nato pa tako pridobljeno zbirko nemudoma anonimizira, začasno združeno zbirko osebnih podatkov pa uniči. Rezultati križanja zbirk osebnih podatkov so lahko objavljeni le v agregirani obliki. Postopek križanja se izvede v varni sobi IVZ;
15. Zaupen podatek – podatek, ki je tako pomemben, da bi z njegovo izdajo nastale ali lahko nastale hujše škodljive posledice za IVZ ali za posameznika.

II. OBDELAVA OSEBNIH PODATKOV

3. člen

Osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon.

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.

Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

Odgovorne osebe ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke (v nadaljevanju pooblaščeni obdelovalci), morajo biti pred obdelavo osebnih podatkov seznanjene z določbami ZVOP-1 ter z vsebino tega pravilnika.

Vse zbirke osebnih podatkov, s katerimi upravlja IVZ, se morajo bodisi v elektronski bodisi v papirni obliki voditi tako, da omogočajo poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

4. člen

Zaposleni, ki je zadolžen za sprejem in evidenco pošte:
- mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, ali organizacijski enoti, na katero je ta pošiljka naslovljena;
- odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v IVZ (prinesejo jih stranke ali kurirji), razen pošiljk iz naslednjih dveh alinei;
- ne sme odpirati tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis;
- 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 zaposlenega brez označbe njegovega položaja oziroma delovnega mesta in šele nato naslov IVZ.

Glede ostalih opravil v zvezi z evidentiranjem zadev, dosjejev in dokumentov, ki vsebujejo osebne podatke, se uporabljajo določila notranjih aktov in predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.

5. člen

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.

Posredovanje osebnih podatkov iz prejšnjega odstavka lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne vloge mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščeni obdelovalec v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.

Posredovanje občutljivih osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna vloga mora biti po vsebini enaka pisni vlogi iz prejšnjega odstavka.

O upravičenosti do posredovanja odloči odgovorna oseba za zbirko osebnih podatkov, v kateri se zahtevani osebni podatki nahajajo.

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 opraviti brez vidne sledi odpiranja ovojnice.

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.

Občutljive osebne podatke je dovoljeno posredovati preko komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

Originalni dokument, ki vsebuje osebne podatke, se lahko posreduje uporabniku samo na podlagi pisne odredbe sodišča. Posredovani originalni dokument mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

6. člen

Vsako posredovanje osebnih podatkov iz prejšnjega člena se zaznamuje v evidenco posredovanj vsaj z navedbo naslednjih podatkov:
- kateri osebni podatki so bili posredovani,
- osebno ime/firmo in naslov/sedež osebe, ki so ji bili posredovani osebni podatki,
- datum in ura posredovanja osebnih podatkov ter
- pravna podlaga, na kateri so bili posredovani osebni podatki.

Evidenca posredovanja in oblika zaznamka sta odvisna od nosilca podatkov, ki vsebuje posredovani osebni podatek (spis, informacijski sistem ipd.). Evidenco posredovanj za posamezno zbirko osebnih podatkov vzpostavi in vodi pooblaščeni obdelovalec, ki ga pisno določi odgovorna oseba za zbirko osebnih podatkov.

Zaznamek iz prvega odstavka tega člena naredi odgovorna oseba ali pooblaščeni obdelovalec, ki je osebne podatke posredoval uporabniku.

7. člen

Zaposleni na IVZ, ki pri izvajanju svojih delovnih nalog kopirajo, 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.

Kopiranje in tiskanje dokumentov, ki vsebujejo občutljive osebne podatke, se lahko opravi samo na napravah, do katerih ima dostop le zaposleni, ki je naredil ali prejel takšen dokument.

8. člen

Osebni podatki se lahko shranjujejo le toliko časa, kolikor je zakonski rok hrambe, ki je razviden tudi iz kataloga zbirke osebnih podatkov.

Po preteku roka hranjenja 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.

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

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

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

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

Pri prenosu nosilcev podatkov, ki vsebujejo občutljive osebne podatke, na mesto uničenja, je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov.

Prenos nosilcev podatkov, ki vsebujejo občutljive osebne podatke, na mesto uničenja ter uničevanje takih nosilcev podatkov nadzoruje posebna tričlanska komisija, ki jo vsakokrat imenuje direktor. O uničenju komisija sestavi ustrezen zapisnik.

Komisijo iz prejšnjega odstavka sestavljajo zaposleni na IVZ, en član komisije mora biti odgovorna oseba za zbirko osebnih podatkov.

9. člen

Opisi zbirk osebnih podatkov, katerih upravljavec je IVZ, se vodijo v katalogu zbirk osebnih podatkov (opisu zbirk osebnih podatkov), ki se vodi v skladu z določbami 26. člena ZVOP-1. Podatki iz 1., 2., 4., 5., 6., 9., 10., 12. in 13. točke kataloga zbirk osebnih podatkov se morajo posredovati državnemu organu, pristojnemu za vodenje Registra zbirk osebnih podatkov. Katalog zbirke osebnih podatkov se za vsako zbirko osebnih podatkov zagotovi najkasneje 15 dni pred vzpostavitvijo zbirke osebnih podatkov, v istem roku pa se podatki iz kataloga posredujejo tudi pristojnemu državnemu organu. Katalog zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki, spremembe pa se v roku 8 dni posredujejo tudi pristojnemu državnemu organu. Katalogi zbirk osebnih podatkov, katerih upravljavec je IVZ so navedeni v Prilogi 1 tega pravilnika.

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk osebnih podatkov pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

IVZ za vsako zbirko osebnih podatkov vodi 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, delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov, ter delovna mesta oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov.

Seznam iz prejšnjega odstavka je sestavni del tega pravilnika in predstavlja Prilogo 2. V seznamu so določene odgovorne osebe za vsako od zbirk osebnih podatkov in delovna mesta oseb, ki lahko zaradi narave dela obdelujejo osebne podatke iz določene zbirke, kot določa prejšnji odstavek.

Konkretne osebe, ki lahko zaradi narave dela obdelujejo osebne podatke iz določene zbirke, poimensko pisno določi odgovorna oseba za posamezno zbirko osebnih podatkov, ki je dolžna voditi ažuren poimenski seznam oseb, ki lahko zaradi narave dela obdelujejo osebne podatke iz določene zbirke.

Odgovorna oseba za posamezno zbirko osebnih podatkov skrbi in odgovarja, da so z vsakokratnim katalogom zbirk osebnih podatkov IVZ usklajeni tudi podatki v Registru zbirk osebnih podatkov, ki ga vodi državni organ, pristojen za vodenje Registra zbirk osebnih podatkov.

10. člen

Ne glede na prvotni namen zbiranja se lahko v skladu z ZVOP-1 osebni podatki nadalje obdelujejo za zgodovinsko, statistično in znanstveno-raziskovalne namene. Takšen namen mora uporabnik osebnih podatkov pisno izkazati.

Osebni podatki se posredujejo uporabniku osebnih podatkov za namen obdelave iz prejšnjega odstavka v anonimizirani obliki, če zakon ne določa drugače ali če posameznik, na katerega se nanašajo osebni podatki, ni predhodno podal pisne privolitve, da se lahko obdelujejo brez anonimiziranja.

Kadar se v skladu z drugim odstavkom tega člena obdelujejo osebni podatki in če je to primerno, se takšna obdelava praviloma vrši v varni sobi IVZ. Varna soba IVZ je delovni prostor v območju varovanih prostorov IVZ. Delovna postaja v varni sobi nima aktivne nobene enote, ki bi lahko omogočala prenos osebnih podatkov iz varovanih prostorov. Osebne podatke za delo na določen del računalniške mreže, do katerega se lahko dostopa le z računalnika v varni sobi, preko mreže naloži za to pristojna oseba, ki jo določi odgovorna oseba za posamezno zbirko osebnih podatkov. Na posebnih obrazcih se beleži, kdo in kdaj je v varni sobi dostopal do posameznih podatkov. Gesla za dostop do računalnika za delo v varni sobi spreminja oseba, odgovorna za delovanje informacijskega sistema IVZ.

Podrobnejša ureditev obdelave podatkov v varni sobi IVZ je določena z navodili, ki urejajo uporabo varne sobe IVZ.

V varni sobi IVZ se izvede tudi križanje zbirk osebnih podatkov, pri čemer mora direktor na predlog odgovorne osebe ali več odgovornih oseb s sklepom določiti posameznika, ki križanje izvede, in pogoje, pod katerimi se mora križanje izvesti. Direktor lahko pred izdajo sklepa zahteva mnenje Odbora za varstvo osebnih podatkov.

Križanje zbirk osebnih podatkov lahko izvajajo samo zaposleni v IVZ in to le v primeru predhodno izdanega sklepa iz prejšnjega odstavka.

11. člen

Elektronska pošta in lokalne delovne postaje se uporabljajo v službene namene.

Ne glede na prejšnji odstavek se elektronska pošta in ostala programska oprema na lokalnih delovnih postajah lahko uporabljajo v omejenem obsegu in razumnih mejah tudi v zasebne namene. Vsebina elektronske pošte ne sme vsebovati neprimerne, žaljive, škodljive ali nelegalne vsebine.

Oseba, odgovorna za delovanje informacijskega sistema IVZ, lahko na posebej utemeljeno pisno zahtevo direktorja v prisotnosti komisije iz 4. odstavka tega člena, v izrednih primerih (nenadna odpoved zaposlenega, smrt zaposlenega ali drug izreden dogodek) vpogleda v elektronsko pošto zaposlenega le, če je to neobhodno nujno potrebno za vodenje oziroma nadaljevanje delovnega procesa.

Vpogled v vsebino službene elektronske pošte zaposlenega opravi tričlanska komisija, ki jo vsakokrat imenuje direktor. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik.

Če se pojavi utemeljen sum, da zaposleni ne spoštujejo omejitev iz drugega odstavka tega člena, lahko oseba, odgovorna za delovanje informacijskega sistema IVZ, na posebej utemeljeno pisno zahtevo direktorja opravi nadzor količine uporabe elektronske pošte, a zgolj z vidika obsega priponk, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebine elektronske pošte.

O namenu uporabe elektronske pošte in ostale programske opreme iz prvega in drugega odstavka tega člena ter možnosti nadzora iz tretjega in četrtega odstavka tega člena mora biti zaposleni pisno obveščen. Kot zadostno obvestilo se šteje objava tega pravilnika na intranetu IVZ in obvestilo vsem zaposlenim po e-pošti.

12. člen

Internet se uporablja v službene namene.

Ne glede na prejšnji odstavek se internet lahko uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene. Obiskane internetne strani ne smejo vsebovati neprimerne, žaljive, škodljive ali nelegalne vsebine.

Direktor lahko s posebno odredbo pisno odredi blokado določenih spletnih strani. Blokado dostopa do določenih spletnih strani na podlagi pisne odredbe direktorja izvede oseba, odgovorna za delovanje informacijskega sistema IVZ.

O blokadi se obvesti vse zaposlene po elektronski pošti in z objavo na intranetu IVZ.

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

13. člen

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

Dostop do varovanih prostorov je mogoč le v rednem delovnem času IVZ, izven tega časa pa samo na podlagi pisnega dovoljenja odgovorne osebe za zbirke osebnih podatkov, ki se nahajajo v varovanih prostorih.

Ključi varovanih in ostalih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključi se ne smejo puščati v ključavnici v vratih z zunanje strani. Vodi se evidenca izdaje in vrnitve ključev izven delovnega časa oziroma elektronska evidenca kartičnega vstopa in izstopa.

Rezervni ključi za vstop v varovane prostore se hranijo izven rednega delovnega časa pri uslužbencu službe za varovanje objekta, ki sme izdati ključ samo osebam, ki teh prostorih delajo, ali direktorju.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti zaposlenih, 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 na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov, morajo biti stalno zaklenjeni.

Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov. Če se občutljivi osebni podatki hranijo tudi v papirni obliki, morajo biti shranjeni v zaklenjenih ognjevarnih omarah.

14. člen

Za prostore, v katerih se nahajajo osebni podatki oziroma nosilci teh podatkov (varovani prostori) veljajo še naslednja pravila:

- zadrževanje zaposlenih v teh prostorih, razen tistih, ki v njih delajo ali pa je njihova prisotnost nujno potrebna za nemoteno opravljanje delovnih nalog, ni dovoljeno brez odobritve odgovorne osebe za zbirke osebnih podatkov, ki se obdelujejo v teh prostorih;
- obiski zunanjih strank so dovoljeni samo z odobritvijo odgovorne osebe za zbirke osebnih podatkov, ki se nahajajo v varovanih prostorih, in v stalnem spremstvu zaposlenega v IVZ, ki ga določi odgovorna oseba za zbirke osebnih podatkov, ki se obdelujejo v teh prostorih;
- obiski serviserjev oziroma vzdrževalcev informacijske ali telekomunikacijske opreme so dovoljeni samo na poziv, serviserja oziroma vzdrževalca pa mora med obiskom nadzorovati zaposleni v IVZ, ki ga za to določi odgovorna oseba za zbirke osebnih podatkov, ki se obdelujejo v teh prostorih.

15. člen

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

16. člen

Vzdrževanje in popravila strojne računalniške in druge opreme (ki se uporablja za obdelavo osebnih podatkov) je dovoljeno samo z vednostjo osebe, odgovorne za delovanje informacijskega sistema IVZ, in vednostjo odgovorne osebe za zbirke osebnih podatkov, ki se obdelujejo v teh prostorih, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z IVZ sklenjeno ustrezno pogodbo oziroma pisni dogovor.

17. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih samo z vednostjo odgovorne osebe za zbirke osebnih podatkov, ki se obdelujejo v teh prostorih.

Zaposleni v varovanih prostorih morajo po zaključku svojega rednega delovnega časa zagotoviti, da je v prostorih popolnoma 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). V primeru, da to iz kakršnega koli razloga ni izvedljivo, se lahko čistilke in varnostniki v varovanih prostorih gibajo oziroma opravljajo svoje delo le ob prisotnosti zaposlenih v prostoru.

18. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim, ki jih določi oseba, odgovorna za delovanje informacijskega sistema IVZ v soglasju z direktorjem, ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

19. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme (ki se uporablja za obdelavo osebnih podatkov) je dovoljeno samo na podlagi odobritve direktorja po predhodnem predlogu osebe, odgovorne za delovanje informacijskega sistema IVZ, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije ter posamezniki, ki imajo z IVZ sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

20. člen

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

21. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov in druge škodljive programske opreme. Ob pojavu računalniškega virusa oziroma druge škodljive programske opreme se to čim prej odpravi s pomočjo organizacijske enote, ki je na IVZ odgovorna za informacijsko-komunikacijsko tehnologijo, obenem pa se ugotovi vzrok pojava virusa oziroma škodljive programske opreme v računalniškem informacijskem sistemu.

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

22. člen

Zaposleni ne smejo namestiti nobene programske opreme brez vednosti osebe, odgovorne za delovanje informacijskega sistema IVZ. Prav tako ne smejo odnašati programske opreme iz prostorov IVZ brez odobritve vodje organizacijske enote in vednosti osebe, odgovorne za delovanje informacijskega sistema IVZ.

23. člen

Pristop do osebnih podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.

Sistem gesel iz prejšnjega odstavka mora omogočati možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

Oseba, odgovorna za delovanje informacijskega sistema, določi režim dodeljevanja, hranjenja in spreminjanja gesel.

Kadar kontrola in evidentiranje dostopa do podatkov in drugih virov temelji na osebnih geslih, mora uporabnik geslo zamenjati najkasneje po 3 mesecih uporabe, pri tem pa ne sme uporabiti iste kombinacije znakov.

24. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervisorska oziroma nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnicah in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih lahko samo s pisno privolitvijo lastnika gesla, brez privolitve pa le v naslednjih primerih:

- smrt lastnika gesla,
- daljša bolezen ali drugo zdravstveno stanje lastnika gesla, ki onemogoča pridobitev pisne privolitve, kadar je geslo nujno potrebno pridobiti zaradi izvajanja obveznosti, ki jih določajo predpisi,
- prenehanje delovnega razmerja lastnika gesla, če ob prenehanju ni bila opravljena primopredaja zaradi razlogov na strani lastnika gesla.

Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova gesla.

25. 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. Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

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

26. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (v nadaljevanju pogodbeni obdelovalec), se sklene pisna pogodba, predvidena v drugem odstavku 11. člena ZVOP-1. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

Pogodbeni obdelovalci smejo opravljati samo storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe iz prejšnjega odstavka in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pogodbeni obdelovalci, ki za IVZ opravljajo dogovorjene storitve izven prostorov IVZ, morajo imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

V. ODBOR ZA VARSTVO OSEBNIH PODATKOV

27. člen

Na IVZ direktor s sklepom ustanovi Odbor za varstvo osebnih podatkov (v nadaljevanju odbor), ki predstavlja posvetovalno telo za področje varstva osebnih podatkov. Člane odbora imenuje

direktor izmed zaposlenih v IVZ, lahko pa tudi zunanjih strokovnjakov. Član in vodja odbora je po svoji funkciji predstojnik Zdravstvenopodatkovnega centra.

Presojo odbora lahko zahtevata direktor ali odgovorna oseba za posamezno zbirko osebnih podatkov predvsem v primerih, ko so za odločanje o utemeljenosti oziroma upravičenosti do posredovanja ali druge obdelave osebnih podatkov potrebna znanja z različnih strokovnih področij. Zahtevo se naslovi na predstojnika Zdravstvenopodatkovnega centra.

Naloge odbora so predvsem:
- presojanje utemeljenosti posredovanja osebnih podatkov uporabniku v skladu s tem pravilnikom, kadar presojo odbora zahteva odgovorna oseba za posamezno zbirko osebnih podatkov ali direktor,
- presojanje utemeljenosti druge obdelave osebnih podatkov v skladu s tem pravilnikom (tudi križanja zbirk osebnih podatkov), kadar presojo odbora zahteva odgovorna oseba za posamezno zbirko osebnih podatkov ali direktor,
- presojanje, ali gre v posameznih primerih za obdelavo osebnih podatkov, kadar to vnaprej ni nedvoumno jasno, kadar presojo zahteva odgovorna oseba za posamezno zbirko osebnih podatkov ali direktor,
- obravnavanje zadev in svetovanje direktorju in odgovornim osebam glede vprašanj, ki jih ni mogoče rešiti s splošnimi pravili s področja varstva osebnih podatkov.

Odbor za varstvo osebnih podatkov se sestaja po potrebi, vendar najmanj dvakrat letno. O posameznem zahtevku za presojo upravičenosti posredovanja ali druge obdelave osebnih podatkov mora odbor podati svoje mnenje najkasneje v desetih dneh od prejema zahteve. Končno odločitev o upravičenosti do posredovanja osebnih podatkov ali do vpogleda v zbirko osebnih podatkov sprejme odgovorna oseba za zbirko osebnih podatkov, na katero se podatki nanašajo. Končno odločitev o drugih obdelavah (npr. križanje zbirk osebnih podatkov) sprejme direktor.

Seje odbora sklicuje predstojnik Zdravstvenopodatkovnega centra, ki skrbi za spoštovanje roka iz prejšnjega odstavka.

Odbor za varstvo osebnih podatkov enkrat letno pripravi poročilo o svojem delu in ga posreduje direktorju.

VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

28. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih oziroma osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti odgovorno osebo ali direktorja, sami pa poskušajo z zakonitimi ukrepi takšno aktivnost preprečiti.

VII. ZAUPNI PODATKI

29. člen

Kot zaupni so poleg osebnih podatkov na IVZ opredeljeni tudi vsi ostali podatki, ki so tako pomembni, da bi z njihovo izdajo nastale ali lahko nastale hujše škodljive posledice za IVZ ali za posameznika. Podatke, ki so določeni kot zaupni, so dolžni zaposleni in zunanji sodelavci varovati kot poslovno skrivnost.

Direktor sporoča ostale podatke, ki imajo značaj poslovne skrivnosti in so označeni kot zaupni.

Z žigi, papirji z glavo oziroma logotipom IVZ in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati kot z zaupnimi podatki.

VIII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

30. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so zadolžene odgovorne osebe za vsako od zbirk osebnih podatkov, ki so določene v Prilogi 2 tega pravilnika in ki odgovarjajo za morebitne kršitve postopkov in ukrepov za zavarovanje osebnih podatkov.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravljajo: direktor, notranji revizor, pomočnik direktorja, oseba, odgovorna za delovanje informacijskega sistema IVZ, ali druge osebe, ki jih za to določi direktor s sklepom.

31. člen

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

Vsak zaposleni na IVZ, ki na delovnem mestu obdeluje osebne podatke, mora podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami pravilnika, ki na IVZ ureja zavarovanje osebnih podatkov, ter določbami ZVOP-1, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega pravilnika in ZVOP-1. Obrazec izjave je naveden v Prilogi 3 tega pravilnika.

Tudi vse ostale osebe, ki v IVZ delajo na podlagi pogodb civilnega prava (na primer podjemne, avtorske pogodbe in podobno) ali na podlagi drugega razmerja (na primer študentsko delo) in ki pri svojem delu obdelujejo osebne podatke, morajo pred pričetkom svojega dela v IVZ podpisati posebno izjavo, s katero se zavezujejo varovati osebne in zaupne podatke, s katerimi se bodo seznanile med delom v IVZ. Izjava je lahko že sestavni del pogodbe z zunanjimi sodelavci, kadar se z njimi sklepa pogodba. Vzorec izjave je naveden v Prilogi 4 tega pravilnika.

32. člen

Za zaposlene na IVZ kršitev določil tega pravilnika šteje za hujšo kršitev delovnih obveznosti, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

Odgovornost iz prejšnjega odstavka ne izključuje kazenske ali odškodninske odgovornosti.

IX. PREHODNE IN KONČNE DOLOČBE

33. člen

V kolikor sledljivost obdelave osebnih podatkov (možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil) ni zagotovljena že z aplikacijo, s katero se upravlja posamezna zbirka osebnih podatkov, ali pa če se zbirka osebnih podatkov vodi tudi ali zgolj v papirni obliki, se za zagotavljanje spoštovanja določb ZVOP-1 glede sledljivosti obdelave za vsako takšno zbirko osebnih podatkov

vodi evidenca obdelav. Evidenco obdelav vzpostavi in vodi oseba, ki jo pisno določi odgovorna oseba za zbirko osebnih podatkov. V evidenco obdelav se vpiše vsaj, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani, kateri osebni podatki so bili obdelani in kdo je to storil. Vpisovanje in vodenje evidence obdelav podrobneje določi posamezna odgovorna oseba s pisnimi navodili.

34. člen

Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o varstvu osebnih in zaupnih podatkov ter o varovanju dokumentarnega gradiva št. 900-013-17/09 z dne 4. 12. 2009 ter spremembe in dopolnitve št. 900-013-17/09-1/10 z dne 7. 5. 2010, spremembe in dopolnitve št. 900-013-17/09-2/10 z dne 5. 7. 2010, spremembe in dopolnitve št. 900-013-17/09-3/10 z dne 2. 8. 2010 in spremembe in dopolnitve št. 900-013-17/09-4/10 z dne 11. 11. 2010.

Z dnem uveljavitve tega pravilnika preneha veljati Sklep o imenovanju poblaščene osebe za izvajanje postopkov in ukrepov za varstvo osebnih podatkov, ki je bila imenovana na podlagi Pravilnika o varstvu osebnih in zaupnih podatkov ter o varovanju dokumentarnega gradiva št. 900-013-17/09 z dne 4. 12. 2009, ter Sklep o imenovanju odbora za varstvo osebnih podatkov št. 900-104-75/10 z dne 23. 11. 2010.

35. člen

Ne glede na določila 34. člena pravilnika tudi po uveljavitvi tega pravilnika ostanejo v veljavi Navodila za uporabo varne sobe št. 900-013-18/09 z dne 4. 12. 2009, ki so bila izdana na podlagi Pravilnika o varstvu osebnih in zaupnih podatkov ter o varovanju dokumentarnega gradiva št. 900-013-17/09 z dne 4. 12. 2009.

36. člen

Ta pravilnik je sprejet z dnem podpisa direktorja, veljati pa začne 1. 10. 2011 dan po objavi na intranetni strani IVZ.

Za tolmačenje določb pravilnika je pristojen direktor.

Številka: 0071-015/11/021

V Ljubljani, 14. 9. 2011

INŠTITUT ZA VAROVANJE ZDRAVJA REPUBLIKE SLOVENIJE

Marija Seljak
Direktorica

Priloge:

- *Priloga 1* *Katalogi zbirk osebnih podatkov IVZ,*
- *Priloga 2* *Odgovorne osebe za zbirke osebnih podatkov in osebe, ki lahko obdelujejo osebne podatke v določeni zbirki,*
- *Priloga 3* *Obrazec izjave o varovanju osebnih podatkov (zaposleni),*
- *Priloga 4* *Vzorec izjave o varovanju podatkov (zunanji sodelavci).*