PRAVILNIK
O POSTOPKIH IN UKREPIH ZA ZAVAROVANJE OSEBNIH PODATKOV

Verzija dokumenta	: 1.1
Datum veljavnosti	:
Skrbnik dokumenta	: generalni sekretar
Oznaka dokumenta	: 020-5/2010/48

Zgodovina dokumenta

Verzija dokumenta	Status	Bistvene spremembe glede na prejšnjo verzijo	Datum začetka veljave
1.0	končna		5. 5. 2011
1.1	dopolnjena	prilagoditev določb glede na spremenjeno dejansko stanje po selitvi IP na novo lokacijo (15.3.2013), uskladitev s Pravilnikom o postopkih in ukrepih pri delovanju in vzdrževanju informacijskega okolja Informacijskega pooblaščenca	

Priprava, pregled in potrditev

Podpisnik in funkcija podpisnika	Datum podpisa	Podpis
mag. Andrej Tomšič, namestnik IP		
Alenka Jerše, generalna sekretarka		
Nataša Pirc Musar, informacijska pooblaščenka		

Na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št, 94/07, uradno prečiščeno besedilo) in 3. odstavka 2. člena Zakona o Informacijskem pooblaščencu (Uradni list RS, št. 113/05) izdaja Informacijski pooblaščenec naslednji

PRAVILNIK
o postopkih in ukrepih za zavarovanje osebnih podatkov

I. SPLOŠNE DOLOČBE

Vsebina in namen pravilnika

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov pri Informacijskem pooblaščencu z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava osebnih podatkov.

Določbe tega pravilnika se smiselno uporabljajo tudi za zavarovanje podatkov, ki so v dokumentarnem gradivu pri Informacijskem pooblaščencu s strani subjektov zasebnega prava označeni kot poslovne skrivnosti. Varovanje tajnih podatkov ureja poseben pravilnik.

Zaposleni pri Informacijskem pooblaščencu 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.

Pomen izrazov

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. Osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
2. 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;
3. 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;
4. 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);
5. 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;
6. 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;
7. Uporabnik osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
8. Nosilec podatkov - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);
9. Poslovna skrivnost - so podatki, ki so označeni z oznako zaupnosti v skladu z Zakonom o gospodarskih družbah.

II. OBDELAVA OSEBNIH PODATKOV

Vzpostavitev zbirke osebnih podatkov

3. člen

Posamezno zbirko osebnih podatkov na posameznem delovnem področju Informacijskega pooblaščenca vzpostavi odgovorna oseba za določeno zbirko osebnih podatkov (v nadaljevanju: odgovorna oseba), ki jo določi pooblaščenec.

Obdelava osebnih podatkov

4. člen

(1) V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno zakonsko podlago po določbah Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo; v nadaljevanju: zakon).

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

(3) Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

(4) O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbo 19. člena zakona.

(5) 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 zakona ter z vsebino tega pravilnika.

Evidentiranje dokumentov

5. člen

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

Posredovanje osebnih podatkov

6. člen

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

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

(3) Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

Evidenca posredovanj

7. člen

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

- kateri osebni podatki so bili posredovani,
- osebno ime/firmo in naslov/sedež osebe, ki so ji bili posredovani osebni podatki, oziroma navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
- datum in ura posredovanja osebnih podatkov ter
- pravna podlaga, na kateri so bili posredovani osebni podatki.

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

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

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

Posredovanje osebnih podatkov znotraj Informacijskega pooblaščenca

8. člen

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

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

(3) Oseba iz četrtega odstavka prejšnjega člena mora zaznamovati vsako posredovanje občutljivih osebnih podatkov znotraj Informacijskega pooblaščenca v skladu s prejšnjim členom.

Pregledovanje, prepisovanje in kopiranje osebnih podatkov s strani strank oziroma upravičencev

9. člen

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

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

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

katerega je ugotovljena identiteta ter namen, zaredi katerega je bil opravljen pregled, prepis oziroma kopiranje dokumenta.

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

Kopiranje in tiskanje osebnih podatkov s strani zaposlenih

10. člen

(1) Zaposleni pri Informacijskemu pooblaščencu, 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.

Hramba osebnih podatkov

11. člen

(1) Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe razviden iz 7. točke kataloga zbirke osebnih podatkov.

(2) 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.

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

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

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

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

(7) Pri prenosu nosilcev podatkov, ki vsebujejo 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.

(8) Prenos nosilcev podatkov, ki vsebujejo občutljive osebne podatke, na mesto uničenja ter uničevanje takih nosilcev podatkov nadzoruje posebna tričlanska komisija, ki jo imenuje pooblaščenec.

(9) Komisijo iz prejšnjega odstavka sestavljajo zaposleni pri Informacijskemu pooblaščencu, en član komisije je odgovorna oseba.

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

Katalog zbirke osebnih podatkov

12. člen

Opis zbirk osebnih podatkov, katerih upravljavec je Informacijski pooblaščenec, se vodi v katalogu zbirk osebnih podatkov (opisu zbirk osebnih podatkov), ki se vodi v skladu z določbami 26. člena zakona. Podatki iz 1., 2., 4., 5., 6., 9., 10., 12. in 13. točke katalogov zbirk osebnih podatkov se posredujejo 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.

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

Informacijski pooblaščenec je dolžan 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 delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov ter osebno ime in delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov.

III. PODROČNE UREDITVE VARSTVA OSEBNIH PODATKOV

Evidentiranje obiskovalcev

13. člen

(1) Administrativno tehnična služba Informacijskega pooblaščenca lahko vodi knjigo obiskovalcev, v katero za namene varovanja premoženja, življenja ali telesa posameznika ter reda v prostorih Informacijskega pooblaščenca lahko vpiše vsako osebo, ki namerava vstopiti v ali izstopiti iz prostorov Informacijskega pooblaščenca, z izjemo zaposlenih pri Informacijskemu pooblaščencu.

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

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

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

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

Elektronska pošta in uporaba druge programske opreme na računalniku

14. člen

(1) Elektronska pošta in računalnik se uporabljata v službene namene.

(2) Ne glede na prejšnji odstavek se elektronska pošta in ostala programska oprema na računalniku lahko uporabljata v omejenem obsegu in razumnih mejah tudi v zasebne namene. Vsebina elektronske pošte v zasebne namene ne sme biti neprimerna ali žaljiva.

(3) Oseba, zadolžena za delovanje računalniškega informacijskega sistema, lahko na posebej utemeljeno pisno zahtevo pooblaščenca v prisotnosti komisije iz 4. odstavka tega člena, v izrednih primerih (nenadna odpoved delavca, smrt delavca, ali drug izreden dogodek) vpogleda v elektronsko pošto le, če je to nujno potrebno za vodenje delovnega procesa.

(4) Vpogled v vsebino e-pošte zaposlenega opravi 3 članska komisija, ki jo vsakokrat imenuje pooblaščenec. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik.

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

(6) 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 na intranetnem portalu Pooblaščenca in obvestilo vsem zaposlenim po e-pošti.

(7) Vpogled v telefonske prometne podatke priključkov, katerih lastnik je Informacijski pooblaščenec, lahko informacijski pooblaščenec zahteva od operaterjev telekomunikacijskih storitev ali vzdrževalca hišne centrale le takrat, kadar pride med Informacijskim pooblaščencem in zaposlenim do kakršnegakoli spora glede višine stroškov porabe konkretnega telefonskega priključka.

Internet

15. člen

(1) Internet se uporablja v službene namene.

(2) Ne glede na prejšnji odstavek se internet lahko uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene. Internetne strani, ki se pregledujejo v zasebne namene, ne smejo vsebovati neprimerne ali žaljive vsebine.

(3) Pooblaščenec lahko s posebno odredbo odredi blokado določenih spletnih strani.

(4) Blokado dostopa do določenih spletnih strani izvede oseba, zadolžena za delovanje računalniškega informacijskega sistema, na podlagi pisne odredbe pooblaščenca.

(5) O blokadi se obvesti vse zaposlene po elektronski pošti in z objavo na intranetnem portalu Pooblaščenca.

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

Varovanje prostorov

16. člen

(1) Prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke, tajne podatke in druge varovane podatke, strojna in programska oprema (v nadaljevanju: varovani prostori), morajo biti varovani z organizacijskimi in/ali tehničnimi ukrepi iz tega pravilnika, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

(2) Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven njega pa samo na podlagi dovoljenja pooblaščenca.

(3) Vsak zaposleni ima službeno kartico, s katero lahko vstopa v vse varovane prostore pri Informacijskemu pooblaščencu, razen v prostore, kjer se hranijo tajni podatki, v prostore s strojno in računalniško opremo ter v prostore arhiva. V prostore, kjer se hranijo tajni podatki, lahko s službeno kartico vstopajo samo zaposleni, ki imajo pravico do vpogleda v tajne podatke, v prostore, kjer se nahaja strojna in programska oprema, pa zgolj tisti, ki so po pooblastilu pooblaščenca pristojni za nadzor in vzdrževanje opreme, in pooblaščenec. V kletne prostore arhiva lahko poleg Pooblaščenca vstopajo tudi zaposleni v Administrativno tehnični službi Pooblaščenca, namestniki Pooblaščenca ter generalni sekretar Pooblaščenca in oseba zadolžena za delovanje računalniškega informacijskega sistema.

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

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

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

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

(8) Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

Varovanje nosilcev podatkov, ki vsebujejo osebne podatke

17. člen

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

(2) Nosilci podatkov, ki vsebujejo občutljive osebne podatke, se ne smejo hraniti izven varovanih prostorov.

(3) Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni odnašajo izven prostorov Informacijskega pooblaščenca samo z dovoljenjem pooblaščenca.

(4) Nosilcev podatkov, ki vsebujejo občutljive osebne podatke, zaposleni ne smejo odnašati izven prostorov Informacijskega pooblaščenca, razen izjemoma z dovoljenjem pooblaščenca, če je to nujno potrebno za reševanje zadeve, ki vsebuje te občutljive osebne podatke.

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

Varovanje strojne in programske opreme

18. člen

(1) Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo z Informacijskim pooblaščencem sklenjeno ustrezno pogodbo.

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

(3) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije ter posamezniki, ki imajo z Informacijskim pooblaščencem sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

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

(5) Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se vsakodnevno preveri z vidika prisotnosti računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu Informacijskega pooblaščenca.

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

(7) Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz prostorov Informacijskega pooblaščenca brez odobritve pooblaščenca in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

(8) Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vnešeni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil.

(9) Oseba, zadolžena za delovanje računalniškega informacijskega sistema, določi režim dodeljevanja, hranjenja in spreminjanja gesel.

(10) Postopke varnostnega kopiranja in posodabljanja varnostnih mehanizmov ureja Pravilnik o postopkih in ukrepih pri delovanju in vzdrževanju informacijskega okolja Informacijskega pooblaščenca.

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

Pogodbena obdelava

19. člen

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (v nadaljevanju: pogodbeni obdelovalec), Informacijski pooblaščenec sklene pisno pogodbo, določeno v drugem odstavku 11. člena zakona.

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

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

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

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

(6) Vodi se seznam zunanjih izvajalcev, ki vsebuje: naziv in sedež pravne osebe, ime in priimek oseb, ki izvajajo zunanje storitve ter kontaktne podatke teh oseb (naslov e-pošte in telefonska številka). Seznam se hrani na mrežnem disku J:\, dostop do seznama je omejen na zaposlene osebe v Administrativno tehnični službi Pooblaščenca in Delovnem področju informacijske tehnologije. Seznam se po potrebi ažurira.

VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

Obveščanje

20. člen

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

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

Izvajanje postopkov in ukrepov

21. člen

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

Odgovornost za izvajanje in nadzor nad izvajanjem

22. člen

(1) Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov, določenih s tem pravilnikom, so odgovorne pooblaščene osebe, ki jih imenuje pooblaščenec.

(2) Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja generalni sekretar skupaj z osebo, zadolženo za delovanje računalniškega informacijskega sistema.

Izjava

23. člen

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

(2) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami zakona, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega pravilnika in zakona.

Odgovornost za kršitev

24. člen

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

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

VIII. KONČNE DOLOČBE

Začetek veljavnosti

25. člen

Z dnem začetka uporabe tega pravilnika preneha veljati Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov št. 020-5/2010/26, z dne 5. 5. 2011.

Ta pravilnik prične veljati na dan objave na spletnih straneh Informacijskega pooblaščenca.

Informacijski pooblaščenec:
Nataša Pirc Musar, univ. dipl., prav.,
pooblaščenka

V Ljubljani, dne 30. 5. 2013