

Na podlagi 16. člena Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14 in 90/14) in 38. člena Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10 in 60/11) ministrica za notranje zadeve izdaja

PRAVILNIK

o varovanju tajnih podatkov na Ministrstvu za notranje zadeve

I. SPLOŠNE DOLOČBE

1. člen (vsebina)

(1) S tem pravilnikom se natančneje določajo splošni in posebni postopki ter ukrepi za varovanje in obravnavanje tajnih podatkov na Ministrstvu za notranje zadeve in organih v njegovi sestavi (v nadaljevanju: ministrstvo), ki so določeni v Zakonu o tajnih podatkih (v nadaljevanju: zakon) ter predpisih, sprejetih na njegovi podlagi.

(2) Določene pristojnosti, naloge in postopke podregistrskega sistema NATO in Evropske unije (v nadaljevanju: EU) določajo tudi posebni predpisi.

2. člen (namen)

Namen pravilnika je enotna ureditev splošnih in posebnih postopkov ter ukrepov za zagotavljanje učinkovitega varovanja tajnih podatkov na ministrstvu.

3. člen (veljavnost)

Določbe tega pravilnika veljajo za vse zaposlene na ministrstvu. Ta pravilnik, morajo upoštevati tudi zunanji izvajalci in pogodbeni delavci ministrstva.

4. člen (pomen izrazov)

Poleg izrazov, opredeljenih v zakonu, in predpisih, sprejetih na njegovi podlagi, se v tem pravilniku uporabljajo še izrazi z naslednjim pomenom:

1. predstojnik organa: minister za notranje zadeve;
2. predstojnik organa v sestavi: generalni direktor policije ali glavni inšpektor;
3. ministrstvo: notranje organizacijske enote ministrstva in organa v sestavi ministrstva;

4. organa v sestavi: Inšpektorat Republike Slovenije za notranje zadeve in policija;
5. prostori ministrstva: prostori, objekti in okoliši ministrstva, v katerih se varujejo in obravnavajo tajni podatki;
6. uslužbenec: javni uslužbenec, zaposlen na ministrstvu;
7. uradne osebe s posebnimi pooblastili: uradniki, zaposleni v notranji organizacijski enoti ministrstva, pristojni za usmerjanje in nadzor, ki se izkazujejo s službeno izkaznico;
8. vodja varnostnega območja: uslužbenec, odgovoren za izvajanje predpisanih ukrepov in postopkov za varno obravnavanje tajnih podatkov v posameznem varnostnem območju;
9. informacijski sistem: programska, strojna, komunikacijska in kriptografska oprema, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugemu obravnavanju tajnih podatkov v elektronski obliki na ministrstvu; v policiji je opredeljen kot informacijsko-telekomunikacijski sistem;
10. drugi informacijski sistemi: Informacijsko-komunikacijski sistem, ki ni v upravljanju in pod nadzorom ministrstva;
11. upravljavec informacijskega sistema: uslužbenec, odgovoren za vzpostavitev, vodenje in vzdrževanje informacijskega sistema, skladno z Uredbo o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih;
12. vodja informacijske varnosti: uslužbenec, odgovoren za izvajanje predpisov in ukrepov s področja tajnih podatkov v informacijskem sistemu, skladno z Uredbo o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih;
13. lokalni vodja informacijske varnosti: uslužbenec, odgovoren za izvajanje predpisov in ukrepov s področja tajnih podatkov v informacijskem sistemu, skladno z Uredbo o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih, v primeru, da informacijski sistem vsebuje tudi dislocirane enote;
14. skrbnik kriptografskega materiala: uslužbenec, odgovoren za upravljanje s kriptografskim materialom in za pravilno obravnavanje in hranjenje kriptografskega materiala;
15. informacijski varnostni dogodek: vsak dogodek, ki lahko vpliva na varnost tajnih podatkov v informacijskem sistemu ali na delovanje informacijskega sistema;
16. varnostno območje MNZ: varnostno območje II. stopnje, v 4. nadstropju Litostrojske 54 v Ljubljani, ki obsega tudi podregister tajnih podatkov EU in podregister tajnih podatkov zveze NATO.

5. člen

(pooblaščen osebe)

(1) Predstojnik organa v aktu o notranji organizaciji, sistemizaciji, delovnih mestih in nazivih na ministrstvu določi delovna mesta na ministrstvu, na katerih imajo zaposleni:

1. pooblastilo za določanje tajnosti podatkov, spreminjanje stopnje tajnosti podatkov in preklic tajnosti podatkov,
2. pooblastilo za pregled tajnih podatkov,
3. pooblastilo za razmnoževanje in kopiranje tajnih podatkov,
4. pooblastilo za prevajanje tajnih podatkov,
5. pooblastilo za podajo predlogov za izdajo dovoljenja za dostop do tajnih podatkov,
6. pooblastilo za podajo predlogov za izdajo dovoljenja za dostop do tujih tajnih podatkov in preklic dovoljenja za dostop do tujih tajnih podatkov,
7. pooblastilo za podajo predlogov za vmesno varnostno preverjanje in odrejanje prepovedi začasnega dostopa do tajnih podatkov.

(2) Predstojnik organa oziroma predstojnik organa v sestavi določi uslužbence ministrstva, ki imajo:

1. pooblastilo za sprejem pošte, ki vsebuje tajne podatke,
2. pooblastilo za odpiranje pošte, ki vsebuje tajne podatke,
3. pooblastilo za prenos tajnih podatkov,
4. pooblastilo za opravljanje razgovorov z uslužbenci,
5. pooblastilo za uporabo naprav in opreme, nameščenih v prostorih varnostnega območja,
6. pooblastilo za samostojen vstop v varnostno območje,
7. pooblastilo za skrbnika kriptografskega materiala,
8. pooblastilo za samostojen vstop v prostor, v katerem so nameščene ključne sestavine informacijskega sistema.

(3) Predlog za izdajo pooblastil iz prejšnjega odstavka poda vodja notranje organizacijske enote ministrstva, v kateri uslužbenec opravlja delo, ali oseba, ki ga nadomešča. Soglasje za izdajo pooblastila poda notranja organizacijska enota ministrstva, pristojna za tajne podatke.

6. člen *(notranji nadzor)*

(1) Notranji nadzor s področja tajnih podatkov (v nadaljevanju: notranji nadzor) nad izvajanjem zakona in predpisov, sprejetih na njegovi podlagi, ter tega pravilnika se izvaja v skladu z Uredbo o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisi, izdanimi na njegovi podlagi.

(2) Notranji nadzor se v notranjih organizacijskih enotah ministrstva opravi na podlagi odredbe predstojnika organa.

(3) Kadar predstojnik organa odredi notranji nadzor nad policijo, nadzor vodijo uradne osebe s posebnimi pooblastili. Za opravljanje nalog v okviru takšnega nadzora predstojnik organa v odredbi lahko imenuje tudi posamezne uslužbence notranje organizacijske enote ministrstva, pristojne za tajne podatke.

(4) Vodja notranje organizacijske enote ministrstva ali oseba, ki ga nadomešča, je dolžan nadzornikom zagotoviti pogoje za neovirano in nemoteno izvršitev nadzora.

*7. člen
(poročanje)*

Notranje organizacijske enote ministrstva so dolžne enkrat letno na poziv notranje organizacijske enote ministrstva, pristojne za tajne podatke, posredovati statistične podatke glede obravnavanja in poslovanja s tajnimi podatki.

*8. člen
(obvestilna dolžnost ob kadrovskih spremembah)*

Notranja organizacijska enota ministrstva, pristojna za organizacijo in kadre, je dolžna o sklenitvi ali prenehanju delovnega razmerja ter premestitvi posameznega uporabnika informacijskega sistema takoj obvestiti upravljavca informacijskega sistema.

II. VAROVANJE TAJNIH PODATKOV

1. Splošni varnostni ukrepi

*9. člen
(osnovne varnostne dolžnosti uslužbencev)*

Uslužbenec, ki obravnava tajne podatke, je zaradi učinkovitega varovanja tajnih podatkov dolžan izvajati naslednje splošne ukrepe in postopke:

1. ob zapuščanju delovnih prostorov mora zakleniti predale, omare, blagajne in prostore, v katerih se hranijo tajni podatki;
2. številčne kombinacije in ključe od predalov, omar, blagajn in prostorov, v katerih se hranijo tajni podatki, mora zavarovati tako, da niso dostopni nepooblaščenim ali nepoklicanim osebam;
3. dokumentov ali drugih medijev, ki vsebujejo tajne podatke, ne sme puščati brez nadzora;
4. varovati mora gesla za dostop do informacijskega sistema;
5. za opravljanje telefonskih pogovorov, ki vsebujejo tajne podatke, mora uporabljati samo predpisano ščitene (kriptirane) komunikacijske kanale oziroma sredstva;

6. pri dostopu do tajnih podatkov, shranjenih v informacijskih sistemih, mora izvesti postopek osebne prijave;
7. navodila za uporabo informacijskega sistema mora hraniti tako, da niso dostopna nepooblaščenim ali nepoklicanim osebam;
8. ob zaznavi okoliščin, ki bi lahko imele za posledico razkritje tajnih podatkov nepooblaščenim ali nepoklicanim osebam, mora o tem nemudoma obvestiti nadrejenega.

10. člen

(ustno obravnavanje tajnih podatkov)

(1) Kadar se tajni podatki obravnavajo neposredno ustno (npr. sestanek) ali posredno s pomočjo multimedijskih pripomočkov (npr. videokonferenca), mora organizator takšnega dogodka izvesti vse predpisane ukrepe in postopke za varno obravnavanje tajnih podatkov.

(2) Organizator dogodka iz prejšnjega odstavka mora v vabilu navesti stopnjo tajnosti obravnavanih podatkov in pogoje, ki jih morajo izpolnjevati udeleženci dogodka, ter določiti rok, v katerem morajo biti zahtevani podatki posredovani organizatorju dogodka. Vabilo mora vsebovati tudi podatke o morebitni dovoljeni uporabi informacijske in komunikacijske opreme na dogodku.

(3) Organizator dogodka iz prvega odstavka tega člena mora prisotne na dogodku obvestiti o stopnji tajnosti obravnavanih podatkov in preveriti, da vsi udeleženci navedenega dogodka izpolnjujejo pogoje za obravnavanje tajnih podatkov ustrezne stopnje tajnosti. Obvestilo se evidentira v zapisnik ali drug dokument, katerega priloga je seznam prisotnih, potrjen z njihovimi lastnoročnimi podpisi.

(4) Vsaka predstavitev tajnih podatkov na zaslonu ali s pomočjo drugih multimedijskih pripomočkov mora vsebovati vidno oziroma slišno opozorilo, da gre za tajne podatke.

2. Označevanje tajnih podatkov

11. člen

(oznaka o načinu prenehanja tajnosti)

(1) Tajni podatki, ki jim je bila stopnja tajnosti določena na ministrstvu, morajo imeti poleg oznak, predpisanih z zakonom in predpisi, sprejetimi na njegovi podlagi, tudi oznako o načinu prenehanja tajnosti podatka.

(2) Oznaka o načinu prenehanja tajnosti se zapiše pod oznako stopnje tajnosti na prvi strani dokumenta. Na drugem posameznem nosilcu tajnega podatka se oznaka o načinu prenehanja tajnosti doda poleg oznake stopnje tajnosti.

12. člen

(oznaka pregleda tajnega podatka)

Pooblaščen oseba, ki je opravila pregled tajnega podatka v skladu z določbami zakona, ki predpisujejo pregled tajnih podatkov z namenom ocene obstoja potrebe po njihovi tajnosti, mora na sprednji strani

dokumenta oziroma na drugem nosilcu tajnega podatka narediti uradni zaznamek »Pregledano, dne _____«, tiskano izpisati ime in priimek ter se podpisati.

13. člen

(oznake delovnega gradiva)

(1) Delovno gradivo, ki nastane oziroma se uporablja pri obravnavi tajnih podatkov in ni namenjeno drugim osebam oziroma hrambi, se po končanem obravnavanju tajnih podatkov uniči.

(2) Za delovno gradivo, ki vsebuje tajne podatke in po končanem obravnavanju tajnih podatkov ni uničeno, se izdelata pisna ocena škodljivih posledic. To delovno gradivo se označi s predpisanimi oznakami – pod oznako stopnje tajnosti se pripiše oznaka »delovno gradivo«.

3. Varovanje oseb, ki imajo dostop do tajnih podatkov, in način seznanitve uporabnikov z ukrepi in postopki varovanja tajnih podatkov

14. člen

(varnostna tveganja)

(1) Uslužbenci ministrstva morajo biti pred pridobitvijo pravice do dostopa do tajnih podatkov in nato periodično opozorjeni na varnostna tveganja, in sicer:

1. na razgovore z osebami, ki nimajo potrebe po seznanitvi s tajnimi podatki,
2. na njihove odnose z zunanjo javnostjo,
3. na ogrožanja, ki jih predstavlja dejavnost tujih obveščevalnih služb, organizacij in posameznikov.

(2) Uslužbenci se z varnostnimi tveganji seznanjajo na osnovnem in dodatnem usposabljanju s področja obravnavanja in varovanja tajnih podatkov, v razgovorih z nadrejenimi in razgovorih z osebo, ki je za to pisno pooblaščen (v nadaljevanju: pooblaščenec za razgovore).

15. člen

(obveščanje o spremembi podatkov)

(1) Imetnik dovoljenja za dostop do tajnih podatkov (v nadaljevanju: imetnik dovoljenja) je dolžan o vsaki spremembi podatkov iz osnovnega, dodatnega ali posebnega vprašalnika za varnostno preverjanje v najkrajšem času obvestiti pooblaščenca za razgovore.

(2) Imetnik dovoljenja spremenjene podatke vpiše v prvi del obrazca »SPREMEMBA PODATKOV IZ VPRAŠALNIKA« (obrazec TP-SPV). Izpolnjen in podpisan obrazec imetnik posreduje pooblaščenca za razgovore.

(3) Obrazec TP-SPV »SPREMEMBA PODATKOV IZ VPRAŠALNIKA« je objavljen v prilogi 1 tega pravilnika in je njegov sestavni del.

16. člen

(razgovor z imetnikom dovoljenja)

- (1) Pooblaščenec za razgovore v čim krajšem času po prejemu obrazca TP-SPV iz drugega odstavka prejšnjega člena opravi razgovor z imetnikom dovoljenja. Vsebino razgovora in mnenje o obstoju ali neobstoju suma varnostnega zadržka vpiše v drugi del obrazca TP-SPV in ga podpiše.
- (2) Pooblaščenec za razgovore pošlje izpolnjen obrazec TP-SPV uslužbencu, pooblaščenemu za podajo predloga za vmesno varnostno preverjanje (v nadaljevanju: pooblaščen predlagatelj).

17. člen

(naloge pooblaščenega predlagatelja)

- (1) Pooblaščen predlagatelj po seznaitvi z izpolnjenim obrazcem TP-SPV oceni, ali so podani pogoji za podajo predloga za vmesno varnostno preverjanje imetnika dovoljenja.
- (2) Če obstaja sum varnostnega zadržka, pooblaščen predlagatelj poda predlog za vmesno varnostno preverjanje, ki mu priloži izpolnjen obrazec TP-SPV z vsemi dokumenti.
- (3) Pooblaščen predlagatelj, ob podaji predloga za vmesno varnostno preverjanje iz prejšnjega odstavka, imetniku dovoljenja do zaključka postopka varnostnega preverjanja začasno prepove dostop do tajnih podatkov. O tem mora obvestiti predstojnika organa oziroma predstojnika organa v sestavi, notranjo organizacijsko enoto ministrstva, pristojno za tajne podatke, in vodjo notranje organizacijske enote ministrstva, kjer je imetnik dovoljenja zaposlen, da mu onemogočijo dostop do tajnih podatkov.
- (4) Če pooblaščen predlagatelj oceni, da ne obstaja sum varnostnega zadržka, sprememba podatkov pa bi lahko imela za posledico izpostavljenost imetnika dovoljenja, njegovega zakonca, zunajzakonskega partnerja, partnerja iz registrirane istospolne partnerske skupnosti, otrok ali drugih oseb, ki živijo z imetnikom dovoljenja v skupnem gospodinjstvu, mora predlagati ustrezne ukrepe za zagotovitev njihove varnosti in za preprečitev morebitne zlorabe tajnih podatkov.
- (5) Pooblaščen predlagatelj mora o dejstvih in okoliščinah ter sprejetih ukrepih iz prejšnjega odstavka seznaiti predstojnika organa oziroma predstojnika organa v sestavi in notranjo organizacijsko enoto ministrstva, pristojno za tajne podatke.

18. člen

(hramba dokumentov, nastalih v razgovoru z imetnikom dovoljenja)

- (1) Vsi dokumenti, nastali ali pridobljeni v postopku razgovora z imetnikom dovoljenja, se evidentirajo.
- (2) Kadar pooblaščen predlagatelj ne poda predloga za vmesno varnostno preverjanje, dokumente iz prejšnjega odstavka hrani v skladu z določbami Uredbe o upravnem poslovanju.

19. člen

(usposabljanje)

- (1) Notranja organizacijska enota ministrstva, pristojna za tajne podatke, v sodelovanju z notranjo organizacijsko enoto ministrstva, pristojno za organizacijo in kadre, in policijo izvaja osnovna in

dodatna usposabljanja s področja obravnavanja in varovanja tajnih podatkov za zaposlene na ministrstvu.

(2) Za izdajo potrdil o udeležbi na osnovnem ali dodatnem usposabljanju s področja obravnavanja in varovanja tajnih podatkov poskrbi tista notranja organizacijska enota ministrstva, ki je določena v aktu o izvedbi usposabljanja.

(3) Usposabljanje uslužbencev ministrstva za delo v informacijskem sistemu izvajata notranja organizacijska enota ministrstva, pristojna za tajne podatke, in notranja organizacijska enota policije, pristojna za zaščito podatkov, na predlog vodje notranje organizacijske enote, v kateri uslužbenec opravlja delo.

4. Varovanje prostorov in objektov

20. člen *(služba varovanja)*

Prostore in objekte ministrstva, v katerih se obravnavajo tajni podatki, varuje policija z organizacijskimi, fizičnimi in/ali tehničnimi ukrepi.

21. člen *(odgovorna oseba za izdelavo načrta varovanja tajnih podatkov)*

(1) Predstojnik organa oziroma predstojnik organa v sestavi v organu oziroma organu v sestavi, v katerem se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje, določi odgovorno osebo za izdelavo načrta varovanja tajnih podatkov.

(2) Naloge odgovorne osebe za izdelavo načrta varovanja tajnih podatkov so zlasti:

1. izdelava in ažuriranje načrta varovanja tajnih podatkov,
2. načrtovanje, organiziranje in usmerjanje dela v varnostnem območju,
3. izvajanje sistemskih nalog v zvezi z zagotavljanjem varovanja tajnih podatkov na ministrstvu oziroma v organu v sestavi.

22. člen *(vodja varnostnega območja)*

(1) Predstojnik organa oziroma predstojnik organa v sestavi za posamezno varnostno območje v organu oziroma organu v sestavi določi vodjo varnostnega območja.

(2) Naloge vodje varnostnega območja so zlasti:

1. sodelovanje pri izdelavi in ažuriranju načrta varovanja tajnih podatkov v varnostnem območju,
2. sodelovanje pri načrtovanju, organiziranju in usmerjanju dela v varnostnem območju,

3. vodenje seznamov za posamezno varnostno območje ter priprava analiz in informacij, na njihovi podlagi,
4. zagotavljanje varovanja tajnih podatkov v varnostnem območju.

23. člen

(podregister tajnih podatkov EU in NATO)

(1) V sklopu varnostnega območja ministrstva delujeta tudi podregister tajnih podatkov Evropske unije (v nadaljevanju: podregister EU) in podregister tajnih podatkov zveze NATO (v nadaljevanju: podregister NATO), prek katerih se sprejemajo in pošiljajo tajni podatki Evropske unije in zveze NATO z delovnega področja ministrstva.

(2) Predstojnik organa s sklepom določi uslužbenca, ki lahko samostojno vstopajo v prostore podregistra tajnih podatkov.

24. člen

(varnostno-tehnična oprema)

(1) Varnostno-tehnična oprema, ki se lahko uporablja za varovanje posameznega varnostnega ali upravnega območja na ministrstvu, mora izpolnjevati standarde in pogoje, ki so določeni v predpisih oziroma sklepih.

(2) Če za posamezno varnostno-tehnično opremo v Republiki Sloveniji še ni veljavnega standarda, zahtevane lastnosti varnostno-tehnične opreme določi notranja organizacijska enota ministrstva, pristojna za tehnično varovanje, po pridobljenem mnenju notranje organizacijske enote ministrstva, pristojne za tajne podatke.

25. člen

(nameščanje in vzdrževanje varnostno-tehnične opreme)

(1) Varnostno-tehnično opremo namešča in vzdržuje notranja organizacijska enota ministrstva, pristojna za tehnično varovanje.

(2) Zunanji izvajalci, ki izpolnjujejo predpisane pogoje, lahko varnostno-tehnično opremo nameščajo in vzdržujejo le pod neposrednim nadzorom uslužbenca notranje organizacijske enote ministrstva, pristojne za tehnično varovanje.

26. člen

(protiprisluškovalni pregledi)

(1) Protiprisluškovalne preglede varnostnih območij, naprav in opreme za varnostna območja opravlja notranja organizacijska enota policije, pristojna za zaščito podatkov, in sicer na predlog predstojnika organa ali vodje notranje organizacijske enote ministrstva, v čigar pristojnost sodi varnostno območje.

(2) Protiprisluškovalni pregledi drugih prostorov ministrstva, kjer se razpravlja o tajnih podatkih stopnje tajnosti ZAUPNO ali višje, se opravijo na podlagi predloga predstojnika organa ali predstojnikov organov v sestavi.

(3) Predloga za protiprisluškovalni pregled ni dovoljeno pripraviti ali o njem razpravljati v prostoru, ki je predmet protiprisluškovalnega pregleda, niti se ne sme posredovati iz tega prostora.

5. Varovanje dokumentov in medijev, ki vsebujejo tajne podatke, ter kontrola in evidentiranje pošiljanja in distribucije tajnih podatkov

27. člen

(sprejem tajnih podatkov)

Tajne podatke lahko sprejme le uslužbenec, ki je pooblaščen za prevzem oziroma sprejem pošte v fizični ali elektronski obliki in ima dovoljenje za dostop do tajnih podatkov stopnje tajnosti, ki ustreza tajnosti podatka, ali višje stopnje tajnosti.

28. člen

(vstopne točke za tajne podatke)

(1) Vstopna točka za poštne pošiljke, označene s stopnjo tajnosti, ki vsebujejo nacionalne tajne podatke, naslovljene na ministrstvo, razen na policijske uprave in policijske postaje, je varnostno območje MNZ.

(2) Vstopna točka za poštne pošiljke, označene s stopnjo tajnosti, ki vsebujejo tuje tajne podatke, naslovljene na ministrstvo, je varnostno območje MNZ.

(3) Vstopna točka za poštne pošiljke, označene s stopnjo tajnosti ZAUPNO ali višje, ki vsebujejo nacionalne tajne podatke in so naslovljene na posamezne policijske uprave ali notranje organizacijske enote policijskih uprav, je varnostno območje posamezne policijske uprave.

(4) Vstopna točka za poštne pošiljke, označene s stopnjo tajnosti INTERNO, ki vsebujejo nacionalne tajne podatke in so naslovljene na posamezne policijske uprave ali posamezne notranje organizacijske enote policijskih uprav, je v upravnem območju posamezne policijske enote oziroma posamezne policijske uprave.

(5) Ne glede na določbe prejšnjih odstavkov tega člena, lahko predstojnik organa, v skladu z 21. členom Uredbe o varovanju tajnih podatkov, za posamezne pošiljke, označene s stopnjo tajnosti, odredi dodatno vstopno točko in način poslovanja s tajnimi podatki na tej točki.

(6) Vstopna točka za pošiljke v elektronski obliki, označene s stopnjo tajnosti, ki so naslovljene na ministrstvo, je informacijski sistem, ki ima izdano varnostno dovoljenje za delovanje informacijskega sistema, skladno z Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih.

29. člen

(kurirska dejavnost)

(1) Na ministrstvu kurirsko službo za prenos tajnih podatkov organizira in izvaja policija. Za potrebe ministrstva, razen policijskih uprav in policijskih postaj, kurirsko službo izvaja OKC GPU, za potrebe

policijskih uprav oziroma notranjih organizacijskih enot policijskih uprav pa kurirsko službo za prenos tajnih podatkov organizira posamezni OKC policijske uprave.

(2) Kurir ob predaji tajnega podatka preveri, ali ima prejemnik tajnega podatka pooblastilo za sprejem tajnih podatkov in ustrezno dovoljenje za dostop do tajnih podatkov.

30. člen
(sledljivost)

Sledljivost dokumentov, ki vsebujejo tajne podatke, se zagotavlja z evidenco tajnih podatkov v evidenci dokumentarnega gradiva ali v drugih aplikacijah ter s kurirsko oziroma dostavno knjigo. Evidenca tajnih podatkov mora ves čas omogočati pregled nad tem, komu je bil posamezen tajni podatek izročen in kje trenutno je.

31. člen
(hramba)

(1) Notranje organizacijske enote ministrstva morajo nacionalne tajne podatke stopnje tajnosti ZAUPNO ali višje po končani obravnavi vrniti v varnostno območje.

(2) Notranje organizacijske enote ministrstva morajo tajne podatke Evropske unije in zveze NATO stopnje tajnosti ZAUPNO ali višje po končani obravnavi vrniti v hrambo podregistru EU oziroma podregistru NATO.

32. člen
(tekoča zbirka)

(1) Dokument, ki vsebuje tajne podatke stopnje tajnosti INTERNO in je del zadeve, uvrščene v tekočo zbirko, se hrani v upravnem območju.

(2) Dokument, ki vsebuje tajne podatke stopnje tajnosti ZAUPNO ali višje in je del zadeve, uvrščene v tekočo zbirko, se hrani ločeno v varnostnem območju MNZ.

33. člen
(stalna zbirka)

(1) Dokument, ki vsebuje tajne podatke stopnje tajnosti INTERNO in je del zadeve, uvrščene v stalno zbirko, se hrani v upravnem območju.

(2) Dokument, ki vsebuje tajne podatke stopnje tajnosti ZAUPNO ali višje in je del zadeve, uvrščene v stalno zbirko, se hrani ločeno v varnostnem območju MNZ.

34. člen
(komisija za uničenje tajnih podatkov)

(1) Uničenje vseh vrst tajnih podatkov na ministrstvu izvaja petčlanska komisija, ki jo imenuje predstojnik organa.

(2) Od petih članov komisije za uničenje tajnih podatkov se imenujeta dva člana iz policije. Kot vodja oziroma predsednik komisije pa se imenuje uslužbenec, zaposlen v notranji organizacijski enoti ministrstva, pristojni za tajne podatke.

(3) Zapisnik o uničenju mora predsednik komisije za uničenje tajnega podatka posredovati v hrambo v varnostno območje MNZ. Zapisnik se evidentira kot lastni dokument in se hrani trajno (T).

35. člen

(brisanje podatkov na elektronskih nosilcih)

(1) Brisanje tajnih podatkov stopnje tajnosti INTERNO na elektronskih nosilcih podatkov se izvede le za tiste elektronske nosilce podatkov, ki bodo namenjeni ponovni uporabi znotraj ministrstva.

(2) Za brisanje tajnih podatkov na elektronskih nosilcih podatkov se lahko uporabijo le namenska oprema in postopki, ki večkratno prepišejo/izbrišejo podatke in tako zagotavljajo, da podatkov ni mogoče rekonstruirati z orodji za rekonstrukcijo podatkov. Vsak sektor elektronskega nosilca mora biti najmanj sedemkrat prepisan z različnim bitnim vzorcem.

(3) Postopek brisanja podatkov na elektronskih nosilcih se natančneje določi s posebnim navodilom, ki ga izda predstojnik organa.

36. člen

(fizično uničenje elektronskih nosilcev podatkov)

(1) Fizično uničenje tajnih podatkov na elektronskih nosilcih podatkov se izvede za vse tiste elektronske nosilce podatkov, ki ne bodo namenjeni ponovni uporabi znotraj ministrstva.

(2) Optični pomnilni mediji (BD, CD, DVD, CD-RW, CD-R, CD-ROM, diskete, itd.) se uničijo z ustrezno metodo fizičnega uničenja (razrez z rezalnikom).

(3) Za fizično uničenje tajnih podatkov na ostalih elektronskih nosilcih podatkov (Solid State Disk, USB-ključi, pomnilniške kartice, trdi diski, diskete, magnetni trakovi, itd.) se najprej uporabijo namenske naprave, ki v postopku razmagnetanja vplivajo na elektronski nosilec podatkov s spreminjajočim magnetnim poljem.

(4) Po fizičnem uničenju optičnih pomnilnih medijev in ostalih elektronskih nosilcev podatkov se uporabi še ustrezna metoda kemičnega uničenja ali zažiga.

(5) Postopek fizičnega uničenja elektronskih nosilcev podatkov se natančneje določi s posebnim navodilom, ki ga izda predstojnik organa.

6. Varovanje komunikacij, po katerih se prenašajo tajni podatki

37. člen

(skrbnik kriptografskega materiala)

(1) Predstojnik organa za vsako lokacijo, kjer je kriptografski material, pooblasti skrbnika kriptografskega materiala in uporabnike, ki imajo dostop do kriptografskega materiala.

(2) Uporabnik iz prejšnjega odstavka mora imeti dovoljenje za dostop do tajnih podatkov najmanj stopnje tajnosti ZAUPNO, izkazati potrebo po seznanitvi in podpisati dokument »Kriptografska avtorizacija«.

38. člen

(informacijski varnostni dogodek)

Vsakdo, ki zazna informacijski varnostni dogodek, mora svojo zaznavo takoj sporočiti vodji informacijske varnosti ali lokalni vodji informacijske varnosti ter svojemu neposrednemu vodji.

39. člen

(varovanje podatkov v informacijskih sistemih)

(1) V informacijskih sistemih se tajni podatki varujejo z ukrepi in postopki, s katerimi se:

1. uporabnikom informacijskega sistema dostop do tajnih podatkov omejuje na podatke, ki jih potrebujejo za izvajanje delovnih nalog in za katere posedujejo ustrezno dovoljenje,
2. preprečuje razkritje tajnih podatkov nepoklicanim osebam,
3. preprečuje zloraba, nepooblaščen dostop, nepooblaščen sprememba ali nepooblaščen izbris tajnih podatkov in
4. pri obravnavanju tajnih podatkov stopnje tajnosti ZAUPNO ali višje omogoča poznejše ugotavljanje, kdaj so bili posamezni tajni podatki obravnavani, komu so bili posredovani in kdo je to storil.

(2) Tajni podatki stopnje tajnosti STROGO TAJNO se lahko obdelujejo na samostojni delovni postaji ali v okviru informacijskega sistema, ki je fizično ločen od drugih delov informacijskega sistema.

40. člen

(ščitenje informacijskega sistema)

(1) Informacijski sistemi morajo biti učinkovito zaščiteni pred računalniškimi virusi in drugo škodljivo programsko opremo.

(2) Ključne sestavine informacijskega sistema, v katerem se obravnavajo tajni podatki stopnje tajnosti INTERNO, morajo biti v upravnem območju.

(3) Ključne sestavine informacijskega sistema, v katerem se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje, morajo biti v varnostnem območju.

(4) V prostor, v katerem so nameščene ključne sestavine informacijskega sistema, lahko samostojno vstopajo le pooblaščen osebe. Druge osebe lahko v ta prostor vstopajo le v spremstvu prej navedenih pooblaščenih oseb.

41. člen

(varovanje povezav z drugimi informacijskimi sistemi in uporaba interneta)

(1) Informacijski sistem za obravnavanje tajnih podatkov stopnje tajnosti INTERNO sme imeti povezave z drugimi informacijskimi sistemi, če so povezave primerno varovane. Povezovanje lahko poteka le prek namenskih povezovalnih točk v informacijskem sistemu. Prenos tajnih podatkov stopnje tajnosti INTERNO izven varnostnega oziroma upravnega območja mora biti varovan z odobrenimi šifrirnimi rešitvami, ki jih potrdi notranja organizacijska enota ministrstva, stvarno pristojna za varovanje tajnih podatkov v informacijskem sistemu.

(2) Povezovalne točke morajo biti opremljene z varnostnimi pregradami in drugimi varnostnimi mehanizmi, ki onemogočajo zlorabe informacijskega sistema. Varnostne mehanizme potrdi notranja organizacijska enota ministrstva, stvarno pristojna za varovanje tajnih podatkov v informacijskem sistemu.

(3) Elektronska izmenjava tajnih podatkov z drugimi organi in organizacijami se izvaja z vzpostavitvijo dostopne točke informacijskega sistema v drugem organu ali organizaciji ali z vzpostavitvijo dostopne točke drugega informacijskega sistema na ministrstvu.

(4) Dostop do drugih informacijskih sistemov imajo lahko le tisti uslužbenci, ki to potrebujejo zaradi izvajanja svojih delovnih nalog.

(5) Informacijski sistem je lahko povezan z drugimi informacijskimi sistemi samo na tak način, da nepoklicane osebe nimajo dostopa do tajnih podatkov ali naprav informacijskega sistema.

(6) Informacijski sistem nima povezave z drugim informacijskim sistemom, če je od njega fizično ločen ali če je z njim fizično povezan, vendar logično ločen in zaščiten v skladu s standardi tako, da ni možnosti, da bi se podatki med sistemoma izmenjevali.

(7) Informacijski sistem za obravnavanje tajnih podatkov stopnje tajnosti ZAUPNO ali višje ni dovoljeno povezovati z drugimi informacijskimi sistemi. Ti informacijski sistemi ne smejo imeti povezave z internetom.

(8) Uslužbenci lahko kot uporabniki informacijskega sistema do interneta dostopajo le prek skupne, enotne priključne točke informacijskega sistema na internet.

(9) Delovna postaja, ki je z internetom povezana mimo varnostne pregrade, ne sme biti povezana z informacijskim sistemom, na njej ne smejo biti shranjeni tajni podatki, nameščena pa mora biti zaščita pred škodljivimi vsebinami. Način neposredne povezave in varovanje te povezave določi notranja organizacijska enota ministrstva, stvarno pristojna za varovanje tajnih podatkov v informacijskem sistemu.

42. člen

(prenos tajnih podatkov v informacijskem sistemu)

(1) Prenos tajnih podatkov stopnje tajnosti STROGO TAJNO prek informacijskega sistema izven varnostnega območja ni dovoljen.

(2) Prenos tajnih podatkov stopnje tajnosti INTERNO, ZAUPNO in TAJNO izven varnostnega oziroma upravnega območja mora biti varovan z odobrenimi šifrirnimi rešitvami.

7. Varovanje opreme, s katero se obravnavajo tajni podatki

43. člen

(oprema informacijskega sistema)

(1) Oprema, namenjena obravnavanju tajnih podatkov v informacijskem sistemu, mora biti praviloma v lasti ministrstva.

(2) Kadar oprema, namenjena obravnavanju tajnih podatkov v informacijskem sistemu, ni v lasti ministrstva, mora biti sklenjen sporazum med ministrstvom in lastnikom takšne opreme, v katerem so opredeljene pristojnosti, obveznosti in odgovornosti o ravnanju s to opremo.

(3) Informacijska in komunikacijska oprema, namenjena varovanju in zaščiti tajnih podatkov v informacijskem sistemu, mora biti v skladu s standardi, ki jih na podlagi tehničnih in normativnih rešitev Komisije Vlade Republike Slovenije za informacijsko varnost določi notranja organizacijska enota ministrstva, stvarno pristojna za varovanje tajnih podatkov v informacijskem sistemu.

(4) Za strojno opremo, ki se vgrajuje v informacijski sistem, mora notranja organizacijska enota ministrstva, pristojna za vzdrževanje informacijskih sistemov, v sodelovanju z upravljavcem informacijskega sistema določiti, kdo jo sme vgrajevati, vzdrževati in odstranjevati.

(5) Notranja organizacijska enota ministrstva, pristojna za vzdrževanje informacijskih sistemov, si mora pred določitvijo ukrepov iz tretjega odstavka tega člena pridobiti soglasje notranje organizacijske enote ministrstva, stvarno pristojne za varovanje tajnih podatkov v informacijskem sistemu.

(6) V informacijskem sistemu se uporablja kriptografska oprema, ki ima izdano potrdilo o varnostni ustreznosti in jo odobri notranja organizacijska enota ministrstva, stvarno pristojna za varovanje tajnih podatkov v informacijskem sistemu.

(7) Nacionalni kriptografski material za ščitenje tajnih podatkov stopnje tajnosti ZAUPNO ali višje sme biti v bližini elektronske opreme tuje države ali mednarodne organizacije, če so izpolnjeni pogoji in standardi, ki so določeni v predpisih in drugih aktih s področja izvajanja zaščite pred neželenim elektromagnetnim sevanjem.

(8) Za vso programsko opremo, vgrajeno v informacijski sistem, mora upravljavec informacijskega sistema določiti:

1. kdo jo sme brisati, kopirati ali spreminjati,
2. kje se hranijo kopije programske opreme in
3. kdo je odgovoren za ažurnost kopij.

44. člen

(zaščita pred neželenim elektromagnetnim sevanjem)

(1) Uporaba elektronske opreme za obravnavo tajnih podatkov stopnje tajnosti ZAUPNO, TAJNO in STROGO TAJNO se mora ščititi z varnostnimi ukrepi in postopki, ki nepoklicanim osebam preprečujejo razkritje podatkov prek neželenega elektromagnetnega sevanja.

(2) Varnostna območja, v katerih so naprave, katerih neželeno elektromagnetno sevanje bi lahko povzročilo razkritje tajnih podatkov stopnje tajnosti ZAUPNO ali višje, morajo biti zaščitena pred neželenim elektromagnetnim sevanjem.

(3) Zaščita pred neželenim elektromagnetnim sevanjem se zagotavlja s kombinacijo lastnosti opreme in prostora, v katerem je oprema. Lastnosti se kombinirajo tako, da je elektromagnetno sevanje omejeno oziroma zadušeno do take mere, da tajni podatki zaradi neželenega elektromagnetnega sevanja niso ogroženi.

(4) Pregled zaščite pred neželenim elektromagnetnim sevanjem v varnostnem območju se opravi:

1. ob vzpostavitvi varnostnega območja,
2. ob vsakem gradbenem, vzdrževalnem in drugem podobnem posegu v varnostnem območju,
3. ob zamenjavi pisarniške opreme,
4. ob spremembi zaposlenih v varnostnem območju,
5. na zahtevo vodje enote, v okviru katere je varnostno območje, ali
6. v drugih primerih, ko pregled odredi predstojnik organa.

45. člen

(uporaba opreme informacijskega sistema izven upravnega ali varnostnega območja)

Uslužbenci so z opremo informacijskega sistema, dolžni ravnati na način, ki onemogoča, da bi oprema prišla v roke nepoklicani osebi. Oprema informacijskega sistema mora biti ves čas uporabe izven upravnega oziroma varnostnega območja varovana z enakimi ali primerljivimi ukrepi in postopki, kot so določeni za varovanje tajnih podatkov.

46. člen

(vzdrževanje opreme informacijskega sistema)

(1) O vsaki okvari oziroma izpadu strojne in programske opreme informacijskega sistema je uporabnik te opreme dolžan takoj obvestiti upravljavca informacijskega sistema.

(2) Vse pogodbe in postopki v zvezi z vzdrževanjem in servisiranjem opreme informacijskega sistema morajo vsebovati varnostne zahteve in pogoje, ki jih mora izpolnjevati vzdrževalno osebje oziroma oprema izvajalca vzdrževanja oziroma servisiranja.

(3) Vzdrževanje in servisiranje opreme informacijskega sistema smejo izvajati le tista podjetja oziroma pravne osebe, ki imajo ustrezno varnostno dovoljenje za organizacijo.

(4) Če se vzdrževanje in servisiranje opravlja na lokaciji zunanjega izvajalca, mora ta imeti ustrezno varnostno dovoljenje za organizacijo iz 35. člena zakona in vzpostavljeno upravno oziroma ustrezno varnostno območje.

47. člen

(varnostne kopije programske opreme in podatkov informacijskega sistema)

(1) V skladu z oceno varnostnih tveganj informacijskega sistema je upravljavec informacijskega sistema v sodelovanju z notranjo organizacijsko enoto, pristojno za vzdrževanje informacijskih sistemov, dolžan izdelati načrt izdelave varnostnih kopij za programsko opremo in podatke v informacijskem sistemu. V načrtu morajo biti predvideni izdelovalci varnostnih kopij, roki, način izdelovanja kopij in mediji, na katerih se hranijo kopije ter drugi podatki, ki so potrebni za učinkovito izdelovanje in hrambo kopij.

(2) Varnostne kopije programske opreme in podatkov v informacijskem sistemu morajo biti shranjene v skladu s stopnjo tajnosti podatkov praviloma izven objekta ali v zaščiteni blagajni izven prostora, v katerem so originali.

8. Kontrola in evidentiranje dostopov do tajnih podatkov

48. člen

(seznam vpogledov)

(1) Uslužbenci so vsak vpogled v tajni podatek oziroma seznanitev s tajnim podatkom stopenj tajnosti **TAJNO** in **STROGO TAJNO**, razen pri vpogledu v tajni podatek v informacijskem sistemu, dolžni evidentirati v obrazec »seznam vpogledov«.

(2) Vsebina in oblika obrazca »seznam vpogledov« je objavljena v prilogi 2 tega pravilnika.

49. člen

(posredovanje tajnih podatkov drugim osebam ali organizacijam)

Uslužbenec mora pred posredovanjem tajnih podatkov drugi osebi ali organizaciji preveriti, ali ta oseba ali organizacija izpolnjuje predpisane pogoje za obravnavanje tajnih podatkov.

50. člen

(identifikacija in overitev dostopa uporabnikov informacijskega sistema)

(1) Dostop do tajnih podatkov mora biti varovan na način, ki preveri identiteto uporabnika in njegova pooblastila za dostop do tajnih podatkov ter evidentira dostop.

(2) Sistem ugotavljanja identitete in preverjanja pooblastil uporabnika informacijskega sistema mora biti zgrajen tako, da je otežena lažna predstavitev identitete ali zloraba identitete drugega uporabnika.

(3) Vsak uporabnik informacijskega sistema mora imeti svojo lastno prijavo, ki ga enolično identificira v informacijskem sistemu in ki jo je dolžan varovati. Zloraba prijave ali sum, da lahko drug uporabnik zlorabi njegovo prijavo, se šteje kot informacijski varnostni dogodek.

(4) Kadar kontrola in evidentiranje dostopa do tajnih podatkov temeljita na osebnem geslu, si mora geslo določiti uporabnik sam, in sicer v skladu z varnostnimi navodili za delo v informacijskem sistemu.

(5) Kontrola in evidentiranje dostopa do tajnih podatkov lahko temeljita tudi na drugih metodah, ki omogočajo zanesljiv in nedvoumen postopek identifikacije (biometrične značilnosti, pametna kartica ipd.).

(6) S sistemi kontrole in evidentiranja dostopa do tajnih podatkov upravlja upravljavec informacijskega sistema.

51. člen

(spremljanje in nadzor pristopa v informacijski sistem in dostopa do tajnih podatkov)

(1) Spremljanje in nadzor pristopa v informacijski sistem in dostopa do tajnih podatkov stopnje tajnosti ZAUPNO ali višje morata biti evidentirana v dnevniku dela (npr. datoteka .log), ki mora omogočati revizijsko nespremenjeno naknadno ugotavljanje naslednjih podatkov:

1. kateri uporabnik je obravnaval tajne podatke,
2. katere tajne podatke je obravnaval,
3. čas obravnave tajnih podatkov,
4. katere funkcije informacijskega sistema je uporabljal in
5. fizična lokacija terminala ali delovne postaje, s katere je uporabnik obravnaval tajne podatke.

(2) V dokumentih, potrebnih za izdajo varnostnega dovoljenja za delovanje informacijskega sistema, se določi obdobje, za katerega se posamezni podatki iz dnevnika dela hranijo, če ni s predpisi določeno drugače.

(3) Z dnevniki dela upravlja upravljavec informacijskega sistema. Upravljavca informacijskega sistema določi podrobnejši način vodenja in vsebino podatkov, ki se vodijo v dnevniku dela, ter način evidentiranja izvedbenih in kontrolnih posegov v informacijski sistem.

(4) Predstojnik organa lahko na predlog upravljavca informacijskega sistema za spremljanje določenih podatkov iz dnevnika dela pooblasti tudi posameznega uslužbenca.

(5) Nadzor posegov v informacijskem sistemu izvajata upravljavec informacijskega sistema in vodja informacijske varnosti.

III. PREHODNE IN KONČNE DOLOČBE

52. člen

(veljavnost drugih aktov)

- (1) Do zdaj izdani sklepi in pooblastila ostanejo v veljavi do izdaje novih sklepov in pooblastil.
- (2) Novi sklepi in pooblastila morajo biti izdani v roku treh mesecev po uveljavitvi tega pravilnika.

53. člen

(izdaja navodila o poslovanju s tajnimi podatki)

V šestih mesecih po uveljavitvi tega pravilnika predstojnik organa izda navodilo o poslovanju s tajnimi podatki, ki bo na ministrstvu uredilo enotno poslovanje s tajnimi podatki.

54. člen

(prehodno obdobje za usklajitev)

Ostale akte in postopke je treba uskladiti z določbami tega pravilnika v treh mescih po uveljavitvi tega pravilnika.

55. člen

(razveljavitvena določba)

Z dnem veljavnosti tega pravilnika prenehata veljati Pravilnik o varovanju tajnih podatkov na Ministrstvu za notranje zadeve, št. 007-15-2007/49 z dne 31. 5. 2008, in Pravilnik o spremembi Pravilnika o varovanju tajnih podatkov na Ministrstvu za notranje zadeve, št. 007-102/2009/15 z dne 15. 5. 2009.

56. člen

(uveljavitvena določba)

Ta pravilnik začne veljati z dnem 1. 6. 2016. Pravilnik se objavi na intranetu Ministrstva za notranje zadeve in intranetu policije.

Številka: 007-262/2015/32 (144-05)

Datum: 18. 05. 2016



Mag. Vesna Gyomai Žnidar
Ministrica

Priloga 1: Sprememba podatkov iz vprašalnika

Priloga 2: Seznam vpogledov