Na podlagi četrtega odstavka 17. člena, šestega in desetega odstavka 39. člena ter osmega in štirinajstega odstavka 39.a člena Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10 in 60/11 in 8/20) izdaja Vlada Republike Slovenije

U R E D B O

o varovanju tajnih podatkov

I. SPLOŠNE DOLOČBE

1. člen
(namen uredbe)

Ta uredba določa načine in oblike označevanja tajnih podatkov, fizične, organizacijske in tehnične ukrepe ter obvezne sestavine postopkov za varovanje tajnih podatkov, ki jih morajo pri vzpostavitvi sistema ukrepov in postopkov varovanja tajnih podatkov upoštevati in zagotoviti vsi organi in organizacije iz drugega in tretjega odstavka 1. člena Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20; v nadaljnjem besedilu: zakon).

2. člen
(namen ukrepov varovanja)

(1) Namen ukrepov varovanja tajnih podatkov je, da se z vzpostavitvijo ukrepov neposrednega fizičnega varovanja tajnih podatkov, varovanih prostorov ali objektov (fizični ukrepi), ukrepov ravnanja organa pri obravnavanju tajnih podatkov (organizacijski ukrepi) ter ukrepov varovanja tajnih podatkov, varovanih prostorov ali objektov s tehničnimi sredstvi skladno s to uredbo (tehnični ukrepi), vzpostavi sistem postopkov in ukrepov varovanja tajnih podatkov, ki ustreza stopnji tajnosti tajnih podatkov in stopnji tajnosti komunikacijsko informacijskih sistemov ter onemogoča njihovo razkritje nepooblaščenim osebam.

(2) Določbe, ki v tej uredbi urejajo varovanje tajnih podatkov veljajo tudi za varovanje tajnih podatkov tujih držav ali mednarodnih organizacij, razen če ni izrecno navedeno drugače.

3. člen
(pomen izrazov)

Izrazi uporabljeni v tej uredbi pomenijo:

1. javni prostor je prostor, dostopen vsem, v katerem se odvija javno življenje;
2. lastna prenosna mreža je organizirana znotraj posameznega organa ali organizacije za fizični prenos tajnih podatkov;
3. komunikacijsko informacijski sistem (v nadaljnjem besedilu: sistem) je namenjen varovanju tajnih podatkov, ki ga sestavljajo programska, strojna, komunikacijska in druga oprema in deluje samostojno ali v omrežju ter je

namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi podatkov v elektronski obliki;

4. varovanje tajnih podatkov v komunikacijsko informacijskih sistemih zajema določanje in uporabo ukrepov varovanja tajnih podatkov, ki se obravnavajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti tajnih podatkov ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov;
5. elektronski nosilec podatkov je vsako sredstvo, na katerem je možno dolgoročno shranjevati podatke v elektronski obliki (trdi diski, diskete, magnetni trakovi, elektronski pomnilni nosilci podatkov, optični pomnilni nosilci podatkov);
6. ključne sestavine sistema so strežniki, usmerjevalniki in delilniki prometa, oprema za upravljanje in nadzor, aktivna oprema za prenos podatkov v nešifrirani obliki, oprema za kriptirno zaščito podatkov, varnostne pregrade, oprema za odkrivanje in zaščito pred vdori, oprema za izdelavo varnostnih kopij in druge;
7. iznos podatka iz sistema pomeni tiskanje, shranjevanje na izmenljivi elektronski nosilec podatkov (USB ključ, CD/DVD nosilec podatkov, zunanji disk ...) ali izmenjavo z drugim sistemom s pomočjo medsebojne povezave sistemov;
8. neželeno elektromagnetno sevanje je sevanje, ki se nekontrolirano razširja in omogoča nepooblaščeno seznanitev s tajnimi podatki;
9. revizijska sled je elektronska evidenca dejavnosti sistema tako po sistemskih ter aplikacijskih procesih kot po uporabniški rabi sistema in aplikacij ter omogoča odkrivanje varnostnih kršitev, težav z zmogljivostjo, rekonstrukcijo dogodkov in analizo.
10. razvid je namensko in sistematično spremljanje, beleženje ali vodenje podatkov;
11. preostalo varnostno tveganje je tveganje, ki v sistemu ostane tudi po implementaciji varnostnih ukrepov;
12. kriptografija je znanstvena veda, ki se ukvarja s konstrukcijo in analizo kriptografskih prvin in protokolov, kateri zagotavljajo zaupnost, celovitost, pristnost, razpoložljivost in nezatajljivost;
13. kriptografska rešitev je strojna in/ali programska oprema ter z njo povezani sestavni deli, ki so vgrajeni v sistem in so namenjeni zaščiti podatkov s pomočjo kriptografije;
14. kriptografski algoritem je končno zaporedje pravil ali ukazov, ki sosledje bitov, ki predstavlja čistopis, pretvori v drugo sosledje, ki predstavlja neberljivo sporočilo.
15. kriptografske prvine so osnovni sestavni deli kriptografske rešitve;
16. overjanje je preverjanje pristnosti entitete;

II. DOLOČANJE IN OZNAČEVANJE TAJNIH PODATKOV

4. člen
(določanje tajnih podatkov)

Pooblaščena oseba, določena v 10. členu zakona, s pisno oceno, glede na možne škodljive posledice, podatkom določi ustrezno stopnjo tajnosti. V pisni oceni

opredeli katere podatke je treba varovati, razloge za določitev stopnje tajnosti ter določi način prenehanja tajnega podatka.

5. člen
(hramba pisne ocene)

Pisna ocena, na podlagi katere je bila določena stopnja tajnosti podatka se hrani skladno z rokom hrambe tajnega podatka.

6. člen
(označevanje tajnih podatkov)

(1) Vsak dokument, nosilec podatkov in ključna sestavina sistema mora biti ob določitvi stopnje tajnosti vidno označena s predpisanimi oznakami stopnje tajnosti. Vsi dokumenti morajo imeti na vseh straneh dokumenta, v glavi in nogi označeno stopnjo tajnosti vključno z zunanjimi stranmi prednjih platnic, če obstajajo. Vsaka stran dokumenta mora imeti v nogi poleg stopnje tajnosti navedeno tudi zaporedno številko strani glede na skupno število strani dokumenta (npr. 3/10). Naslovna stran je lahko brez oznake zaporedne številke strani. Oznaka stopnje tajnosti na nosilcih (npr. zemljevidi, fotografije, CD/DVD, USB), ki vsebujejo tajne podatke, mora biti na nosilcu podatkov vidno natiskana, natipkana, napisana, naslikana, nalepljena ali kako drugače pritrjena s primernimi sredstvi.

(2) Naslov dokumenta mora biti oblikovan na način, da ne vsebuje tajnih podatkov. Če to ni mogoče se na koncu naslova, ki vsebuje tajne podatke vpiše oznako stopnje tajnosti npr. (I).

(3) Če spremni dopis ne vsebuje tajnih podatkov, se ne označi s stopnjo tajnosti. Pri navajanju prilog, ki vsebujejo tajne podatke se poleg navedbe priloge vpiše oznaka stopnje tajnosti npr. (I).

(4) Če se dokument ali nosilec podatkov hrani v kakršnemkoli ovoju, mora le ta biti označen z ustrezno stopnjo tajnosti.

(5) Z označevanjem dokumentov ali nosilcev podatkov se tajnega podatka ne sme uničiti, poškodovati ali povzročiti, da postane kako drugače neuporaben.

(6) Sistem mora imeti vgrajen mehanizem, ki uporabnika seznani s tajnostjo pri prikazu ali iznosu. V primeru, da sistem ne omogoča prikaza stopnje tajnosti posameznega podatka, je dolžnost upravljavca sistema zagotoviti, da se uporabnika sistema nedvoumno seznani ob vsakokratnem vstopu v sistem z najvišjo stopnjo varovanja tajnih podatkov v sistemu.

(7) V primeru, da je tajnost podatka določil organ, ki ni upravljavec sistema, mora imeti prikaz oznako tega organa.

(8) Vsi dokumenti ali nosilci podatkov, ki vsebujejo tajne podatke morajo poleg oznak, določenih v tem členu, vsebovati številko dokumenta in datum pisne ocene iz četrtega člena te uredbe.

(9) Vsi dokumenti ali nosilci podatkov stopnje tajnosti TAJNO in STROGO TAJNO morajo poleg oznak, določenih v tej uredbi, vsebovati še:

- številko izvoda dokumenta;
- števil morebitnih prilog.

(10) Vsi dokumenti, ki so označeni s stopnjo tajnosti STROGO TAJNO, se poleg oznak, predpisanih v tej uredbi, dodatno označijo z rdečo črto debeline najmanj štiri milimetre, ki poteka diagonalno pod kotom 45 stopinj štiri centimetre od zgornjega desnega roba strani.

(11) Oznaka stopnje tajnosti se mora jasno razlikovati od drugih zapisov, pri čemer se za zapis oznake uporabijo poudarjene velike tiskane črke, ki morajo biti večje od črk preostalih zapisov.

(12) Oznake stopnje tajnosti iz tega člena so razvidne iz vzorcev oznak INTERNO, ZAUPNO, TAJNO IN STROGO TAJNO, ki so v Prilogi 1, ki je sestavni del te uredbe.

7. člen
(označevanje tujih tajnih podatkov)

Tuji tajni podatki ohranijo izvirno oznako.

8. člen
(izjemno označevanje)

(1) V dokumentu, ki vsebuje tajne podatke, se izjemoma lahko označi vsak odstavek, del odstavka ali posamezna beseda z različno stopnjo tajnosti, in sicer tako, da:

- se na začetku in koncu vsakega odstavka, dela odstavka ali besede vpišejo oznake (I), (Z), (T), (ST);
- je dokument, ki vsebuje več delov besedila različnih stopenj tajnosti, označen z najvišjo stopnjo tajnosti posameznega odstavka;
- se v prostor za dodatne oznake vpiše, da so odstavki/deli odstavkov/ posamezne besede označeni z različno stopnjo tajnosti.

(2) Pooblaščena oseba, ki je določila stopnjo tajnosti, mora v pisni oceni zapisati tudi razloge za določitev različne stopnje tajnosti posameznih delov besedila.

9. člen
(označevanje sprememb stopnje tajnosti ali preklica)

(1) Kadar se tajnemu podatku spremeni stopnja tajnosti ali se tajni podatek prekliče, se na dokumentu ali nosilcu podatkov, ki vsebuje tajni podatek, prečrtajo prvotne oznake tajnosti, pod staro oznako ali nad njo pa se navede novo oznako stopnje tajnosti ali preklic stopnje tajnosti. Poleg navedenih oznak se na dokumentu navede še sklic na pisno obrazložitev spremembe ali preklica stopnje tajnosti. Aplikacija za evidentiranje in hranjenje dokumentarnega gradiva v elektronski obliki mora omogočati razvid vseh sprememb označevanja in podlag za te spremembe.

(2) Tajnim podatkom v dokumentih, ki so označeni še po predpisih, ki so veljali pred uveljavitvijo Zakona o tajnih podatkih (Uradni list RS, št. 87/01), se ob njihovi ponovni uporabi določi stopnja tajnosti v skladu z zakonom in to uredbo. Stare

oznake stopnje tajnosti se prečrtajo, pod ali nad njimi, pa se navedejo nove oznake stopnje tajnosti.

(3) Pooblaščena oseba organa, ki je tajnemu podatku spremenila stopnjo tajnosti ali jo preklicala mora o spremembi ali preklicu obvestiti vse, ki so tajni podatek prejeli ali imajo dostop do njega.

10. člen
(označevanje kopij)

(1) Fizična kopija celotnega ali dela dokumenta, ki vsebuje tajne podatke, mora imeti oznako stopnje tajnosti izvirnika in oznako, da je kopija, in sicer tako, da se na prvi strani v višini zgornje oznake stopnje tajnosti na desno stran napišeta beseda KOPIJA, njena zaporedna številka in datum izdelave kopije. Tako mora biti označen tudi dodaten izpis tajnega podatka v elektronski obliki, kadar je v obliki kopije.

(2) Iz kopije tajnega podatka mora biti razvidno, iz katerega zapisa ali dela zapisa izhaja kopija (številka, datum, številka strani dokumenta, ki vsebuje tajni podatek).

11. člen
(izločanje tajnih podatkov iz dokumentov)

(1) Če dokument ali njegov del le delno vsebuje tajne podatke, oziroma so le posamezni odstavki dokumenta označeni s stopnjo tajnosti in jih je zaradi izvedbe določenih nalog organa mogoče izločiti iz dokumenta, ne da bi to ogrozilo njihovo tajnost, lahko pooblaščena oseba organa, ki je določila stopnjo tajnosti izloči te podatke iz dokumenta.

(2) Z dokumenta, s katerega so bili skladno s prejšnjim odstavkom izločeni tajni podatki, se odstranijo oznake stopenj tajnosti.

(3) Na dokumentu, iz katerega so bili izločeni tajni podatki, je treba navesti, da so bili iz dokumenta izločeni tajni podatki.

III. OBRAVNAVA IN HRAMBA TAJNIH PODATKOV

12. člen
(obravnava tajnih podatkov)

(1) Tajni podatki stopnje tajnosti INTERNO se obravnavajo v upravnem območju. Tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti se obravnavajo v določenem, vidno označenem prostoru (v nadaljnjem besedilu: varnostno območje), ki je glede na način obravnavanja tajnih podatkov uvrščen v varnostno območje I. ali II. stopnje.

(2) Ne glede na določbo prejšnjega odstavka se lahko tajni podatki stopnje tajnosti ZAUPNO in TAJNO pod določenimi pogoji obravnavajo v upravnem območju.

(3) Tajni podatki do vključno stopnje tajnosti TAJNO se lahko obravnavajo tudi izven varnostnega in upravnega območja ob pogojih določenih s to uredbo.

(4) Kadar je tajni podatek do vključno stopnje tajnosti TAJNO zaradi izvedbe točno določene naloge treba izjemoma obravnavati izven upravnega ali varnostnega območja, mora organ zagotoviti, da se na takšnem območju vzpostavi začasno upravno ali varnostno območje, kjer se smiselno izvajajo ukrepi in postopki, predpisani s to uredbo.

13. člen
(pogoji za vzpostavitev začasnega upravnega območja)

(1) Predstojnik organa ali od njega pooblaščena oseba mora izdelati dokument, v katerem se opredelijo:

- obseg začasnega upravnega območja;
- način varovanja;
- režim vstopa in izstopa;
- in druge potrebne ukrepe ob izrednih dogodkih (za primer požara, vloma, potresa…).

(2) Zagotoviti je treba 24 urno neposredno in neprekinjeno fizično ali tehnično varovanje in kontrolo vstopa oz. preverjanje identitete vstopajočih.

14. člen
(pogoji za vzpostavitev začasnega varnostnega območja)

(1) Predstojnik organa ali od njega pooblaščena oseba mora izdelati dokument, v katerem se opredelijo:

- obseg začasnega varnostnega območja;
- način varovanja;
- režim vstopa in izstopa;
- oceno varnostnih tveganj obravnave tajnih podatkov;
- in druge potrebne ukrepe ob izrednih dogodkih (za primer požara, vloma, potresa…).

(2) Zagotoviti je treba 24 urno neposredno in neprekinjeno fizično varovanje začasnega varnostnega območja in okolice ter kontrola vstopa oz. preverjanje identitete vstopajočih. Fizično varovanje se lahko dopolni z elementi tehničnega varovanja.

(3) Kadar se bo v prostorih, ki niso v upravljanju organa razpravljalo o tajnih podatkih stopnje tajnosti ZAUPNO in višje, se na podlagi presoje iz ocene tveganja, po potrebi opravi proti prisluškovalni pregled.

(4) Tajni podatki stopnje tajnosti ZAUPNO ali višje se morajo hraniti v skladu z določili te uredbe.

(5) Voditi je treba seznam oseb, ki bodo vstopale v začasno varnostno območje.

15. člen
(pogoji za obravnavanje tajnih podatkov izven upravnega in varnostnega območja)

(1) Kadar začasnega upravnega ali varnostnega območja iz tehničnih, organizacijskih in drugih razlogov ni mogoče vzpostaviti se tajni podatki lahko obravnavajo le pod pogoji določenimi v tem členu. Predstojnik organa ali od njega pooblaščena oseba določi, da se za izvedbo določene naloge ali dogodka, tajni podatki varujejo izven upravnega ali varnostnega območja.

(2) Tajnih podatkov ni dovoljeno obravnavati na javnem prostoru oz. na poti. Izjemoma se lahko tajni podatek stopnje tajnosti INTERNO obravnavajo izven upravnega območja, pri čemer je treba zagotoviti, da se s tajnim podatkom ne seznanijo nepooblaščene osebe.

(3) Kadar se tajni podatek stopnje tajnosti INTERNO obravnavajo zunaj upravnega območja je treba zagotoviti, da ima oseba tajni podatek ves čas pod nadzorom.

(4) Kadar se tajni podatek stopnje tajnosti ZAUPNO in TAJNO varuje zunaj varnostnega in upravnega območja je treba zagotoviti, da ima oseba tajni podatek ves čas pod nadzorom in zagotoviti, da se s tajnim podatkom ne seznanijo nepooblaščene osebe. Oseba, ki tak tajni podatek obravnava zunaj varnostnega in upravnega območja mora biti oborožena ali v spremstvu oborožene osebe.

(5) Obravnavanje tajnih podatkov izven varnostnega in upravnega območja je dovoljeno v sistemih z izdanim varnostnim dovoljenjem za delovanje in z uporabo kriptografskih rešitev z izdanim potrdilom o varnostni ustreznosti. Sistemi, kriptografske rešitve in podatki morajo biti zaščiteni pred nepooblaščenim dostopom

(6) Vsak iznos ali vnos nosilca tajnega podatka zunaj upravnega ali varnostnega območja se evidentira. Oseba, ki prevzame tajni podatek, to potrdi s podpisom in s tem prevzame odgovornost in skrb za varnost tajnega podatka.

16. člen
(hramba tajnih podatkov)

(1) Tajni podatki stopnje tajnosti INTERNO se hranijo v upravnem območju v pisarniških ali kovinskih omarah. Tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti se hranijo v varnostnem območju II. stopnje v ustreznih blagajnah ali v varnostnem območju I. stopnje.

(2) Organi, tajne podatke, ki so del zadeve organa, hranijo skladno z roki, določenimi s predpisi, ki urejajo poslovanje z dokumentarnim gradivom.

(3) Ne glede na določbo prejšnjega odstavka centralna registra EU in zveze NATO hranita tajne podatke največ dve leti od prejema.

(4) Organizacije tajne podatke hranijo dokler jih potrebujejo za opravljanje delovnih nalog. Po uporabi tajne podatke uničijo skladno z določbami te uredbe ali jih vrnejo pristojnemu organu.

IV. FIZIČNI UKREPI VAROVANJA

17. člen
(varnostno območje I. stopnje)

(1) Varnostno območje I. stopnje je označen prostor, v katerem se lahko varujejo tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti tako, da že sam vstop v varnostno območje pomeni dostop do teh podatkov. V varnostnem območju I. stopnje se izvajajo najmanj ti varnostni postopki in ukrepi:

- jasno določen in varovan perimeter, ki zagotavlja nadzor nad vstopom ali izstopom oseb in vozil v to območje, dovoljuje vstop samo osebam, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov in imajo dovoljenje za vstop v to območje;
- vodenje razvida tajnih podatkov, s katerimi se oseba seznani že ob samem vstopu v varnostno območje;
- prepoved vnosa mehanskih, elektronskih in magnetno optičnih sestavnih delov, s katerimi je mogoče tajne podatke nepooblaščeno posneti, odnesti ali prenesti oziroma kakršnih koli naprav, s katerimi je mogoča zloraba tajnih podatkov. Izjemoma vnos in uporabo takih naprav odobri oseba, odgovorna za varnost varnostnega območja;
- neposredno in neprekinjeno fizično varovanje varnostnega območja ali delovnih prostorov, v katerih se varnostno območje nahaja, in z elektronskim sistemom za protivlomno varovanje varnostnega območja. Po končanem delovnem času se pregledajo prostori. Intervencijski čas po sproženem alarmnem signalu mora biti krajši od sedem minut.

(2) Vstop oseb v varnostno območje in njihov izstop ter dostop vozil mora biti nadzorovan. Vsi vstopi in izstopi se morajo evidentirati.

(3) predstojnik organa določi seznam oseb, ki lahko samostojno vstopajo v varnostno območje I. stopnje .

18. člen
(varnostno območje II. stopnje)

(1) Varnostno območje II. stopnje je označen prostor, v katerem se tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti varujejo tako, da sam vstop in gibanje v tem območju še ne omogoča dostopa do teh podatkov, saj so pred nepooblaščenim dostopom znotraj območja dodatno zaščiteni. V varnostnem območju II. stopnje se izvajajo najmanj ti varnostni postopki in ukrepi:

- jasno določen in varovan perimeter, ki zagotavlja nadzor nad vstopom in izstopom oseb in vozil v to območje in dovoljuje vstop v to območje samo osebam, ki imajo dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti
- vstop brez ustreznega dovoljenja za dostop do tajnih podatkov se lahko omogoči drugim osebam, ki se zaradi opravljanja svoje delovne naloge ne bodo seznanile s tajnimi podatki in imajo ves čas zadrževanja v varnostnem območju zagotovljeno spremstvo oseb iz tretjega odstavka tega člena;
- taka organizacija dela, ki zagotavlja, da bodo imeli zaposleni v organu ali organizaciji, dostop le do tistih tajnih podatkov, ki jih potrebujejo za opravljanje delovnih nalog, in sicer do tiste stopnje tajnosti, za katero imajo dovoljenje;

- ki zagotavljajo, da druge osebe organa ali organizacije, ki niso na seznamu iz tretjega odstavka tega člena, vstopajo v varnostno območje samo v spremstvu oseb iz tretjega odstavka tega člena. ali ob izvajanju druge enakovredne oblike nadzora, ki zagotavlja, da bo oseba vstopila samo v dele območja, povezane z namenom obiska, in če je to potrebno, se bo seznanila le s tistimi tajnimi podatki, ki so povezani z namenom obiska, in sicer do tiste stopnje tajnosti, za katero ima dovoljenje;
- protivlomno varovanje varnostnega območja z elektronskim sistemom, katerega alarmni signal je vezan na enoto, odgovorno za ukrepanje ob alarmu (varnostno nadzorni center). Intervencijski čas po sproženem alarmnem signalu mora biti krajši od petnajstih minut. Izjemoma, kadar to zahteva izvajanje nalog organa, lahko predstojnik organa v sklepu o določitvi varnostnega območja določi, da se intervencijski čas po sproženem alarmnem signalu podaljša, vendar ne več kot na 30 minut. Na podlagi ocene ogroženosti se lahko izvaja tudi neposredno in neprekinjeno fizično varovanje varnostnega območja ali delovnih prostorov, v katerih se varnostno območje nahaja;
- prepoved vnosa mehanskih, elektronskih in magnetno optičnih sestavnih delov, s katerimi je mogoče tajne podatke nepooblaščeno posneti, odnesti ali prenesti oziroma kakršnih koli naprav, s katerimi je mogoča zloraba tajnih podatkov. Izjemoma vnos in uporabo takih naprav odobri oseba, odgovorna za varnost varnostnega območja;
- po končanem delovnem času se varnostno območje varuje s sistemom fizičnega ali protivlomnega varovanja oziroma z občasnimi fizičnimi pregledi prostorov, določenimi v načrtu varovanja.

(2) Vstop oseb v varnostno območje in njihov izstop ter dostop vozil mora biti pod nadzorom. Vsi vstopi in izstopi se morajo evidentirati.

(3) Predstojnik organa določi seznam oseb, ki lahko samostojno vstopajo v varnostno območje II. stopnje

19. člen
(upravno območje)

Upravno območje je vidno določen obseg prostora v katerem organ ali organizacija nadzira vstopanje in izstopanje oseb in vozil ter njihovo gibanje. V upravnih območjih se lahko varujejo tajni podatki stopnje tajnosti INTERNO, z varnostnimi postopki in ukrepi pa morajo zagotavljati, da imajo dostop do teh podatkov samo osebe, ki so s pisno izjavo potrdile, da so seznanjene s predpisi, ki urejajo varovanje tajnih podatkov, in se morajo s temi podatki seznaniti zaradi opravljanja delovnih nalog.

20. člen
(centralni register zveze NATO in EU)

(1) Centralna registra zveze NATO in EU sta pristojna za obravnavanje in varovanje tajnih podatkov zveze NATO in EU stopnje tajnosti ZAUPNO in višje. Centralna registra zveze NATO in EU obravnavata tudi tajne podatke zveze NATO in EU stopnje tajnosti INTERNO, v kolikor jih prejemniki teh podatkov ne prejmejo na drug način ali zanje zaprosijo pristojni register.

(2) Zaposleni v centralnih registrih morajo imeti veljavno dovoljenje za dostop do tajnih podatkov stopnje tajnosti STROGO TAJNO.

(3) Predstojnik organa določi vodjo in namestnika centralnega registra, ki skrbi za izvajanje varnostnih ukrepov v zvezi z varovanjem tajnih podatkov v centralnem registru.

(4) V Centralnem registru zveze NATO predstojnik organa določi pooblaščeno osebo Cosmic Control Officer (CCO), katerega naloge so določene v varnostni politiki zveze NATO.

21. člen
(podregistri in kontrolne točke zveze NATO in EU)

(1) Podregistri in kontrolne točke so pristojni za varovanje tajnih podatkov EU in zveze NATO, stopnje tajnosti ZAUPNO in višjih stopenj tajnosti znotraj posameznih organov. Podregistri in kontrolne točke lahko obravnavajo tudi tajne podatke zveze NATO in EU stopnje tajnosti INTERNO, v kolikor jih prejemniki teh podatkov ne prejmejo na drug način ali zanje zaprosijo pristojni podregister oziroma kontrolno točko.

(2) Podregister ali kontrolna točka se določi na podlagi predhodno opravljenega ogleda. Z ogledom se preveri ali postopki in ukrepi tehničnega in fizičnega varovanja ter organizacija varovanja zagotavljajo ustrezno raven varovanja tajnih podatkov glede na vrsto, količino in oceno ogroženosti tajnih podatkov. Pri ocenjevanju ustreznosti varovanja je treba upoštevati kombinacijo postopkov in ukrepov tehničnega in fizičnega varovanja ter organizacijo varovanja, ki mora biti določena v načrtu varovanja, načrt pa mora biti izdelan pred ogledom.

(3) Zaposleni v podregistrih ali kontrolnih točkah morajo imeti veljavno dovoljenje za dostop do tajnih podatkov najmanj stopnje tajnosti za katero je vzpostavljen podregister ali kontrolna točka.

(4) Predstojnik organa določi vodjo in namestnika podregistra ali kontrolne točke, ki skrbi za izvajanje varnostnih ukrepov v zvezi z varovanjem tajnih podatkov v podregistru ali kontrolni točki.

(5) V podregistru ali kontrolni točki zveze NATO, ki je vzpostavljen za varovanje tajnih podatkov do vključno stopnje tajnosti STROGO TAJNO, predstojnik organa določi pooblaščeno osebo Cosmic Control Officer (CCO), katerega naloge so določene v varnostni politiki zveze NATO.

22. člen
(oprema varnostnega in upravnega območja)

Oprema varnostnega in upravnega območja, in ostali pogoji, ki jih morajo izpolnjevati upravna in varnostna območja, so navedeni v Prilogi 2, ki je sestavni del te uredbe.

23. člen
(identifikacijska izkaznica)

(1) Vse osebe, ki se gibljejo v upravnem ali varnostnem območju, morajo imeti na vidnem mestu pripeto identifikacijsko izkaznico za vstop in gibanje v upravnem oziroma varnostnem območju (v nadaljnjem besedilu: identifikacijska izkaznica). Z internim aktom se lahko izjemoma določi, kdaj nekaterim osebam v upravnem oziroma varnostnem območju ni treba na vidnem mestu nositi identifikacijskih izkaznic.

(2) Podobo identifikacijskih izkaznic in njihovo tehnično izvedbo določi predstojnik organa.

24. člen
(določitev varnostnega in upravnega območja)

(1) Predstojnik organa ali organizacije ali oseba, ki jo on pooblasti, določi varnostna in upravna območja s sklepom in o tem obvesti nacionalni varnostni organ.

(2) Varnostno oziroma upravno območje v organizaciji se določi na podlagi predhodno opravljenega ogleda, ki ga izvede organ, pristojen za izdajo varnostnega dovoljenja organizaciji. Z ogledom se preveri ali postopki in ukrepi tehničnega in fizičnega varovanja ter organizacija varovanja zagotavljajo ustrezno raven varovanja tajnih podatkov glede na vrsto, količino in oceno ogroženosti tajnih podatkov. Pri ocenjevanju ustreznosti varovanja varnostnega območja je treba upoštevati kombinacijo postopkov in ukrepov tehničnega in fizičnega varovanja ter organizacijo varovanja, ki mora biti določena v načrtu varovanja, načrt pa mora biti izdelan pred ogledom. V primeru vzpostavitve upravnega območja v organih ogled ni potreben.

(3) Organ ali organizacija mora pred določitvijo varnostnega območja pridobiti mnenje nacionalnega varnostnega organa o ustreznosti varnostnotehnične opreme, vgrajene v varnostno območje, ter postopkov in ukrepov varovanja varnostnega območja. Nacionalni varnostni organ izda mnenje na podlagi predhodno opravljenega ogleda, ki ga opravi v ta namen.

25. člen
(označevanje varnostnih in upravnih območij)

(1) Oseba, ki bo vstopila v varnostno območje, mora biti o tem nedvoumno in jasno obveščena, še preden vstopi v to območje.

(2) Obvestilo iz prejšnjega odstavka mora vsebovati dobro vidne napise: »naziv organa – VARNOSTNO OBMOČJE – II. oziroma I. stopnje«, ki so jim lahko dodana še druga obvestila, povezana z varnostnimi postopki in ukrepi, ki se izvajajo v varnostnem območju.

(3) Za označitev upravnega območja ni potrebno posebno obvestilo iz prvega odstavka tega člena, ampak zadošča, da je območje oziroma stavba ali okoliš, v katerem je območje, označena s tablami o imenu organa ter obvestilo o nadzoru vstopa in gibanja, če se ta izvaja.

(4) Izjemoma, kadar to zahteva izvajanje nalog organa, lahko predstojnik organa v sklepu o določitvi varnostnega območja določi, da se varnostno območje ne označi

z obvestilom iz drugega odstavka tega člena ali da se označi na način, ki javnosti ne razkriva, da je to objekt organa.

(5) Vzorec napisov iz drugega odstavka tega člena je razviden iz Priloge 3, ki je sestavni del te uredbe.

26. člen
(nadzor vhoda in izhoda)

(1) Samostojen vstop pooblaščenih oseb v varnostno območje se nadzira z ugotavljanjem identitete vstopajoče osebe. Fizični ali video nadzor vstopa v varnostna območja je lahko dopolnjen s sistemom samodejne kontrole vstopa, ki temelji na identifikaciji z uporabo elektronskih identifikacijskih kartic in prepoznave biometričnih značilnosti vstopajoče osebe. Biometrična prepoznava je lahko dopolnjena ali nadomeščena z uporabo unikatne osebne identifikacijske številke.

(2) Nadzor vstopa zaposlenega osebja v upravna območja temelji na sistemu fizične ali samodejne kontrole vstopa.

(3) Pred vstopom drugih oseb v varnostno in upravno območje mora oseba, ki nadzira vstop v varnostno in upravno območje, preveriti njihovo identiteto in namen obiska ter izpolnjevanje drugih pogojev za vstop v varnostno območje.

(4) V načrtu varovanja varnostnega območja morajo biti predvideni ukrepi in postopki poostrenega nadzora ter omejitev vstopa in gibanja v varnostnem in upravnem območju, kadar to narekuje ocena ogroženosti ali spremenjene varnostne razmere.

(5) V prostore, ki so posebej namenjeni za poslovanje s strankami, lahko obiskovalci in druge osebe (stranke) vstopajo in izstopajo ob navzočnosti v organu zaposlenih oseb brez preverjanja identitete.

27. člen
(varovanje opreme)

(1) Varnostnotehnična oprema, ki je nameščena v upravnih in varnostnih območjih, mora biti zavarovana tako, da je ne morejo uporabljati nepooblaščene osebe.

(2) Pri vzdrževanju in servisiranju opreme, ki se uporablja za varovanje tajnih podatkov je treba preprečiti iznos tajnih podatkov (npr. tistih, ki bi lahko ostali zapisani v iznesenih gradnikih vzdrževane opreme).

28. člen
(varovanje ključnih sestavin sistema)

(1) Vse ključne sestavine sistema, s katerimi se obravnavajo tajni podatki v nešifrirani obliki (razen pri prenosu tajnih podatkov po optičnih povezavah v upravnem območju), morajo biti, glede na stopnjo tajnosti v tem sistemu varovanih tajnih podatkov, postavljene v upravno ali varnostno območje.

(2) Ne glede na prejšnji odstavek se ključne sestavine sistema lahko nameščajo zunaj varnostnega ali upravnega območja, pod pogoji določenimi v 15. členu te uredbe.

29. člen
(varovanje tajnih podatkov v sistemih)

(1) Sistem namenjen varovanju tajnih podatkov, se ne glede na izvedbo in njegove komponente obravnava kot en elektronski nosilec podatkov. Dostop do tega nosilca je možen z različnih lokacij.

(2) Pri dostopu do tajnih podatkov mora biti uporabnik nedvoumno opozorjen o najvišji stopnji tajnosti podatkov, ki se varujejo v sistemu.

(3) Elektronski nosilec podatkov, na katerih se opravi iznos tajnih podatkov, se obravnava kot vsi ostali nosilci s tajnimi podatki. Elektronski nosilec podatkov, na katerih so tajni podatki šifrirani s kriptografsko rešitvijo, ki ima potrdilo o varnostni ustreznosti, se obravnavajo v skladu z minimalnimi varnostnimi zahtevami kriptografske rešitve.

30. člen
(protiprisluškovalni pregled)

(1) Varnostna območja, v katerih se ustno ali drugače zvočno obravnavajo tajni podatki stopnje tajnosti TAJNO ali višje stopnje tajnosti, se morajo zaščititi pred pasivnimi ali aktivnimi poskusi prisluškovanja s protiprisluškovalnimi pregledi. Protiprisluškovalni pregled takih območij se opravi:

- ob določitvi varnostnega območja,
- spremembi zaposlenih v območju, če to zahteva ocena ogroženosti,
- po odločitvi predstojnika ali
- najmanj vsakih 24 mesecev.

(2) V organih in organizacijah iz 1. člena zakona varnostna območja iz prejšnjega odstavka protiprisluškovalno pregleda notranje organizacijska enota Policije.

(3) Ne glede na prejšnji odstavek, protiprisluškovalni pregled varnostnih območij v Ministrstvu za obrambo in drugih organih in organizacijah na obrambnem področju izvedejo notranje organizacijske enote Ministrstva za obrambo, v Slovenski obveščevalno-varnostni agenciji ter organizacijah, ki zanjo izvajajo naročilo, pa notranje organizacijska enota agencije.

31. člen
(omare in blagajne)

(1) V zgornji levi kot omar in blagajn na zunanji strani se glede na stopnjo tajnosti podatkov, ki se hranijo v njej, prilepi nalepka primerne velikosti z velikimi tiskanimi črkami:

- I za stopnjo tajnosti INTERNO;
- Z za stopnjo tajnosti ZAUPNO;
- T za stopnjo tajnosti TAJNO;
- ST za stopnjo tajnosti STROGO TAJNO.

(2) Če se v blagajni hranijo podatki različnih stopenj tajnosti, mora vrsta blagajne ustrezati najvišji stopnji tajnosti podatkov, ki se hranijo v njem, in se s tako stopnjo tajnosti tudi označiti.

32. člen
(nastavitev kombinacij ključavnic za blagajne)

(1) Posamezno nastavitev kombinacije elektronskih ali mehanskih ključavnic za dostop do tajnih podatkov lahko poznajo samo osebe, ki jih določi predstojnik organa ali organizacije oziroma od njega pooblaščena oseba. Predstojnik organa ali organizacije oziroma od njega pooblaščena oseba mora delovne naloge razporediti tako, da je število oseb, ki so seznanjene s posameznimi kombinacijami, čim manjše.

(2) Nastavitve kombinacij elektronskih in mehanskih ključavnic se zamenjajo:

- ob začetku uporabe in po vsakem popravilu,
- ko se zamenja oseba, ki pozna kombinacijo,
- ko pride do dejanskega ali domnevno nepooblaščenega razkritja,
- vsakih 12 mesecev ali
- po odločitvi predstojnika.

V. KOPIRANJE IN PREVAJANJE TAJNIH PODATKOV

33. člen
(kopiranje)

(1) Tajni podatek stopnje tajnosti INTERNO se lahko kopira, razmnožuje, prepisuje (v nadaljnjem besedilu: kopiranje) v upravnem območju. Tajni podatek stopnje tajnosti ZAUPNO ali TAJNO se lahko kopira le v varnostnem območju.

(2) Tajni podatki se lahko kopirajo le na podlagi pisarniške odredbe predstojnika organa ali osebe, ki jo za to pooblasti predstojnik organa.

(3) Naprave za razmnoževanje in izdelavo kopij, ki imajo lastnosti elektronske naprave, morajo izpolnjevati pogoje kot veljajo za naprave za varovanje tajnih podatkov v sistemih.

(4) Iz pisarniške odredbe mora biti razvidno kdo je odobril kopiranje in kdo je prejel kopijo.

(5) Za vsako izdelano kopijo mora biti razvidno kdo je podatke kopiral.

(6) Tajni podatek zveze NATO in EU stopnje tajnosti ZAUPNO ali TAJNO se lahko kopira le v pristojnem registru/podregistru/kontrolni točki, ki je tajni podatke prejel/la, na podlagi pisarniške odredbe predstojnika organa ali osebe, ki jo za to pooblasti predstojnik organa.

(7) Organ, ki je določil podatek za tajnega stopnje tajnosti INTERNO, ZAUPNO ali TAJNO, mora na dokumentu vidno označiti morebitno prepoved kopiranja.

(8) Tajni podatek stopnje tajnosti STROGO TAJNO se ne sme kopirati. Dodatne izvode zapisa tega tajnega podatka sme izdelati le pooblaščena oseba organa, v katerem mu je bila določena stopnja tajnosti. Izjema je tajni podatek zveze NATO stopnje tajnosti STROGO TAJNO, katerega kopiranje lahko odobri pooblaščena oseba v centralnem registru.

34. člen
(prevajanje)

(1) Pred prevodom tajnega podatka stopnje tajnosti STROGO TAJNO je treba pridobiti predhodno soglasje organa, ki je določil podatek za tajnega.

(2) Organ ali organizacija, ki zaradi opravljanja nalog, dokument, ki vsebuje tajne podatke, prevede v drug jezik, mora na prevod napisati vse oznake tajnega podatka in oznako, da gre za prevod.

(3) Izvod prevoda dokumenta se hrani skupaj z dokumentom iz prejšnjega odstavka.

35. člen
(iznos tajnih podatkov iz sistema)

(1) Za vsak iznos tajnega podatka iz sistema je treba voditi ustrezni razvid.

(2) Ne glede na določilo prejšnjega odstavka se varnostna kopija tajnih podatkov, ki je namenjena zagotavljanju neprekinjenega delovanja sistema, ne obravnava kot kopija tajnih podatkov po tej uredbi. Vsi elektronski nosilci varnostnih kopij podatkov sistema morajo biti ustrezno evidentirani in označeni z najvišjo stopnjo tajnosti podatkov, ki se varujejo v sistemu.

(3) V varnostni dokumentaciji sistema, v katerem se obravnavajo tajni podatki ZAUPNO in višje, se opredelijo vsa mesta, kjer je možen iznos tajnega podatka iz sistema. Implementacija sistema mora zagotavljati, da lahko tajne podatke iz sistema iznaša le pooblaščena oseba.

VI. EVIDENTIRANJE

36. člen
(evidentiranje tajnih podatkov v registrskem sistemu)

(1) V okviru registrskega sistema zveze NATO in EU se vzpostavi evidenca tajnih podatkov.

(2) V evidenco iz prejšnjega odstavka se vpisuje naslednje podatke, razen če jih tajni podatek ne vsebuje:

- evidenčna številka;
- datum dokumenta;
- številka dokumenta;
- naslov ali vrsta dokumenta (vabilo, zaprosilo, zapisnik, poročilo…);
- stopnja tajnosti;

- številka kopije;
- datum prejema ali odpreme dokumenta;
- naslovnik (v primeru odpreme dokumenta).

37. člen
(evidentiranje tajnih podatkov)

(1) V evidenco tajnih podatkov se vpisuje naslednje podatke, razen če jih tajni podatek ne vsebuje:

- evidenčna številka;
- datum dokumenta;
- številka dokumenta;
- naslov ali vrsta dokumenta (vabilo, zaprosilo, zapisnik, poročilo…);
- stopnja tajnosti;
- številka kopije;
- subjekt dokumenta (pošiljatelj);
- prejemnik dokumenta (signirni znak) ali naslovnik (v primeru odpreme);
- datum prejema ali odpreme dokumenta.

(2) Pri spremembi ali preklicu stopnje tajnosti mora biti iz evidence razvidno kdaj je bila tajnim podatkom preklicana ali spremenjena stopnja tajnosti.

(3) Če niso izpolnjeni pogoji za varovanje tajnih podatkov v sistemu za evidentiranje tajnih podatkov, se dokumentov, ki so označeni s stopnjo tajnosti ne skenira v evidenco tajnih podatkov.

(4) Evidenca iz prvega odstavka tega člena lahko nadomesti evidenco iz prejšnjega člena.

38. člen
(seznam vpogledov)

(1) Vsak organ, ki hrani tajne podatke, označene s stopnjo tajnosti TAJNO ali STROGO TAJNO, vodi seznam vpogledov, iz katerega mora biti razvidno:

- številka dokumenta, datum, stopnja tajnosti in številka izvoda/kopije dokumenta, ki vsebuje tajni podatek;
- ime, priimek in podpis osebe, ki se je seznanila s tajnim podatkom ter datum in čas seznanitve.

(2) Seznam vpogledov se hrani pri vsakem nosilcu zapisa tajnega podatka, označenega s stopnjo tajnosti TAJNO ali STROGO TAJNO.

(3) Vzorec seznama vpogledov v tajni podatek je v Prilogi 4, ki je sestavni del te uredbe.

(4) Ne glede na določbe prejšnjih odstavkov tega člena se seznam vpogledov v tajne podatke stopnje tajnosti TAJNO in STROGO TAJNO v sistemih vodi v obliki računalniškega zapisa dnevniških datotek (log datotek) iz katerih mora biti razvidno:

- uporabniško ime;
- datum in čas seznanitve.

(5) Seznam vpogledov v sistemih se vodijo v elektronskih dnevniških zapisih, katerih vsebine ni možno naknadno spreminjati.

VII. POGOJI ZA DISTRIBUCIJO TAJNIH PODATKOV

39. člen
(izpolnjevanje pogojev)

(1) Tajni podatek se lahko distribuira le na podlagi upoštevanja načela potrebe po seznanitvi z njegovo vsebino in sicer tistim posameznikom, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov in se s tajnimi podatki lahko seznanijo pri opravljanju svoje funkcije ali delovnih nalog.

(2) Če iz naslova ni možno razbrati posameznega prejemnika tajnega podatka, distribucijo tajnega podatka odredi predstojnik organa ali oseba, ki jo za to pisno pooblasti predstojnik organa ali vodja organizacijske enote za delovno področje, ki ga vodi.

(3) Nadaljnjo distribucijo tajnega podatka v organu, lahko odredi tudi naslovnik tajnega podatka.

40. člen
(distribucijski seznam)

(1) Osebe iz drugega in tretjega odstavka prejšnjega člena lahko določijo distribucijski seznam.

(2) Distribucijski seznam se lahko oblikuje za posamezne dokumente ali za dokumente, ki sodijo v skupno vsebinsko področje. Distribucijski seznam oblikovan za posamezen dokument se hrani, skladno z rokom hrambe, tajnega podatka. Distribucijski seznam oblikovan za dokumente, ki sodijo v skupno vsebinsko področje se hrani trajno.

(3) Distribucijski seznam tajnih podatkov zveze NATO in EU, s katerim se določa distribucija centralnih registrov zveze NATO in EU se pripravi na podlagi prejetih predlogov posameznih organov, ki imajo vzpostavljen podregister ali kontrolno točko. Distribucijski seznam centralnih registrov zveze NATO in EU na predlog resornih ministrstev določi Vlada Republike Slovenije (v nadaljnjem besedilu: vlada).

(4) Distribucijski seznam vsebuje vsaj naslednje podatke:

- oznako organa/organizacijske enote/ centralnega registra,
- vsebinsko področje ali številko dokumenta in
- prejemnika/-e tajnih podatkov.

VIII. PRENOS TAJNIH PODATKOV

41. člen
(prenos in pošiljanje tajnih podatkov)

(1) Tajni podatki se prenašajo v dveh ovojnicah. Zunanja ovojnica je iz trdnega in neprosojnega materiala. Na njej morajo biti podatki o naslovniku, pošiljatelju in številka dokumenta. Iz oznak na zunanji ovojnici ne sme biti razvidno, da vsebuje tajni podatek. Notranja ovojnica mora imeti oznako stopnje tajnosti, številko dokumenta, podatke o naslovniku in pošiljatelju ter druge podatke, pomembne za varnost.

(2) Pri prenosu tajnih podatkov stopnje tajnosti ZAUPNO in TAJNO zunaj varnostnega območja lahko zunanjo ovojnico nadomesti zaklenjen ali zapečaten kovček, škatla ali torba.

(3) Pri prenosu tajnih podatkov stopnje tajnosti STROGO TAJNO zunaj varnostnega območja mora biti notranja ovojnica v zaprtem kovčku, škatli ali torbi z zapiranjem na ključ ali šifrirno kombinacijo. Prenos opravita najmanj dve osebi.

(4) Kadar se tajni podatki prenašajo znotraj varnostnega ali upravnega območja, prenos v dveh ovojnicah ni potreben, morajo pa biti zakriti tako, da se prepreči seznanitev z njihovo vsebino.

(5) Vsak organ mora določiti, kje se sprejemajo nosilci tajnih podatkov in kdo jih sprejema. Naslovnik ali oseba, ki je pooblaščena za sprejem nosilcev tajnih podatkov, potrdi njihov prejem z vpisom v dostavno ali kurirsko knjigo.

(6) Osebe, ki prenašajo tajne podatke, morajo biti varnostno preverjene glede na stopnjo tajnosti tajnih podatkov, ki jih prenašajo.

42. člen
(prenos tajnih podatkov na ozemlju RS)

(1) Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo s kurirsko službo, po lastni prenosni mreži, ali priporočeni pošti s povratnico. Tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti pa le s kurirsko službo ali po lastni prenosni mreži. Izjemoma se lahko opravi osebni prenos tajnega podatka do vključno stopnje tajnosti TAJNO, pod pogojem, da ima oseba dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti. Tak osebni prenos odobri predstojnik organa če kurirska služba ni na voljo ali bi uporaba le te imela za posledico zamudo, ki bi imela škodljive posledice za delovanje države, naslovnik pa gradivo nujno potrebuje.

(2) Za prenos tajnih podatkov zveze NATO, stopnje tajnosti ZAUPNO ali višje stopnje tajnosti med organi in organizacijami je pristojna vojaška kurirska služba. Izjemoma se lahko opravi osebni prenos tajnega podatka do vključno stopnje tajnosti ZAUPNO. Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo s kurirsko službo, po lastni prenosni mreži ali priporočeni pošti s povratnico.

(3) Za prenos tajnih podatkov EU, stopnje tajnosti ZAUPNO in višjih stopenj tajnosti med organi in organizacijami je pristojna kurirska služba ministrstva, pristojnega za zunanje zadeve ali v skladu z dogovorom kurirska služba drugega organa. Izjemoma se lahko opravi osebni prenos tajnega podatka do vključno stopnje

tajnosti ZAUPNO. Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo s kurirsko službo ali po priporočeni pošti s povratnico.

43. člen
(mednarodni prenos tajnih podatkov)

(1) Mednarodni prenos tajnih podatkov se opravlja z vojaško ali diplomatsko kurirsko službo. Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo tudi s priporočeno pošto s povratnico ali z osebnim prenosom.

(2) Poleg določb iz 41. člena te uredbe mora biti pošiljka, ki vsebuje tajne podatke stopnje tajnosti TAJNO in STROGO TAJNO zapečatena s pečatom ali na drug način ustrezno označena, da gre za uradno pošiljko.

(3) Pri prenosu tajnih podatkov stopnje tajnosti TAJNO in STROGO TAJNO morajo kurirji imeti kurirski certifikat, s katerim dokazujejo pooblastilo za prenos ter verodostojnost pošiljke. Kurirski certifikat vojaški kurirski službi izda ministrstvo pristojno za obrambo, diplomatski kurirski službi pa ministrstvo pristojno za zunanje zadeve. Obrazec kurirskega certifikata je objavljen na spletni strani nacionalnega varnostnega organa.

(4) Izjemoma je mogoč osebni prenos tajnega podatka do stopnje tajnosti TAJNO, in sicer s kurirskim certifikatom in pod pogojem, da ima oseba dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti. Tak osebni prenos odobri predstojnik organa če diplomatska pošta in vojaška kurirska služba nista na voljo ali bi uporaba teh služb imela za posledico zamudo, ki bi imela škodljive posledice za delovanje države, naslovnik pa gradivo njuno potrebuje.

44. člen
(kurirski prenos)

(1) Kurirji ter osebe, ki v organu opravljajo naloge lastne prenosne mreže (v nadaljevanju: kurirji), in prenašajo tajne podatke stopnje tajnosti ZAUPNO ali višje stopnje tajnosti, morajo biti ustrezno usposobljeni ter seznanjeni s postopki in ukrepi pri varovanju prenosa tajnih podatkov.

(2) Organi morajo za prenose tajnih podatkov stopnje tajnosti TAJNO ali višje stopnje tajnosti zunaj varnostnih območij izdelati načrt poti in varovanja prenosa tajnih podatkov.

(3) Načrt poti in varovanja prenosov tajnih podatkov stopnje tajnosti TAJNO ali višje stopnje tajnosti mora vsebovati tudi postopke in ukrepe ob morebitnem poskusu zlorabe, prometnih in drugih nesrečah, zastojih, postankih, prenočevanju in drugih podobnih dogodkih. V načrtu morajo biti opredeljene glavne in pomožne poti.

45. člen
(usposabljanje kurirjev)

(1) Kurirji se usposobijo po programu, ki je v Prilogi 5, ki je sestavni del te uredbe.

(2) Kurirji, ki prenašajo tajne podatke, najmanj enkrat letno opravijo obnovitveno usposabljanje, po programu, ki mora obsegati skrajšano obliko osnovnega usposabljanja.

(3) Usposabljanji izvajata Ministrstvo za obrambo in Policija, razen usposabljanja kurirjev Slovenske obveščevalno-varnostne agencije, za katerih usposabljanje skrbi ta agencija.

(4) Izvajalci usposabljanj lahko za izvedbo dela programa, ki se nanaša na izvedbo usposabljanja osnov samoobrambe in varne vožnje, sklenejo sporazum s podizvajalci, ki so pravne ali fizične osebe in so registrirane za opravljanje dejavnosti izobraževanja ter izpolnjujejo pogoje glede prostorov in tehnične opremljenosti ter imajo v delovnem ali pogodbenem razmerju za vsako izmed strokovnih področij za katero se sklepa sporazum najmanj enega predavatelja, ki je seznanjen z vsebino in programom usposabljanja.

46. člen
(osebni prenos)

(1) Zaradi izvedbe določene naloge ali kadar je hitrost dostave tajnega podatka bistvenega pomena ter prenos s kurirjem ni možen, se lahko izven upravnega ali varnostnega območja do vključno stopnje tajnosti TAJNO izjemoma opravi osebni prenos tajnega podatka.

(2) Osebni prenos lahko izvede oseba, ki je ustrezno seznanjena s postopki in ukrepi varovanja prenosa tajnih podatkov.

(3) Tajni podatek se prenaša na način, da ni razvidno, da gre za prenos tajnega podatka. Pri prenosu mora biti tajni podatek pod stalnim nadzorom.

(4) Ovojnice v kateri se prenašajo tajni podatki v času prenosa ni dovoljeno odpirati, prav tako tajnih podatkov ni dovoljeno obravnavati na javnih prostorih oziroma na poti.

47. člen
(pooblastilo za prenos)

(1) Osebe, ki prenašajo tajne podatke stopnje tajnosti ZAUPNO ali višje stopnje tajnosti, morajo imeti pooblastilo predstojnika organa za prenos tajnih podatkov.

(2) Vsebina pooblastila za kurirski prenos je določena z obrazcem OBR-KU, ki je v Prilogi 6, ki je sestavni del te uredbe.

(3) Vsebina pooblastila za osebni prenos je določena z obrazcem OBR-OP, ki je v Prilogi 7, ki je sestavni del te uredbe.

48. člen
(pomoč drugih organov)

(1) Pooblaščene uradne osebe morajo osebi, ki prenaša tajne podatke in se izkaže z veljavnim pooblastilom, na njegovo zaprosilo zagotoviti pomoč v obliki in obsegu,

ki omogoča varovanje tajnih podatkov pred odtujitvijo, poškodovanjem ali uničenjem.

(2) Pooblaščene uradne osebe pri postopkih, ki jih izvajajo v skladu s svojimi pooblastili, nimajo pravice vpogleda v vsebino tajnih podatkov.

49. člen
(prenos tajnih podatkov v sistemih)

(1) Prenos tajnih podatkov po sistemih zunaj upravnih in varnostnih območij je dovoljen le z uporabo kriptografskih rešitev, ki imajo potrdilo o varnostni ustreznosti.

(2) Prenos tajnih podatkov stopnje tajnosti ZAUPNO ali višjih stopenj tajnosti je znotraj upravnega in varnostnega območja dovoljen po optičnih povezavah. Morebitno odstopanje odobri organ pristojen za izvajanje zaščite proti neželenemu elektromagnetnemu sevanju na osnovi določil Navodila o izvajanju zaščite pred neželenim elektronskim sevanjem v sistemih, v katerih se obravnavajo tajni podatki, ki je v Prilogi 13, ki je sestavni del te uredbe.

IX. UNIČENJE TAJNIH PODATKOV

50. člen
(uničenje tajnih podatkov)

(1) Tajni podatki se morajo uničiti na način, s katerim se zagotovi, da postane tajni podatek nerazpoznaven in neobnovljiv.

(2) V primeru, da se za uničevanje tajnih podatkov stopnje tajnosti INTERNO in ZAUPNO v papirni obliki uporablja rezalnik papirja, se uporabi rezalnik, ki zagotavlja razrez papirja velikosti največ 10 mm^2. Za uničevanje tajnih podatkov stopnje tajnosti TAJNO in STROGO TAJNO v papirni obliki se uporablja rezalnik papirja, ki zagotavlja razrez papirja velikosti največ 5 mm^2.

(3) Organizacije tajne podatke, z izjemo tajnih podatkov tuje države, uničijo, skladno z določbami te uredbe. V kolikor upravičeno ne morejo zagotoviti ustreznih pogojev za uničevanje tajnih podatkov, tajne podatke vrnejo pošiljatelju.

(4) Organizacija tajni podatek tuje države, namenjen uničenju, vrne pošiljatelju, ki poskrbi za ustrezno uničenje tajnega podatka.

(5) Kopije in dodatni izvodi dokumentov, ki vsebujejo tajne podatke in niso del zadeve organa, ter kopije dokumentov na nosilcih, ki so namenjene izključno prenosu tajnih podatkov se izločijo in uničijo takoj po opravljeni delovni nalogi, za katero so bili izdelani oziroma najkasneje ob predaji dokumentov v tekočo zbirko.

(6) Tajni podatki, se hranijo skladno z roki, določenimi s predpisi, ki urejajo poslovanje z dokumentarnim gradivom. Po preteku roka hrambe se izločijo in uničijo.

(7) Tajni podatki se izločajo in uničujejo komisijsko. Komisijo imenuje predstojnik organa ali oseba, ki jo predstojnik organa za to pooblasti. Komisijo sestavljajo

najmanj tri osebe, med katerimi mora biti oseba, odgovorna za varovanje tajnih podatkov. O uničenju tajnih podatkov komisija pripravi zapisnik. Zapisnik se hrani trajno.

(8) O uničenju tajnih podatkov stopnje tajnosti STROGO TAJNO se pisno obvesti organ, ki je določil stopnjo tajnosti.

(9) Seznam vpogledov iz 38. člena se priloži zapisniku o uničenju tajnega podatka.

(10) V primeru, da je oprema sistema, v katerem so se obravnavali tajni podatki stopnje tajnosti INTERNO, namenjena drugačni ali ponovni uporabi, je treba vse elektronske nosilce podatkov obdelati s postopkom varnega brisanja/prepisovanja ali fizično uničiti, ki je opredeljen v Prilogi 8, ki je sestavni del te uredbe. Za opremo sistema v katerem so se obravnavali tajni podatki stopnje tajnosti ZAUPNO ali višje, ponovna uporaba v druge namene ni možna.

(11) Uničenje tajnih podatkov v sistemih se izvaja s fizičnim uničenjem elektronskih nosilcev podatkov. Postopek (način) fizičnega uničenja elektronskih nosilcev podatkov je opredeljen v Prilogi 8 te uredbe.

(12) Po brisanju tajnih podatkov z elektronskega nosilca podatkov, se ta do fizičnega uničenja obravnava v skladu s predpisi o varovanju tajnih podatkov, ki veljajo za stopnjo tajnosti, s katero je označen.

X. VAROVANJE TAJNIH PODATKOV V SISTEMIH

51. člen
(določitev odgovornih oseb sistema)

(1) Predstojnik organa in organizacije imenuje odgovorne osebe:

- skrbnika sistema organa,
- upravljavca sistema,
- vodjo informacijske varnosti sistema in
- skrbnika kriptografskega materiala.

(2) Če sistem deluje tudi na dislociranih lokacijah organa ali v drugih organih, lahko predstojnik dislocirane enote ali drugega organa določi osebo, odgovorno za informacijsko varnost sistema na dislocirani lokaciji organa ali v drugem organu (v nadaljnjem besedilu: lokalni vodja informacijske varnosti sistema). Lokalni vodja informacijske varnosti sistema poroča vodji informacijske varnosti sistema.

(3) Predstojnik o imenovanju ali preklicu imenovanja odgovornih oseb obvesti nacionalni varnostni organ.

(4) Če vodja informacijske varnosti ni imenovan, njegove naloge opravlja predstojnik organa ali organizacije. Na dislocirani enoti sistema v tem primeru njegove naloge opravlja predstojnik dislocirane enote.

52. člen
(skrbnik sistema)

Skrbnik sistema, ki je praviloma poslovni uporabnik tega sistema, je odgovoren za:

- pridobitev, razvoj, integracijo, spreminjanje, delovanje, vzdrževanje, varovanje in prenehanje uporabe sistema ter varovanje podatkov, ki jih sistem obravnava,
- izvedbo postopka varnostne odobritve sistema,
- pripravo varnostne dokumentacije,
- določitev varnostnega načina delovanja sistema,
- vzpostavitev postopkov identifikacije in overitve dostopa uporabnikov do sistema,
- obvladovanje varnostih tveganj in obvladovanje preostalih varnostnih tveganj,
- sprotno izvajanje nadzora pravilnega delovanja sistema in
- spremljanje vseh posegov v sistem.

53. člen
(upravljavec sistema)

(1) Upravljavec sistema je zadolžen za:

- nameščanje, vzdrževanje, konfiguriranje, integracijo, administriranje in zagotavljanje delovanja in razpoložljivosti sistema,
- uvedbo in upravljanje varnostnih nadzorstev in varovanje sistema,
- spremljanje varovanja tajnih podatkov sistema,
- poročanje vodji informacijske varnosti sistema o dogodkih in incidentih pri varovanju tajnih podatkov v sistemu in
- druge naloge operativnega upravljanja sistema.

(2) Upravljavec sistema izvaja svoje naloge v skladu z navodili skrbnika sistema.

54. člen
(vodja informacijske varnosti sistema)

Vodja informacijske varnosti sistema je odgovoren za:

- upravljanje in nadzor nad ukrepi in postopki varovanja tajnih podatkov v sistemih,
- obravnavo informacijskega varnostnega dogodka v sistemih in poročanje vodji informacijske varnosti organa, skrbniku sistema in nacionalnemu varnostnemu organu in
- sodelovanje pri usklajevanju poslovnih in varnostnih ciljev organa ali organizacije.

55. člen
(skrbnik kriptografskega materiala)

Skrbnik kriptografskega materiala je odgovoren za upravljanje s kriptografskim materialom skladno s sklepom o varovanju kriptografskega materiala, ki ga na predlog nacionalnega varnostnega organa sprejme vlada.

56. člen
(organi za razdeljevanje kriptografskega materiala)

(1) Naloge krovnega organa za razdeljevanje kriptografskega materiala za nacionalne potrebe in povezavo z EU izvaja nacionalni varnostni organ .

(2) Za naloge krovnega organa za razdeljevanje kriptografskega materiala za zagotavljanje varovanja tajnih podatkov v sistemih, ki se uporabljajo za obrambne potrebe in povezavo teh sistemov z mednarodnimi obrambnimi in vojaškimi organizacijami v skladu z mednarodnimi pogodbami, je pristojno Ministrstvo za obrambo.

(3) Za naloge krovnega organa za razdeljevanje kriptografskega materiala za zagotavljanje varovanja tajnih podatkov v sistemih, ki se uporabljajo za obveščevalne in varnostne potrebe in povezavo teh sistemov z mednarodnimi obveščevalnimi in varnostnimi organizacijami v skladu z mednarodnimi pogodbami in sporazumi, je pristojna Slovenska obveščevalno-varnostna agencija.

(4) Koordinacijo med krovnimi organi za razdeljevanje kriptografskega materiala izvaja nacionalni varnostni organ.

(5) Naloge krovnih organov za razdeljevanje kriptografskega materiala se določijo s sklepom o varovanju kriptografskega materiala, ki ga na predlog nacionalnega varnostnega organa sprejme vlada.

57. člen
(določitev varnostnega načina delovanja sistema)

(1) Za vsak sistem je potrebno pisno opredeliti varnostni način delovanja.

(2) Posamezen sistem lahko deluje:

- neselektivno;
- selektivno;
- dvojno selektivno.

(3) V sistemu z neselektivnim varnostnim načinom delovanja morajo imeti vse osebe, ki dostopajo v sistem, dovoljenje za dostop do tajnih podatkov za najvišjo stopnjo tajnosti podatkov, obravnavanih v sistemu, ter neselektivni dostop do vseh v sistemu obravnavanih podatkov na podlagi enotne potrebe po seznanitvi.

(4) V sistemu s selektivnim varnostnim načinom delovanja morajo imeti vse osebe, ki dostopajo v sistem, dovoljenje za dostop do tajnih podatkov za najvišjo stopnjo tajnosti podatkov, obravnavanih v sistemu, vendar imajo te osebe selektivni dostop do podatkov, obravnavanih v sistemu, na podlagi različnih pravic po vedenju.

(5) V sistem z dvojno selektivnim varnostnim načinom delovanja lahko selektivno dostopajo osebe, ki imajo dovoljenje za dostop do tajnih podatkov za različne stopnje tajnosti, ter imajo hkrati selektivni dostop do v sistemu obravnavanih podatkov na podlagi različnih pravic po vedenju.

(6) V primeru, da se v sistemu obravnavajo tudi podatki brez stopnje tajnosti, do katerih lahko dostopajo osebe brez dovoljenja za dostop do tajnih podatkov se smiselno uporablja prejšnji odstavek.

(7) Selektivni dostop v sistem in selektivni dostop do podatkov se rešujeta s pomočjo strojne in programske opreme.

58. člen
(identifikacija in overitev dostopa uporabnikov v sistem)

V sistemu je treba vzpostaviti postopke identifikacije in overitve dostopa za vse uporabnike sistema. Vsak uporabnik mora biti seznanjen s postopki dodeljevanja in uporabe sistema za identifikacijo in overitev dostopa uporabnikov v sistem. Za dostop uporabnikov v sistem se uporablja overitev z uporabniškim imenom in geslom ali drugimi overitvenimi metodami (PIN koda, prstni odtis …).

59. člen
(selekcija dostopa uporabnikov do podatkov)

Uporabniku sistema se dostop omeji le na tiste tajne podatke, ki jih potrebuje za opravljanje svojih nalog ali funkcij in do katerih je upravičen na podlagi pooblastila, določenega z zakonom ali predpisom, izdanim na podlagi zakona. Skrbnik sistema vzpostavi in vzdržuje seznam uporabnikov sistema, iz katerega so za vsakega uporabnika sistema razvidni njegovi identifikacijski podatki in njegove pravice dostopa. (v nadaljnjem besedilu: varnostna shema). Ob spremembi pravic posameznega uporabnika (na primer: prekinitev delovnega razmerja, premestitev in podobno) mora biti varnostna shema ustrezno popravljena in sprememba ustrezno dokumentirana.

60. člen
(spremljanje in nadzor pristopa v sistem in dostopa do tajnih podatkov)

(1) Spremljanje in nadzor dostopa do sistema in tajnih podatkov v njem mora omogočiti ugotavljanje, kdo, kdaj in od kod je dostopal, čas dela v sistemu, kateri tajni podatki so bili obravnavani, in sicer tako, da je mogoče ukrepati ob sumu nepooblaščenega vstopa v sistem, nepooblaščenega dostopa do tajnih podatkov ali zlorabe tajnih podatkov v sistemu ter pozneje rekonstruirati posamezne dostope do tajnih podatkov v sistemu.

(2) Za vsak sistem se pisno določi način nadzora in spremljanja vseh izvedbenih in kontrolnih posegov v sistem ter pooblaščene izvajalce teh posegov. Vsi posegi v sistem morajo biti dokumentirani. Dokumentiranje zajema podatke o naročniku in vzroku posega, vrsto in rezultate posega, čas in datum ter podatke o izvajalcu posega.

(3) Uporabnik mora biti pri dostopu do tajnih podatkov, v sistemu kjer se varujejo tajni podatki, o tem nedvoumno opozorjen.

(4) Zapise o posegih v sistem se morajo hraniti dokler se sistem uporablja za varovanje tajnih podatkov.

(5) Vsak dostop do tajnega podatka tajnosti ZAUPNO ali višje v sistemu mora biti zabeležen (revizijska sled). Čas hrambe dnevnikov dogodkov se določi na podlagi drugih predpisov, ki urejajo področje ravnanja z dokumentarnim gradivom in to uredbo. Če ni drugače določeno, se ti podatki hranijo dve leti.

61. člen
(povezovanje sistemov)

(1) Povezovanje sistemov je dovoljeno le po nadzorovanih in varovanih vstopno-izstopnih točkah, skozi katere potekajo vsi servisi in storitve.

(2) Pred povezovanjem sistemov je treba pridobiti soglasje skrbnikov posameznega sistema.

(3) Povezovanje sistemov mora biti izvedeno skladno z Navodilom za povezovanje komunikacijsko informacijskih sistemov, ki je v Prilogi 9, ki je sestavni del te uredbe.

XI. VARNOSTNO VREDNOTENJE SISTEMOV

62. člen
(varnostno vrednotenje sistema)

(1) Nacionalni varnostni organ varnostno vrednotenje sistema opravi na podlagi pregleda in ocene varnostne dokumentacije ter varnostnega vrednotenja sistema na lokaciji organa ali organizacije, s katerim preveri izpolnjevanje ukrepov in postopkov za zagotovitev varnega delovanja sistema v skladu s to uredbo in drugimi zakonskimi in podzakonskimi predpisi iz področja varovanja tajnih podatkov.

(2) Postopek varnostnega vrednotenja sistema se začne z vlogo organa ali organizacije za izvedbo varnostnega vrednotenja ali ponovnega varnostnega vrednotenja sistema. Vloga mora vsebovati podatke o sistemu in najvišji stopnji tajnosti tajnih podatkov, ki se varujejo v sistemu. Priloga vloge je varnostna dokumentacija, katere sestavni del so dokumenti opredeljeni v Prilogi 10, Prilogi 11 in Prilogi 12, ki so sestavni del te uredbe.

(3) Postopek varnostnega vrednotenja sistema sestavljajo:

- pregled in ocena varnostne dokumentacije,
- varnostno vrednotenje sistema na lokaciji organa ali organizacije in
- izdaja varnostnega dovoljenja.

63. člen
(varnostno vrednotenje sistemov tujih držav ali mednarodnih organizacij)

(1) Nacionalni varnostni organ postopke in varnostno vrednotenje sistemov tujih držav ali mednarodnih organizacij, v katerih se obravnavajo tajni podatki opravi v skladu s prejšnjim členom.

(2) Po končanem postopku varnostnega vrednotenja sistema nacionalni varnostni organ izda izjavo o skladnosti, ki jo posreduje pristojnemu organu tuje države ali mednarodne organizacije.

64. člen

(dokumenti, potrebni za izvedbo varnostnega vrednotenja sistema)

(1) V postopku varnostnega vrednotenja sistema in izdaje varnostnega dovoljenja se izdela varnostna dokumentacija, v kateri se opiše sistem, definirajo varnostne zahteve, ocenijo varnostna tveganja sistema, določijo varnostni ukrepi za njegovo zaščito ter določijo odgovornosti oseb, ki so zadolženi za varno delovanje sistema.

(2) Varnostno dokumentacijo sestavljajo:

- načrt varovanja sistema,
- ocena varnostnih tveganj in
- varnostna navodila za delo.

(3) V postopku varnostnega vrednotenja sistema je treba nacionalnemu varnostnemu organu posredovati ali dati na vpogled tudi drugo relevantno dokumentacijo (poročilo o izvedenih meritvah zaščite prostorov pred neželenim elektromagnetnim sevanjem, potrdilo o varnostni ustreznosti kriptografske rešitve, potrdila o zaščiti sestavin sistema pred neželenim elektromagnetnim sevanjem).

(4) Varnostna dokumentacija iz drugega odstavka tega člena se za sisteme, v katerih se varujejo tajni podatki stopnje tajnosti ZAUPNO ali višje, minimalno označi s stopnjo tajnosti INTERNO. Varnostna navodila za delo so lahko brez stopnje tajnosti.

(5) Ne glede na določbo iz drugega odstavka tega člena, se za sistem, v katerem se varujejo tajni podatki stopnje tajnosti INTERNO, ki deluje v lokalnem omrežju in ni povezan z internetom, izdela samo dokumentacija varnostna navodila za delo v sistemu in je opredeljena v prilogi 14, ki je sestavni del te uredbe.

65. člen
(načrt varovanja sistema)

(1) Načrt varovanja sistema vsebuje opis sistema, načrt sestavin in povezav sistema, varnostne zahteve sistema, varnostna okolja, varnostne protiukrepe in varnostno upravljanje sistema.

(2) Načrt varovanja sistema se izdela v začetni fazi načrtovanja in izgradnje sistema in se vodi ter dopolnjuje dokler se sistem uporablja za varovanje tajnih podatkov.

66. člen
(ocena varnostnih tveganj)

(1) Obvladovanje varnostnih tveganj zajema prepoznavanje in oceno tveganj in njihovih posledic, načrtovanja ukrepov in odgovornosti za varnostna tveganja ter spremljanje in poročanje o obvladovanju varnostnih tveganj.

(2) Za ocenjevanje in obvladovanje varnostnih tveganj se glede na potrebe organa ali organizacije uporabi metodologijo, ki je opredeljena v Prilogi 10, Prilogi 11 in Prilogi 12 te uredbe.

(3) Preostala varnostna tveganja, ki jih ni mogoče odpraviti ali zmanjšati po izvedbi vseh varnostnih ukrepov v sistemu, mora organ ali organizacija spremljati in

upravljati skozi celoten življenjski cikel sistema (grožnje in ranljivost sistema, varnostne nastavitve sistema, vpliv sprememb sistema na varnost, skladnost z varnostnimi zahtevami).

(4) Varnost oskrbovalnih verig na področju varnosti sistemov, vključno z nabavo informacijskih sistemov in njihovih komponent, mora biti dosledno upravljana.

(5) Seznam groženj in ranljivosti sistema vodi nacionalni varnostni organ v sodelovanju z organom, pristojnim za kibernetsko varnost.

67. člen
(varnostna navodila za delo v sistemu)

(1) Z varnostnimi navodili za delo v sistemu se določijo varnostno upravljanje in organiziranost varnosti sistema, načrtovanje ukrepov ob nepredvidenih dogodkih, upravljanje in spreminjanje konfiguracije/nastavitev sistema.

(2) Varnostna navodila za delo se pripravijo za uporabnike in upravljavce sistema.

68. člen
(varnostno vrednotenje sistema na lokaciji)

(1) Nacionalni varnostni organ opravi varnostno vrednotenje sistema na organu ali organizaciji, s katerim preveri izpolnjevanje vseh ukrepov in postopkov za zagotovitev varnega delovanja sistema v skladu s predloženo varnostno dokumentacijo in zakonskimi ter podzakonskimi predpisi s področja varovanja tajnih podatkov in drugimi relevantnimi zakonskimi in podzakonskimi predpisi.

(2) V okviru varnostnega vrednotenja se opravi varnostni pregled sistema, s katerim se preveri implementacija konkretnih fizičnih, organizacijskih in tehničnih ukrepov navedenih v načrtu varovanja sistema

(3) Varnostno vrednotenje se opravi ob navzočnosti vodje informacijske varnosti sistema in vodje informacijske varnosti organa ali organizacije in drugih oseb, odgovornih za varnost sistema (skrbnik sistema, upravljavec sistema, skrbnik kriptografskega materiala itd.).

69. člen
(ponovni postopek varnostne odobritve)

(1) Varnostna dokumentacija se vodi in dopolnjuje skozi celotni življenjski cikel sistema in jo je treba stalno dopolnjevati. V postopku ponovne varnostne odobritve sistema oziroma najmanj enkrat letno je treba pregledati ustreznost vseh ukrepov in postopkov, ki so z njo določeni.

(2) Ponovni postopek varnostne odobritve se izvede ob vsaki spremembi sistema, ki ima ali bi imela posledice za varnost v sistemu obravnavanih tajnih podatkov. Upravljavec ali skrbnik sistema sporoči nacionalnemu varnostnemu organu spremembo in posreduje vlogo za ponovni postopek pridobitve varnostnega dovoljenja za delovanje sistema.

(3) Ob ugotovitvi upravljavca, skrbnika sistema ali nacionalnega varnostnega organa, da sistem več ne izpolnjuje minimalnih pogojev za varnostno delovanje sistema, je treba ponovno izvesti postopek varnostnega vrednotenja sistema.

XII. NEŽELENO ELEKTROMAGNETNO SEVANJE

70. člen
(izvajanje zaščite proti neželenemu elektromagnetnemu sevanju)

(1) Vse sestavine sistemov, v okviru katerih se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje, morajo biti zaščitene proti neželenemu elektromagnetnemu sevanju. Skrbnik sistema hrani potrdila s katerimi dokazuje ustreznost zaščite sestavin sistema proti neželenemu elektromagnetnem sevanju.

(2) Ukrepi za zaščito morajo zajemati izbor in način namestitve vseh sestavin sistemov glede na stopnjo tajnosti podatkov v sistemu in na stopnjo ogroženosti prostorov, kjer so ali bodo nameščene, skladno z Navodilom o izvajanju zaščite pred neželenim elektromagnetnim sevanjem v sistemih, v katerih se obravnavajo tajni podatki, ki je v Prilogi 13 te uredbe.

(3) Ukrepe za zaščito proti neželenemu elektromagnetnemu sevanju zagotovijo skrbniki sistemov, v katerih se obravnavajo tajni podatki. Poročilo o meritvah in/ali ugotovitvah ter ukrepih so del načrta varovanja sistema.

(4) Meritve neželenega elektromagnetnega sevanja opravljajo Ministrstvo za obrambo, Policija, Slovenska obveščevalno varnostna agencija ali drugi organ, ki ga pooblasti nacionalni varnostni organ.

(5) Stopnjo ogroženosti prostorov določijo organi, navedeni v prejšnjem odstavku.

XIII. KRIPTOGRAFIJA

71. člen
(razvoj, uporaba in veljavnost kriptografskih rešitev)

(1) Razvoj in nadgradnja kriptografskih rešitev se izvaja na podlagi pobud državnih organov.

(2) Nacionalni varnostni organ sodeluje z drugimi državnimi organi in zunanjimi izvajalci pri razvoju in nadgradnjah kriptografskih rešitev, ki so namenjene varovanju tajnih podatkov.

(3) Za varovanje tajnih podatkov v sistemih je dovoljeno uporabljati kriptografske rešitve za katere je bilo izdano potrdilo o varnostni ustreznosti. Izjemoma se lahko kriptografske rešitve, za katere je bilo izdano potrdilo o varnostni ustreznosti, uporabljajo tudi v druge namene, vendar je predhodno treba pridobiti soglasje nacionalnega varnostnega organa. Nacionalni varnostni organ periodično preverja varnostno ustreznost kriptografskih rešitev in sicer kriptografske rešitve za varovanje tajnih podatkov stopnje tajnosti STROGO TAJNO in TAJNO na eno leto,

kriptografske rešitve namenjene varovanju tajnih podatkov stopnje tajnosti ZAUPNO na tri leta in kriptografske rešitve namenjene varovanju tajnih podatkov stopnje tajnosti INTERNO na pet let.

(4) Varnostna ustreznost se lahko preveri tudi pred iztekom obdobij iz prejšnjega odstavka.

72. člen
(klasifikacija kriptografskih algoritmov)

(1) Nacionalni varnosti organ klasificira kriptografske algoritme glede na izvor in javno dostopnost v dve skupini.

(2) Kriptografski algoritmi I. nivoja so razviti pod nadzorom nacionalnega varnostnega organa, so v celoti ali deloma tajni podatki, dostop do njih pa se izvaja izključno na podlagi potrebe po vedenju. Kriptografski algoritmi I. nivoja so tudi algoritmi, ki so pridobljeni na podlagi mednarodnih sporazumov in se uporabljajo za varovanje tajnih podatkov stopnje tajnosti TAJNO ali STROGO TAJNO.

(3) Kriptografski algoritmi II. nivoja so lahko razviti pod nadzorom nacionalnega varnostnega organa ali pa so privzeti iz javno dostopnih podatkov.

73. člen
(potrdilo o varnostni ustreznosti kriptografske rešitve)

(1) Potrdilo o varnostni ustreznosti kriptografske rešitve izda nacionalni varnostni organ ali drug z zakonom določen organ, če v postopku ugotavljanja ustreznosti predlagane kriptografske rešitve za varovanje tajnih podatkov ni ugotovljenih varnostnih zadržkov. Vzorec potrdila je v Prilogi 15, ki je sestavni del te uredbe.

(2) Uporaba varnostno ustreznih kriptografskih rešitev je dovoljena samo z upoštevanjem predpisanih minimalnih varnostnih zahtev za označevanje, distribucijo in uporabo.

(3) Pri pripravi minimalnih varnostnih zahtev nacionalni varnostni organ sodeluje s predlagateljem postopka ugotavljanja ustreznosti kriptografske rešitve za varovanje tajnih podatkov.

74. člen
(začetek postopka ugotavljanja ustreznosti kriptografske rešitve)

(1) Organi, ki začnejo postopek ugotavljanja ustreznosti kriptografske rešitve za varovanje tajnih podatkov v skladu z 39.a členom zakona podajo vlogo na predpisanem obrazcu. Vsebina vloge je v Prilogi 16, ki je sestavni del te uredbe. Vlogo predlagatelj označi s stopnjo tajnosti, ki je enaka stopnji tajnosti tajnih podatkov, ki se bodo obravnavali s predlagano kriptografsko rešitvijo.

(2) Sestavna dela vloge iz prejšnjega odstavka sta:

- ustrezno število kosov predlagane kriptografske rešitve za namen ugotavljanja varnostne ustreznosti in

- dokumentacija o predlagani kriptografski rešitvi, ki se označi z enako stopnjo tajnosti kot je stopnja tajnosti tajnih podatkov, ki se bodo obravnavali s predlagano kriptografsko rešitvijo.

(3) Vsebina dokumentacije je predpisana v Prilogi 17, ki je sestavni del te uredbe.

(4) Pri ugotavljanju ustreznosti kriptografskih rešitev v sistemih, ki obravnavajo tajne podatke stopnje tajnosti ZAUPNO ali višjih stopenj tajnosti je obvezni del dokumentacije k vlogi iz prejšnjega odstavka:

- izvorna koda kriptografske rešitve;
- opis uporabljenih strojnih in programskih komponent;
- opis razvojnega okolja in procesov;
- opis dobavne verige.

75. člen
(priznavanje potrdil o varnostni ustreznosti kriptografskih rešitev tujih držav in mednarodnih organizacij)

(1) Nacionalni varnostni organ lahko prizna potrdilo o varnostni ustreznosti kriptografske rešitve drugega nacionalnega organa za komunikacijsko varnost države članice EU, zveze NATO ali mednarodnih organizacij, katerih članica je Republika Slovenija in izda enakovredno potrdilo o varnostni ustreznosti za uporabo teh rešitev v sistemih Republike Slovenije.

(2) Za kriptografske rešitve iz prejšnjega odstavka se lahko pridobi potrdilo o varnostni ustreznosti brez izvedbe postopka ugotavljanja ustreznosti kriptografskih rešitev, če se bodo uporabile v sistemih, ki obravnavajo tajne podatke stopnje tajnosti INTERNO.

(3) Kriptografske rešitve iz prvega odstavka tega člena, namenjene uporabi v sistemih, ki obravnavajo tajne podatke stopnje tajnosti ZAUPNO ali višje, pridobijo potrdilo o varnostni ustreznosti z izvedbo postopka ugotavljanja ustreznosti kriptografskih rešitev.

(4) V sistemih, ki obravnavajo tajne podatke stopnje tajnosti TAJNO, izključno tujih kriptografskih rešitev ni dovoljeno uporabljati.

(5) Tujo kriptografsko rešitev se v sistemih, ki obravnavajo tajne podatke stopnje tajnosti TAJNO, izjemoma lahko uporabi, če nacionalna kriptografska rešitev ne obstaja in ima tuja kriptografska rešitev potrdilo o varnostni ustreznosti za varovanje tajnih podatkov zveze EU ali zveze NATO najmanj stopnje tajnosti enakovredne stopnji tajnosti TAJNO.

(6) V sistemih, ki obravnavajo tajne podatke stopnje tajnosti STROGO TAJNO se sme uporabljati samo kriptografske rešitve v celoti razvite v Republiki Sloveniji.

76. člen
(postopek ugotavljanja ustreznosti kriptografskih rešitev)

(1) Nacionalni varnostni organ v sodelovanju s predlagateljem in s proizvajalcem pripravi načrt izvedbe postopka ugotavljanja ustreznosti predlagane kriptografske rešitve za varovanje tajnih podatkov.

(2) V postopku ugotavljanja varnostne ustreznosti kriptografskih rešitev nacionalni varnostni organ preveri stopnjo varnosti arhitekture, stopnjo varnosti posameznih kriptografskih prvin in izvedbo le-teh v kriptografskih rešitvah.

(3) Pri ugotavljanju varnostne ustreznosti kriptografskih rešitev v sistemih, ki obravnavajo tajne podatke stopnje tajnosti INTERNO, nacionalni varnostni organ pregleda zahtevano dokumentacijo in opravi funkcionalni preizkus delovanja kriptografske rešitve.

(4) Pri ugotavljanju varnostne ustreznosti kriptografskih rešitev v sistemih, ki obravnavajo tajne podatke stopnje tajnosti ZAUPNO, nacionalni varnostni organ poleg postopkov iz prejšnjega odstavka, izvede še funkcionalni preizkus pravilnosti implementacije in uporabe posameznih kriptografskih prvin v tej kriptografski rešitvi.

(5) Pri ugotavljanju varnostne ustreznosti kriptografskih rešitev v sistemih, ki obravnavajo tajne podatke stopnje tajnosti TAJNO ali STROGO TAJNO, nacionalni varnostni organ poleg postopkov iz prejšnjega odstavka, izvede še analizo možnosti kompromitiranja varnostno pomembnih gradnikov, ki vključuje preizkuse vdorov.

(6) Postopek ugotavljanja varnostne ustreznosti se lahko uporablja tudi za druge sestavine sistema, ki so ključne za varovanje tajnih podatkov in nacionalni varnostni organ oceni, da je ugotavljanje varnostne ustreznosti potrebno. Organi, ki začnejo postopek ugotavljanja varnostne ustreznosti takih rešitev za varovanje tajnih podatkov v skladu z 39.a členom zakona, podajo vlogo na predpisanem obrazcu. Vsebina vloge je v Prilogi 15, te uredbe.

77. člen
(postopek ugotavljanja ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve)

Postopek ugotavljanja varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve se izvede na predlog organa v primeru, da pride do spremembe kriptografske rešitve z veljavnim potrdilom o varnostni ustreznosti. Organi, ki začnejo postopek ugotavljanja varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve za varovanje tajnih podatkov v skladu z 39.a členom zakona, podajo vlogo na predpisanem obrazcu. Vsebina vloge je v Prilogi 15 te uredbe.

78. člen
(programske kriptografske rešitve)

Programske kriptografske rešitve, se kot samostojne rešitve lahko uporabljajo za varovanje tajnih podatkov do vključno stopnje tajnosti ZAUPNO.

79. člen
(splošne varnostne zahteve kriptografskih rešitev)

(1) Proizvajalec mora skrbeti za varnost dobavne verige na način, da se zmanjša verjetnost kompromitacije varnostno pomembnih strojnih in programskih komponent.

(2) Proizvajalec mora skrbeti za varnost razvojnega okolja na način, da sprejme tehnološke in procesne ukrepe za preprečevanje, odkrivanje in odzivanje na varnostne incidente. O zaznanih resnejših incidentih proizvajalec nemudoma poroča nacionalnemu varnostnemu organu.

(3) Proizvajalec mora spremljati strokovna dognanja o morebitnih ranljivostih uporabljenih algoritmov in implementacij. To vključuje tako kriptografske kot ostale strojne in programske komponente. O morebitnih ranljivostih mora nemudoma poročati nacionalnemu varnostnemu organu.

80. člen
(osnovne varnostne zahteve za kriptografske rešitve različnih stopenj tajnosti)

(1) Za varovanje tajnih podatkov stopnje tajnosti INTERNO in ZAUPNO se dovoli uporaba kriptografskih algoritmov II. nivoja.

(2) Za varovanje tajnih podatkov stopnje tajnosti TAJNO se zahteva uporaba kriptografskih algoritmov I. nivoja, razen v primeru petega odstavka 75. člena te uredbe.

(3) Za varovanje tajnih podatkov stopnje tajnosti STROGO TAJNO, se zahteva uporaba kriptografskih algoritmov I. nivoja.

(4) Vlada podrobneje določi tehnične varnostne zahteve za kriptografske rešitve, ki so varnostno ustrezne za obravnavo tajnih podatkov različnih stopenj tajnosti.

81. člen
(minimalne varnostne zahteve za označevanje, distribucijo in uporabo)

(1) Za vsako kriptografsko rešitev, ki ima potrdilo o varnostni ustreznosti, se izdelajo minimalne varnostne zahteve za označevanje, distribucijo in uporabo, ki jih odobri nacionalni varnostni organ, in sicer za vsako posamezno kriptografsko rešitev posebej.

(2) Pri določanju minimalnih varnostnih zahtev za označevanje, distribucijo in uporabo za posamezno kriptografsko rešitev, se upoštevajo, tudi varnostne zahteve, ki izhajajo iz članstva Republike Slovenije v mednarodnih organizacijah ali jih je Republika Slovenija sprejela s sklenitvijo drugih mednarodnih pogodb in sporazumov.

82. člen
(drugo vrednotenje ugotavljanja varnostne ustreznosti kriptografskih rešitev)

(1) Drugo vrednotenje ugotavljanja varnostne ustreznosti kriptografske rešitve je postopek, v katerem se ugotovi varnostna ustreznost kriptografske rešitve za varovanje tajnih podatkov EU ali zveze NATO. Podlaga za izvedbo drugega vrednotenja je izdano potrdilo o varnostni ustreznosti kriptografskih rešitev za varovanje tajnih podatkov na podlagi zakona in podan pisni predlog s strani enega

od pristojnih organov (ministrstvo, pristojno za javno upravo, ministrstvo, pristojno za notranje zadeve, ministrstvo, pristojno za obrambo, ministrstvo, pristojno za zunanje zadeve, Slovenska obveščevalno-varnostna agencija). Nacionalni varnostni organ začne postopek po uradni dolžnosti, če ugotovi ali izve, da je treba glede na obstoječe ali dejansko stanje začeti postopek ugotavljanja ustreznosti kriptografske rešitve za varovanje tajnih podatkov EU ali zveze NATO.

(2) Drugo vrednotenje kriptografskih rešitev, za varovanje tajnih podatkov EU, opravi pristojni organ EU na podlagi pisnega predloga nacionalnega varnostnega organa. Drugo vrednotenje kriptografskih rešitev, ki jih uporabljajo organi Republike Slovenije za varovanje tajnih podatkov EU vključno do stopnje tajnosti ZAUPNO, pa lahko opravi nacionalni varnostni organ.

(3) Drugo vrednotenje kriptografskih rešitev za varovanje tajnih podatkov zveze NATO vključno do stopnje tajnosti ZAUPNO opravi nacionalni varnosti organ. Drugo vrednotenje kriptografskih rešitev za varovanje tajnih podatkov zveze NATO stopnje tajnosti TAJNO ali STROGO TAJNO, opravi pristojni organ pri zvezi NATO na podlagi pisnega predloga nacionalnega varnostnega organa.

(4) Pisni predlog za postopek drugega vrednotenja pri pristojnih organih EU ali zvezi NATO poda nacionalni varnostni organ le za kriptografske rešitve, ki se ne uporabljajo v sistemih za varovanje nacionalnih tajnih podatkov in imajo pomembno spremenjene varnostno kritične parametre.

XIV. PREGLED TAJNIH PODATKOV

83. člen
(evidenčni pregled EU in NATO tajnih podatkov)

(1) Organ najmanj enkrat letno opravi evidenčni pregled tajnih podatkov EU in zveze NATO stopnje tajnosti TAJNO in STROGO TAJNO. Ob pregledu preveri ali so bili dokumenti vrnjeni v hrambo v varnostno območje ali podatki iz evidence odražajo dejansko stanje.

(2) Centralna registra EU in zveze NATO v začetku leta pozoveta vse podregistre in kontrolne točke, da jim poročajo o številu prejetih in uničenih tajnih podatkih stopnje tajnosti TAJNO in STROGO TAJNO v preteklem letu.

84. člen
(izpis seznama tajnih podatkov)

(1) Pred prenehanjem delovnega razmerja zaposlenega, organizacijska enota, ki vodi evidenco tajnih podatkov pripravi izpis vseh dokumentov, označenih s stopnjo tajnosti, ki so mu dodeljeni.

(2) Zaposleni pred prenehanjem delovnega razmerja preda dokumente v arhiv/tekočo zbirko oziroma dokumente preda skupaj s primopredajnim zapisnikom.

XV. NAČRTI VAROVANJA

85. člen
(načrt varovanja tajnih podatkov v varnostnih območjih)

(1) Vsak organ in organizacija ob upoštevanju postopkov in ukrepov, določenih s to uredbo, izdela načrt varovanja tajnih podatkov v varnostnem območju ali skupini varnostnih območij, s katerim glede na vrsto in stopnjo tajnosti podatkov ter oceno ogroženosti podrobneje predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov v varnostnem območju.

(2) V organih in organizacijah, v katerih se obdelujejo in hranijo le tajni podatki stopnje tajnosti ZAUPNO, zadošča, da se z načrtom varovanja opredelijo ukrepi iz tretjega odstavka 86. člena te uredbe.

86. člen
(vsebina načrta varovanja)

(1) Načrt varovanja se izdela na podlagi ocene ogroženosti in je sestavljen iz splošnega in posebnega dela.

(2) Splošni del načrta varovanja vsebuje predvsem opis glavnega in pomožnih objektov (lega, vhodi, izhodi, zasilni izhodi, skica ali fotografije objekta, glavne in pomožne poti do objekta ter splošni podatki o sistemih oziroma segmentih fizičnega in tehničnega varovanja.

(3) Posebni del načrta varovanja vsebuje:

- opis in značilnosti varnostnega območja;
- ukrepe fizičnega varovanja (zunanje in notranje fizično varovanje, varnostne točke z opisi nalog izvajalcev);
- ukrepe tehničnega varovanja (zunanje in notranje tehnično varovanje, nadzor nad vstopom in izstopom, alarmni sistem in postopki ob sprožitvah posameznih stopenj alarmov, dokumentiranje);
- postopke ob nasilnem vstopu in nepredvidenem dogodku: požaru, potresu, povodnji in drugih naravnih nesrečah;
- postopke in ukrepe ob izgubi, razkritju ali odtujitvi tajnega podatka;
- podatke o drugih ukrepih in postopkih varovanja tajnih podatkov (opravljanje vzdrževalnih in drugih del v varnostnih območjih...);
- podatke o nosilcu načrta varovanja - osebi, ki je odgovorna za izdelavo načrta varovanja;
- podatke o preventivnih varnostnih ukrepih za osebe, ki dostopajo do tajnih podatkov (evidence usposabljanj, postopki ob zaznavah groženj, notranji nadzor ...).

(4) Vsak organ ali organizacija določiti odgovorno osebo za izdelavo načrta varovanja - nosilca načrta varovanja in njegovega namestnika.

(5) Organ ima lahko tudi skupni splošni del načrta varovanja za organ in organe v sestavi, na katerega se navezujejo delni načrti varovanja tajnih podatkov za konkretna varnostna območja, ki se vsebinsko vežejo na posebni del načrta varovanja.

87. člen

(preverjanje ustreznosti načrta varovanja)

Načrt varovanja je treba stalno dopolnjevati, najmanj enkrat letno pa pregledati in preveriti ustreznost ukrepov in postopkov, ki so z njim določeni.

XVI. IZGUBA IN NEPOOBLAŠČENO RAZKRITJE TAJNEGA PODATKA

88. člen
(zloraba tajnega podatka)

(1) Z vsakim nepooblaščenim dostopom do tajnih podatkov, njihovim uničenjem, izgubo, odtujitvijo, poškodovanjem ali kakršnimkoli drugim dogodkom, ki kaže na zlorabo tajnih podatkov (v nadaljnjem besedilu: zloraba tajnega podatka), je treba takoj seznaniti predstojnika organa ali osebo, ki jo pooblasti, in zagotoviti vse ukrepe za preprečitev nadaljnje zlorabe tajnega podatka in izsledite odtujenih tajnih podatkov.

(2) Tajni podatek, pri katerem se izgubi sledljivost, tudi če gre samo za začasno izgubo, se šteje za zlorabljenega, dokler se ne ugotovi nasprotno.

(3) Za vsako zlorabo tajnega podatka je treba uvesti notranjo preiskavo, katere preiskovalce določi predstojnik organa in niso neposredno povezani z zlorabo.

(4) V preiskavi se ugotovi zlasti kateri tajni podatki so, ali bi lahko bili zlorabljeni, ali imajo osebe, ki bi se lahko seznanile s tajnimi podatki ustrezno dovoljenje za dostop do tajnih podatkov ter oceniti morebitno škodo za interese Republike Slovenije oziroma oceniti morebitno škodo za delovanje organa. V preiskavi se navedejo ukrepi, ki jih je treba izvesti za odpravo škodljivih posledic in preprečitev ponovne zlorabe.

(5) Če zloraba tajnega podatka kaže na sum storitve kaznivega dejanja, mora predstojnik organa ali oseba, ki jo za to predstojnik organa pooblasti s tem seznaniti policijo ali drug pristojni organ.

(6) Predstojnik organa, v katerem je bil zlorabljen tajni podatek, mora o zlorabi nemudoma obvestiti organ, ki je določil tajni podatek in nacionalni varnostni organ.

(7) Odgovorna oseba organizacije iz 35. člena zakona mora o zlorabi tajnega podatka takoj obvestiti naročnika.

(8) Nacionalni varnostni organ po potrebi obvesti pristojne organe zveze NATO in EU ter pristojni inšpektorat v Republiki Sloveniji.

89. člen
(obvestilo o zlorabi tajnega podatka)

Obvestilo o zlorabi tajnega podatka vsebuje:

- podatke, potrebne za identifikacijo tajnega podatka (opis dokumenta ali nosilca podatkov, ki vsebuje tajni podatek, vključno s stopnjo tajnosti podatka, številko

in datumom dokumenta, številko kopije, organom, ki je podatek določil za tajnega in kratko vsebino);
- kratek opis okoliščin, v katerih so bili zlorabljeni tajni podatki, in če je znano, število oseb, ki so ali bi lahko imele dostop do tajnega podatka;
- ali je bil organ, ki je podatek določil za tajnega, obveščen;
- postopke in ukrepe, ki so bili izvedeni, da se prepreči nadaljnja zloraba tajnih podatkov.

XVII. PREHODNE IN KONČNE DOLOČBE

90. člen
(uskladitev obstoječih sistemov)

Obstoječe kriptografske rešitve, ki imajo veljavno dovoljenje za obravnavajo tajne podatke stopnje tajnosti TAJNO ali STROGO TAJNO se najkasneje v petih letih od uveljavitve uredbe uskladijo z 75. členom te uredbe.

91. člen
(uskladitev načrtov varovanja)

Organi načrte varovanja, ki so bili izdelani v skladu z 32. členom Uredbe o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11, 24/11), uskladiti s to uredbo najpozneje v šestih mesecih po njeni uveljavitvi.

92. člen
(uničenje tajnih podatkov v centralnih registrih EU in zveze NATO)

Centralna registra EU in zveze NATO hrambo tajnih podatkov uskladita s to uredbo najpozneje v enem letu po njeni uveljavitvi.

93. člen
(uskladitev evidenc tajnih podatkov)

Evidence tajnih podatkov morajo biti usklajene s to uredbo najpozneje v enem letu po njeni uveljavitvi.

94. člen
(distribucijski seznam centralnih registrov zveze NATO in EU)

Distribucijski seznam centralnih registrov zveze NATO in EU določi vlada najpozneje v šestih mesecih po uveljavitvi te uredbe.

95. člen
(prilagoditev upravnih in varnostnih območij)

Minimalni pogoji, ki jim mora ustrezati varnostno-tehnična oprema upravnih in varnostnih območij morajo biti vzpostavljeni najpozneje v enem letu po uveljavitvi te uredbe.

96. člen
(izpolnjevanje pogojev za uporabo naprav za razmnoževanje in izdelavo kopij)

Naprave za razmnoževanje in izdelavo kopij, ki imajo lastnosti elektronske naprave, morajo izpolnjevati pogoje za varovanje tajnih podatkov najpozneje v dveh letih po uveljavitvi te uredbe.

97. člen
(določitev odgovornih oseb sistema)

Predstojnik določi odgovorne osebe iz 48. člena te uredbe najpozneje v šestih mesecih po uveljavitvi te uredbe.

98. člen
(določitev veljavnih tehničnih navodil za povezovanje sistemov)

Vlada na predlog nacionalnega varnostnega organa določi veljavna tehnična navodila za povezovanje sistemov. Do sprejetja ustreznih nacionalnih tehničnih navodil se uporabljajo predpisi zveze NATO in EU.

99. člen
(določitev izvedbenih navodil za izvajanje zaščite pred neželenim elektromagnetnim sevanjem)

Vlada na predlog nacionalnega varnostnega organa podrobneje določi izvedbena navodila za izvajanje zaščite pred neželenim elektromagnetnim sevanjem. Do sprejetja navodil se uporabljajo predpisi zveze NATO in EU.

100. člen
(določitev varnostnih zahtev za kriptografske rešitve različnih stopenj tajnosti)

Vlada podrobneje določi tehnične varnostne zahteve za kriptografske rešitve, ki so varnostno ustrezne za obravnavo tajnih podatkov različnih stopenj tajnosti najpozneje v enem letu po uveljavitvi te uredbe.

101. člen
(sprejem sklepa o varovanju kriptografskega materiala)

Vlada sprejme sklep o varovanju kriptografskega materiala, najpozneje v roku enega leta po uveljaviti te uredbe.

102. člen
(razveljavitvena določba)

Z dnem uveljavitve te uredbe preneha veljati Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11 in 24/11 – popr.), Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/07 in 86/11) in Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/06).

103. člen
(uveljavitev uredbe)

Ta uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

Ljubljana, dne
EVA 2021-1535-0001

Vlada Republike Slovenije
Janez Janša
predsednik

Priloge:
Priloga 1: Vzorci oznak stopnje tajnosti INTERNO, ZAUPNO, TAJNO IN STROGO TAJNO,
Priloga 2: Pogoji za upravna in varnostna območja
Priloga 3: Vzorec napisov za varnostno območje
Priloga 4: Vzorec seznama vpogledov v tajni podatek
Priloga 5: Program usposabljanja kurirjev
Priloga 6: Pooblastilo za prenos (OBR-KU)
Priloga 7: Pooblastilo za prenos (OBR-OP)
Priloga 8: Navodilo za uničenje in ponovno uporabo elektronskih nosilcev tajnih podatkov
Priloga 9: Postopki in merila za povezovanje sistemov
Priloga 10: Načrt varovanja sistema
Priloga 11: Ocena varnostnih tveganj sistema
Priloga 12: Varnostno navodilo za delo v sistemu
Priloga 13: Postopki in merila za zaščito pred neželenim elektromagnetnim sevanjem v komunikacijskih in informacijskih sistemih, v katerih se obravnavajo tajni podatki
Priloga 14: Varnostno navodilo za delo v sistemu INTERNO
Priloga 15: Potrdilo o varnostni ustreznosti kriptografske rešitve
Priloga 16: Vloga za začetek postopka ugotavljanja ustreznosti kriptografske rešitve
Priloga 17: Vsebina dokumentacije za začetek postopka ugotavljanja ustreznosti kriptografske rešitve

OBRAZLOŽITEV

I. UVOD

1. Pravna podlaga (besedilo, vsebina zakonske določbe, ki je podlaga za izdajo uredbe)

Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20).

2. Rok za izdajo uredbe, določen z zakonom

Rok za sprejem predpisa je določen v Zakonu o spremembah in dopolnitvah Zakona o tajnih podatkih (ZTP-E) (Uradni list RS, št. 8/20), ki v poglavju PREHODNE IN KONČNE DOLOČBE določa, da Vlada Republike Slovenije v šestih mesecih od uveljavitve tega zakona izda predpise iz petega odstavka spremenjenega 22.g člena, sedmega odstavka spremenjenega 35.b člena, šestega in desetega odstavka spremenjenega 39. člena in štirinajstega odstavka novega 39.a člena zakona.

3. Splošna obrazložitev predloga uredbe, če je potrebna

Uredba o varovanju tajnih podatkov je temeljni izvedbeni akt Zakona o tajnih podatkih. Nova uredba združuje prejšnjo Uredbo o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11 in 24/11 – popr.), Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/07 in 86/11) in Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/06), ki bodo s sprejetjem nove uredbe prenehali veljati.

4. Predstavitev presoje posledic za posamezna področja, če te niso mogle biti celovito predstavljene v predlogu zakona

II. VSEBINSKA OBRAZLOŽITEV PREDLAGANIH REŠITEV

I. SPLOŠNE DOLOČBE

K 1. členu

Na podlagi novele Zakona o tajnih podatkih se na novo ureja načine in oblike označevanja tajnih podatkov, fizične, organizacijske in tehnične ukrepe ter obvezne sestavine postopkov za varovanje tajnih podatkov. Z uveljavitvijo te uredbe prenehajo veljati Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11 in 24/11 – popr.), Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/07 in 86/11) in Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/06). Vsebina navedenih predpisov se obravnava enotno v tej uredbi.

K 2. členu

V drugem odstavku 2. člena je na novo opredeljeno, da se določbe, ki urejajo varovanje tajnih podatkov uporabljajo tudi za varovanje tajnih podatkov tujih držav in mednarodnih organizacij, razen če ni izrecno navedeno drugače.

Republika Slovenija se je z mednarodnimi pogodbami zavezala, da bo na primerljiv način varovala tajne podatke tujih držav in mednarodnih organizacij. S to določbo uredba nedvoumno določa, na kakšen način se varujejo nacionalni tajni podatki in tuji tajni podatki.

K 3. členu

V tem členu so pojasnjeni izrazi, ki se uporabljajo v tej uredbi.

II. DOLOČANJE IN OZNAČEVANJE TAJNIH PODATKOV

K 4. členu

Člen podrobneje določa obvezne sestavine pisne ocene. Ocena možnih škodljivih posledic je temelj za določitev stopnje tajnosti tajnih podatkov, zato člen predpisuje minimalne sestavine, ki jih le ta mora vsebovati.

K 5. členu

Pisna ocena mora vedno slediti tajnemu podatku, zato jo je potrebno hraniti skozi ves življenjski cikel tajnega podatka.

K 6. členu

Člen opredeljuje način in obliko označevanja posameznih nosilcev tajnih podatkov. Pri tajnih podatkih praviloma naslov dokumenta/nosilca ne vsebuje tajnih podatkov. Izjemoma, v kolikor to ni mogoče, mora biti to vidno označeno na način, da se na koncu naslova v oklepaju zapiše črka, ki označuje stopnjo tajnosti le tega.

Dodan je tudi nov četrti odstavek v katerem se podrobneje opredeli primer, ko spremni dopis ne vsebuje tajnih podatkov, tajni podatki so navedeni le v prilogi spremnega dopisa. Določba omogoča, da se spremni dopis, ki ne vsebuje tajnih podatkov lahko pripne v zbirko dokumentarnega gradiva, ki se nahaja v sistemih, ki niso akreditirani za obravnavanje tajnih podatkov.

Sedmi odstavek dodatno določa, da mora ob vstopu uporabnik nedvoumno biti opozorjen, da vstopa v tajni sistem kjer se varujejo tajni podatki do določene oziroma najvišje stopnje tajnih podatkov v sistemu (tapeta na ozadju, pojavnim oknom za zaslonu, …).

K 7. členu

Člen določa, da tuji tajni podatki ohranijo izvorno oznako in se ne prevaja.

K 8.členu

V tem členu je opredeljeno, da se lahko posamezni odstavki, deli odstavkov oz. posamezna beseda označujejo z različnimi stopnjami tajnosti, da pa je celoten dokument označen z najvišjo stopnjo tajnosti. Z uporabo te določbe bo prejemnik tajnega podatka seznanjen katere podatke je originator določil kot tajne.

K 9.členu

Člen določa način in tehnično izvedbo spremembe ali preklica podatkov, ki so označeni kot tajni. Dodatno je navedeno, da evidenca dokumentarnega gradiva omogočati razvid vseh sprememb stopenj tajnosti, kot tudi podlag za njihovo spremembo.

K 10.členu

Iz kopije dokumenta, ki vsebuje tajni podatek mora nedvoumno izhajati, da gre za tajni podatek, ter da je kopija. Poleg omenjenega mora kopija vsebovati tudi podatke o zaporedni številki kopije in datum izdelave kopije, ki sta potrebni predvsem v primerih, ko se izdela kopija dokumenta, ki je tudi že sam po sebi kopija. Na ta način bo nedvoumno razvidna katera oznaka »KOPIJA« označuje dokument.

V primeru, da iz same kopije ni razvidno, iz katerega zapisa ali dela zapisa je kopiran del, mora kopija vsebovati tudi podatke o številki, datumu izvirnega dokumenta ter številki strani, ki je na izvirnem dokumentu.

K 11.členu

Člen določa način in obliko izvedbe izločanja tajnih podatkov iz dokumenta v primerih, da bi se z dokumentom morale seznaniti osebe, ki nimajo veljavnega dovoljenja za dostop do tajnih podatkov. Izločanje tajnih podatkov iz dokumenta je potrebno izvesti na način, da izločenih podatkov v dokumentu ni več mogoče rekonstruirati ali prebrati (na primer s prekritjem) Po tem členu postopa tudi organ na podlagi zahteve po dostopu do informacij javnega značaja oziroma na podlagi prejete odločbe informacijskega pooblaščenca. Pri tem je potrebno zagotoviti, da so tajni podatki izločeni na način, da se z dokumentom, iz katerega so bili izločeni tajni podatki, ne bi ogrozila tajnost izvirnega dokumenta.

III. OBRAVNAVA IN HRAMBA TAJNIH PODATKOV

K 12., 13., 14. in 15 členu

Členi določajo prostor, tako imenovano upravno in varnostno območje, kjer se lahko tajni podatki obravnavajo. V upravnem območju se lahko hranijo le tajni podatki stopnje tajnosti INTERNO, obravnavajo (in ne tudi hranijo) pa se lahko tudi tajni podatki višjih stopenj tajnosti (vključno do stopnje tajnosti TAJNO). Slednji morajo biti v času obravnave pod stalnim nadzorom, po končani obravnavi pa mora oseba tajni podatek stopnje tajnosti ZAUPNO ali TAJNO vrniti v hrambo v varnostno območje.

Izjemo predstavljajo obravnavanje tajnih podatkov v začasnih upravnih in varnostnih območjih, saj velikokrat prihaja do situacij, ko je treba tajne podatke obravnavati izven prostorov, ki so v upravljanju organov (npr. izvedba raznih konferenc v za to najetih prostorih – hoteli, Kongresni center Brdo…). V določenih situacijah pa prihaja celo do obravnavanja tajnih podatkov izven upravnih in varnostnih območij (izvedba vojaških

vaj na terenu, razne simulacije na terenu…) itd. kjer se prav tako obravnavajo tajno podatki, niso pa na terenu vzpostavljeni vsi tehnični in fizični pogoji varovanja tajnih podatkov). Med te situacije npr. spada tudi obravnavanje tajnih podatkov stopnje tajnosti INTERNO, ki jih javni uslužbenci potrebujejo za svoje delo pri delu na daljavo (delo od doma, sestanki v tujini itd.).

K 16. členu

Člen opredeljuje hrambo tajnih podatkov glede na stopnjo tajnosti. Novost v tem členu je hramba tajnih podatkov v I. varnostnem območju, kjer se ne zahteva več nujno hramba v dodatnih blagajnah, saj so pogoji za vzpostavitev varnostnega območja I. stopnje strožji in zato omogočajo hrambo tudi v pisarniških ali kovinskih omarah, treba pa je zagotoviti, da se s podatki ne seznanijo nepooblaščene osebe (ta ureditev je povzeta v skladu z varnostno politiko zvete NATO kot t.i. 'Open storage area').

Tajni podatki se lahko hranijo le v ustreznih prostorih, ki zagotavljajo standarde za hrambo posameznih dokumentov, ki vsebujejo tajne podatke. Obenem člen ne prepoveduje hrambe tajnih podatkov nižjih stopenj tajnosti pod pogoji, kot so določeni za višje stopnje tajnosti.

Glede rokov hrambe člen napotuje na druge predpise, ki urejajo poslovanje z dokumentarnim gradivom.
Centralna registra EU in zveze NATO sta primarno namenjena distribuciji tajnih podatkov v Republiki Sloveniji in ne hrambi tajnih podatkov, zato je v uredbi določen rok, da tajne podatke hranita največ dve leti. Organ/organizacija, ki prejme tajne podatke preko centralnega registra le te hrani skladno z drugim odstavkom tega člena.

Organizacije, ki jih ne zavezujejo predpisi, ki urejajo poslovanje z dokumentarnim gradivom tajne podatke hranijo dokler jih potrebujejo za opravljanje delovnih nalog. Po končani uporabi jih uničijo, skladno z določbami te uredbe. V primeru, da nimajo ustreznih pogojev za uničevanje tajnih podatkov, oziroma jih, v dogovoru s pošiljateljem le temu vrnejo.

IV. FIZIČNI UKREPI VAROVANJA

K 17. členu

Člen opredeljuje pogoje za vzpostavitev I. varnostnega območja. Tukaj se zahtevajo najstrožji ukrepi varovanja. Novost je ta, da se zahteva neposredno in neprekinjeno fizično varovanje varnostnega območja ali delovnih prostorov, v katerih se varnostno območje nahaja, in z elektronskim sistemom za protivlomno varovanje varnostnega območja. Obvezno fizično varovanje je dodan kot dodaten pogoj in se nanaša na prejšnji člen, saj se v tem primeru tajni podatki ne rabijo dodatno varovati v protivlomnih blagajnah. Glede na to, da se izvaja fizično varovanje na sami lokaciji, mora biti intervencijski čas po sproženem alarmnem signalu krajši od sedem minut.

K 18. členu

Člen opredeljuje pogoje za vzpostavitev II. varnostnega območja. Novost je ta, da se vstop brez ustreznega dovoljenja za dostop do tajnih podatkov lahko omogoči drugim osebam, ki se zaradi opravljanja svoje delovne naloge ne bodo seznanile s tajnimi podatki in imajo ves čas zadrževanja v varnostnem območju zagotovljeno spremstvo v

varnostnem območju zaposlene osebe. Na ta način se olajšuje investicijsko vzdrževanje varnostnega območja in opreme, saj npr. serviserji, elektroinštalaterji, čistilke in druge osebe, ki morajo vstopiti v varnostno območje zaradi izvedbe vzdrževalnih del, nujno ne potrebujejo dovoljenja za dostop do tajnih podatkov (v kolikor se z njimi pri svojem delu ne bodo seznanili), se pa lahko v varnostnem območju zadržujejo samo v stalnem spremstvu pooblaščenih oseb.

K 19. členu

Člen opredeljuje pogoje za vzpostavitev upravnega območja. Območje mora biti vidno označeno.

K 20. členu

Člen podrobneje opredeljuje naloge centralnih registrov EU in zveze NATO. Vodja in namestnik centralnega registra sta odgovorna za izvajanje vseh varnostnih ukrepov za zagotavljanje varovanja tajnih podatkov v posameznem registru. Člen nadalje tudi določa, da se skladno s predpisi zveze NATO v Centralnem registru zveze NATO določi pooblaščena oseba, ki opravlja naloge, določene v varnostnih politikah zveze NATO. Pooblaščena oseba je hkrati lahko tudi vodja oz. namestnik centralnega registra.

K 21. členu

Za varovanje tajnih podatkov se v ministrstvih, organih v sestavi ministrstev in vladnih službah, vzpostavi podregister oziroma kontrolna točka. Omenjeni organi morajo pred vzpostavitvijo podregistra oz. kontrolne točke predhodno pridobiti soglasje nacionalnega varnostnega organa. Vlogi predložijo tudi načrt varovanja, v katerem opredelijo postopke in ukrepe varovanja. Nacionalni varnostni organ na podlagi prejete vloge opravi ogled, v katerem preveri ali postopki in ukrepi tehničnega in fizičnega varovanja ter organizacija varovanja zagotavljajo ustrezno raven varovanja tajnih podatkov glede na vrsto, količino in oceno ogroženosti tajnih podatkov.

Vodja in namestnik podregistra oz. kontrolne točke sta odgovorna za izvajanje vseh varnostnih ukrepov za zagotavljanje varovanja tajnih podatkov v posameznem podregistru. Člen nadalje tudi določa, da predstojnik organa, skladno s predpisi zveze NATO v podregistru oz. kontrolni točki zveze NATO, v katerem se obravnavajo tajni podatki stopnje tajnosti STROGO TAJNO določi pooblaščeno osebo, ki opravlja naloge, določene v varnostnih politikah zveze NATO. Pooblaščena oseba je hkrati lahko tudi vodja oz. namestnik podregistra.

K 22. členu

Člen opredeljuje pogoje, ki jih morajo izpolnjevati upravna in varnostna območja, in so navedeni v Prilogi 2 te uredbe in so njen sestavni del. Pogoji so primerljivi dosedanjim merilom, ki so določeni v Sklepu o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/06), ki ga je sprejela Vlada Republike Slovenije leta 2006. Novost je ta, da pogoji niso več 'taksativno našteti' in jih ni treba kumulativno izpolnjevati, ampak je določene varnostne elemente mogoče med seboj kombinirati (npr. v kolikor je zagotovljeno neposredno in neprekinjeno fizično varovanje varnostnega območja ali objekta, v katerem se varnostno območje nahaja, kot dodaten pogoj ni obvezna namestitev protivlomni vrat

po standardu SIST EN 1627 protivlomne stopnje IV, ampak so lahko tudi protivlomne stopnje II ali III.) v petnajstih letih od sprejetja omenjenega sklepa so se spremenili tudi določeni varnostni standardi, nekateri pa sploh ne obstajajo več oz. se uvajajo novi standardi, zato smo pri pogojih pri varnostnotehnični opremi, ki se sme vgrajevati v varnostna območja pri posameznem standardu dodati besedilo, ki omogoča vgradnjo primerljive opreme (npr. …mora ustrezati standardu SIST EN 50133 razreda 3, kategorija pristopa B, ali drugemu primerljivemu standardu, katerega skladnost preverja UVTP).

K 23. členu

Člen opredeljuje nošenje različnih identifikacijskih izkaznic za osebe, ki se gibljejo v varnostnih in upravnih območjih.

K 24. členu

Člen opredeljuje postopek razglasitve upravnega ali varnostnega območja. Varnostno oziroma upravno območje v organizaciji se določi na podlagi predhodno opravljenega ogleda, ki ga izvede organ, pristojen za izdajo varnostnega dovoljenja organizaciji (SOVA, MNZ, MORS). Z ogledom se preveri ali postopki in ukrepi tehničnega in fizičnega varovanja ter organizacija varovanja zagotavljajo ustrezno raven varovanja tajnih podatkov glede na vrsto, količino in oceno ogroženosti tajnih podatkov. Kadar se upravno območje vzpostavlja v državnih organih ogled ni potreben.
Organ ali organizacija mora pred določitvijo varnostnega območja pridobiti pozitivno mnenje nacionalnega varnostnega organa (Urada Vlade Republike Slovenije za varovanje tajnih podatkov) o ustreznosti varnostnotehnične opreme, vgrajene v varnostno območje, ter postopkov in ukrepov varovanja varnostnega območja. Na koncu predstojnik organa ali organizacije oziroma oseba, ki jo on pooblasti, določi varnostna in upravna območja s sklepom in o tem obvesti nacionalni varnostni organ (Urad Vlade Republike Slovenije za varovanje tajnih podatkov namreč v skladu z določili 43.e člena zakona vodi evidenco upravnih in varnostnih območij v organih in organizacijah).

K 25. členu

Člen opredeljuje način označevanja upravnih in varnostnih območij. Vsak ki vstopa v upravno ali varnostno območje mora namreč o tem biti nedvoumno obveščen. V prilogi 3 te uredbe so tudi vzorci napisnih tabel.

K 26. členu

Člen opredeljuje predvsem način nadzora vstopa drugih oseb (tistih, ki niso zaposleni v organu ali organizaciji) v upravna in varnostna območja. Pred vstopom drugih oseb v varnostno in upravno območje mora oseba, ki nadzira vstop v varnostno oziroma upravno območje, preveriti njihovo identiteto in namen obiska ter izpolnjevanje drugih pogojev za vstop v varnostno območje. Obiskovalci se v upravnih in varnostnih območjih lahko gibljejo samo v stalnem spremstvu ali pod nadzorom zaposlenega osebja.

K 27. členu

Varnostno tehnično opremo lahko uporabljajo in vzdržujejo le pooblaščene osebe. Pooblastilo je lahko dano s kupoprodajno, vzdrževalno pogodbo, pooblastilom, sklepom…. Pri vzdrževanju opreme, ki vsebuje spominske module, je treba zagotoviti, da se gradniki, kjer bi lahko bili shranjeni tajni podatki, ne iznašajo iz upravnega in varnostnega območja.

K 28. in 29. členu

Člen določa celovitost sistema in možnost dostopa z različnih lokacij do nosilca podatkov (npr. sistem se nahaja na centralni lokaciji do katere se preko lahkih odjemalcev uporabniki iz oddaljenih lokacij povezujejo v sistem). V primeru nosilcev podatkov na katerih so podatki šifrirani s kriptografsko rešitvijo se morajo obravnavati v skladu z minimalnimi varnostnimi zahtevami kriptografske rešitev, ki ima izdano potrdilo o varnostni ustreznosti kriptografske rešitve. Ob vsakokratnem vstopu v sistem mora uporabnik biti obveščen o najvišji stopnji tajnosti podatkov v sistemu.

K 30. členu

Člen opredeljuje kdaj je treba opraviti protiprisluškovalni pregled varnostnih območij in kdo ga opravlja.

K 31. členu

Člen določa na kak način se označijo blagajne, kjer se hranijo tajni podatki.

K 32. členu

Člen določa kdo lahko nastavlja kombinacije elektronskih ali mehanskih ključavnic in kdaj je treba njihove nastavitve zamenjati.

V. KOPIRANJE IN PREVAJANJE TAJNIH PODATKOV

K 33.členu

Člen določa način ter kje in kdo lahko kopira tajne podatke. Tajni podatki se lahko kopirajo le v upravnem oz. varnostnem območju, na napravah ki izpolnjujejo pogoje za varovanje tajnih podatkov v sistemih.

Kopiranje tajnih podatkov je mogoče izvesti le na podlagi pisarniške odredbe predstojnika organa ali od njega pooblaščene osebe. Če je odredba za kopiranje pripravljena v obliki samostojnega dokumenta, mora biti le ta evidentiran v evidenci dokumentarnega gradiva. V primeru, da je odredba odtisnjena, natisnjena ali napisana na dokumentu, ki se bo kopiral, mora biti odtisnjena, natisnjena ali napisana na prvi strani dokumenta.

Organ, ki je izdelal dokument, ki vsebuje tajne podatke lahko navkljub splošnem dovoljenju po kopiranju tajnega podatka po tej uredbi lahko to izrecno prepove. Lastnik podatka izdela oceno in se mu dovoljuje, da sam presodi in zavaruje podatek v taki meri kot je to ocenil. S tem smo preprečili, da se zaradi strahu pred kopiranjem tajnih podatkov umetno ne vzdigujejo stopnje tajnosti.

K 34. členu

Uredba v tem členu določa, da tajni podatek, ki je bil preveden obdrži vse oznake, ki jih ima izvirni dokument. Prevod dokumenta je priloga izvirnika. To določilo je pomembno predvsem zaradi prevajanja tajnih podatkov EU in zveze NATO. Osebe, ki opravljalo prevode, morajo imeti dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti.

K 35. členu

Člen določa kako je potrebno voditi ustrezen razvid iznosa tajnih podatkov iz sistema ter opredeljuje kako se označujejo nosilci podatkov sistema v primeru, da gre za varnostne kopije tajnih podatkov. Člen opredeljuje tudi kaj mora vsebovati varnostna dokumentacija v primeru, da se v sistemu varujejo tajni podatki stopnje ZAUPNO in višje in kdo lahko iz sistema iznaša tajne podatke.

VI. EVIDENTIRANJE

K 36. členu

Člen določa katere podatke mora vsebovati evidenca tajnih podatkov, ki jo vodijo centralni registri, podregistri in kontrolne točke. V posamezen vpis se smiselno vpisujejo podatki iz nosilca tajnega podatka. Da se evidenci iz tega in 33. člena te uredbe ne bi podvojevali ter v primeru, da organ vodi skupno evidenco vseh tajnih podatkov, se evidenca iz tega člena lahko nadomesti z evidenco iz 33. člena.

K 37. členu

Člen določa katere podatke mora vsebovati evidenca tajnih podatkov, ki jo vodijo organi in organizacije, ki prejmejo oziroma imajo v lasti tajne podatke. V posamezen vpis se smiselno vpisujejo podatki iz nosilca tajnega podatka. Da se evidenci ne bi podvojevali ter v primeru, da organ vodi skupno evidenco vseh tajnih podatkov, evidenca iz tega člena lahko nadomesti z evidenco iz 32. člena.

K 38. členu

Nosilcu, ki vsebuje tajne podatke stopenj tajnosti TAJNO in STROGO TAJNO mora biti priložen seznam vpogledov. Vzorec seznama vpogledov je priloga uredbe. Seznam vpogledov je dodatni varnostni kriterij za zagotavljanje sledljivosti tajnih podatkov dveh najvišjih stopenj tajnosti, saj vsakdo, ki se seznani s tajnim podatkom navede datum in čas seznanitve in se tudi podpiše.

VII. DISTRIBUCIJA TAJNIH PODATKOV

K 39. členu

Tajni podatki se lahko distribuirajo le ob upoštevanju načela potrebe po vedenju. Člen podrobneje opredeljuje kdo lahko odredi distribucijo tajnih podatkov znotraj organa.

K 40. členu

Vsak organ ali organizacija lahko za posamezne nosilce tajnih podatkov izdela distribucijski seznam. Hkrati uredba tudi omogoča izdelavo distribucijskega seznama za dokumente, ki po vsebini sodijo v eno delovno področje.

Centralna registra EU in zveze NATO sta enotni vstopni točki za prejemanje tajnih podatkov stopenj tajnosti zaupno in višjih stopenj tajnosti iz inštitucij EU in zveze NATO ter skrbita za distribucijo omenjenih tajnih podatkov na ozemlju Republike Slovenije.

Glede na to da opravljata distribucijo tajnih podatkov za vse organe v Republiki Sloveniji, Vlada na predlog Ministrstva za zunanje zadeve za tajne podatke EU in Ministrstva za obrambo, za tajne podatke zveze NATO, določi distribucijski seznam. Ministrstvi oblikujeta predlog distribucijskega seznama na podlagi predhodnih predlogov posameznih organov.

VIII. PRENOS TAJNIH PODATKOV

K 41. členu

Člen opredeljuje kako morajo biti nosilci tajnih podatkov zaščiteni med prenosom. Ob enem tudi določa, da mora vsak organ določiti kje in kdo v organu lahko sprejema nosilce tajnih podatkov.

K 42. členu

Člen določa kdo lahko prenaša tajne podatke na ozemlju Republike Slovenije.

K 43. členu

Člen določa kdo in na kakšen način lahko opravlja mednarodni prenos tajnih podatkov.

K 44.členu

V drugi točki se predvideva izdelava načrta varovanja prenosa tajnih podatkov. Načrt je potrebno izdelati za poti, po katerih prenos poteka dnevno oziroma periodično (vsak drugi dan, tedensko itd.)

K 45. členu

Z definicijo tega člena se zadosti tudi zahtevi iz varnostne politike zveze NATO, da se morajo kurirji oziroma osebe usposabljati. Ne glede na to, se kurirske službe lahko organizirajo tudi v drugih organih in je v takih primerih potrebno tudi ta kader strokovno usposabljati.

Predvideno je, da bodo kurirje usposabljali MORS in Policija ter za lastne potrebe tudi v Slovenska obveščevalno-varnostna agencija. Glede na to, da bosta usposabljanje

kurirjev iz drugih organov izvajala MORS in Policija bo to za oba organa predstavljalo določena finančna sredstva.

K 46. členu

Člen predvideva izjemne primere, v katerih se lahko opravi osebni prenos tajnega podatka. Oseba, ki bo opravila osebni prenos mora biti pred tem seznanjena s postopki in ukrepi varovanja prenosa tajnega podatka, predstojnik organa pa ji mora izdati ustrezno pooblastilo za vsakokraten prenos. Pooblastilo mora vsebovati podatke o tajnih podatkih, ki jih pooblaščena oseba sme prenašati.

K 47. členu

Za varovanje tajnih podatkov je nujno, da ima oseba/kurir pri prenosu tajnih podatkov pri sebi pooblastilo za prenos, katerega izda predstojnik organa. V prilogi je predlog enotnega obrazca (OBR-KU) katerega naj bi predstojniki organov podelili samo tistim osebam, ki imajo nalogo oziroma dolžnost za prenos tajnih podatkov.

K 48. členu

V prvi točki tega člena je pomembno, da delavci policije na zaprosilo osebe/kurirja , ki se izkaže z veljavnim pooblastilom, nudijo pomoč v taki meri, ki zagotavlja varovanje tajnih podatkov pred odtujitvijo, poškodovanjem ali uničenjem. Oseba/kurir lahko zaprosi za pomoč ob okvari vozila, slabosti, nesreči ali drugih nepredvidenih dogodkih.

Policija ima v svojem zakonu predvideno asistenco, vendar se nam zdi prav, da je taka oblika pomoči s ciljem varovanja tajnih podatkov zapisana tudi v tej uredbi. Pri postopkih policije, ko se oseba izkaže s pooblastilom in ob ugotovitvi, da oseba prenaša tajne podatke, pri postopku pa ugotovi, da je ta oseba pod vplivom alkohola, mamil ali drugih substanc ali kakorkoli nesposobna nadalje opravljati nalogo, preprečijo osebi/kurirju nadaljevanje prenosa in storijo vse potrebno da ohranijo tajne podatke pred odtujitvijo, poškodovanjem ali uničenjem. Zoper tako osebo se uvedejo postopki, ki so predpisani z zakoni ali drugimi predpisi.

Pomembno je določilo, da delavci policije in carine pri opravljanju nalog iz svojih pristojnosti nimajo pravice vpogleda v vsebino tajnih podatkov.

K 49. členu

Člen določa na kakšen način je dovoljen prenos tajnih podatkov v sistemih izven upravnega ali varnostnega območja in na kakšen način je dovoljen prenos tajnih podatkov znotraj upravnega in varnostnega območja (optične povezave). Morebitno odstopanje je dovoljeno v primeru odobritve pristojnega organa za izvajanje zaščite proti neželenem elektromagnetnem sevanju in v skladu z navodilom kot je navedeno v tem členu.

IX. UNIČENJE TAJNIH PODATKOV

K 50. členu

Tajni podatki se uničijo po preteku roka hrambe oz. takoj ko niso več neobhodno potrebni za opravljanje delovnih nalog.
Uničeni morajo biti na način, da postane nerazpoznavni in neobnovljivi. V primeru, da razrezan papir ne ustreza standardu navedenem v tem členu oz. da komisija ne razpolaga z ustreznim rezalnikom, je potrebno papir, ki je večji od dimenzije razrezanega papirja, določenega v uredbi, dodatno obdelati oz. predelati (npr. sežgati, obdelati v raztopini). Komisija za uničevanje mora imeti nosilce tajnih podatkov med postopkom uničevanja ves čas pod nadzorom.

X. VAROVANJE TAJNIH PODATKOV V SISTEMIH

K 51. členu

S tem členom se določa odgovorne osebe za sistem na organu oziroma dislocirani lokaciji organa in v organizacijah, ki bodo vzpostavili sistem, v katerem se bodo varovali tajni podatki z določeno stopnjo tajnosti. Predstojnik organa ali organizacije imenuje in preklicuje odgovorne osebe za sistem v katerem se varujejo tajni podatki ter obvešča nacionalni varnostni organ o določitvah in spremembah.

K 52. členu

Člen opredeljuje funkcije in odgovornosti, ki jih izvaja skrbnik sistema za varovanje tajnih podatkov na organu ali v organizaciji bodisi za pridobitev varnostnega dovoljenja bodisi izvajanja pravilnega delovanja in spremljanje vseh posegov v sistemu, v katerem se varujejo tajni podatki določene stopnje tajnosti. Na novo so opredeljene naloge skrbnika sistema.

K 53. členu

Člen opredeljuje funkcije in odgovornosti, ki jih izvaja upravljavec sistema za varovanje tajnih podatkov na organu ali v organizaciji. Na novo so opredeljene naloge upravljavca sistema.

Kot je določeno v 2. točki tega člena upravljavec sistema izvaja svoje naloge v skladu z navodili skrbnika sistema.

K 54. členu

Člen opredeljuje odgovornosti vodje informacijske varnosti sistema v katerem se obravnavajo tajni podatki določene stopnje tajnosti. Na novo so opredeljene naloge vodje informacijske varnosti sistema.

K 55. členu

Člen določa skrbnika kriptografskega materiala, ki je odgovoren za upravljanje s kriptografskim materialom skladno s sklepom o varovanju kriptografskega materiala, ki ga na predlog nacionalnega varnostnega organa sprejme Vlada Republike Slovenije.

K 56. členu

Člen določa krovne organe za razdeljevanje kriptografskega materiala, katerih naloge bodo določene s sklepom Vlade RS.

K 57. členu

Člen opredeljuje, da mora vsak vzpostavljen sistem, v katerem se obravnavajo tajni podatki, imeti določen varnostni način delovanja sistema. Hkrati so tudi opredeljene pravice oziroma potrebno dovoljenje za dostop do tajnih podatkov oseb in v katere sisteme le te lahko dostopajo glede na varnostni način delovanja sistema oziroma imajo pravico po vedenju.

K 58. členu

V tem členu je opredeljena identifikacija in overitev uporabnikov, ki imajo pravico za dostop v sistem v katerem se obravnavajo tajni podatki in postopek overitve za vstop v sistem.

K 59. členu

Člen določa pravice in selekcijo uporabnika, ki je glede na opravljanje svojih nalog ali funkcij oziroma do katerih je upravičen na podlagi pooblastila, določenega z zakonom ali predpisom, izdanim na podlagi zakona, do dostopa do tajnih podatkov v sistemu. Prav tako so v tem členu opredeljene naloge skrbnika sistema, ki vzpostavi in vzdržuje seznam uporabnikov sistema, iz katerega so za vsakega uporabnika sistema razvidni njegovi identifikacijski podatki in njegove pravice dostopa (varnostna shema). Skrbnik sistema tudi posodablja varnostno shemo ob spremembi pravic posameznega uporabnika (na primer: prekinitev delovnega razmerja, premestitev in podobno).

K 60. členu

V tem členu so opredeljeni postopki za spremljanje in nadzor dostopa do sistema in tajnih podatkov, ki se v sistemu varujejo. Opredeljeni so postopki ugotavljanja , kdo, kdaj in od kod je dostopal, čas dela v sistemu, kateri tajni podatki so bili obravnavani, in sicer tako, da je mogoče ukrepati ob sumu nepooblaščenega vstopa v sistem, nepooblaščenega dostopa do tajnih podatkov ali zlorabe tajnih podatkov v sistemu ter pozneje rekonstruirati posamezne dostope do tajnih podatkov v sistemu. Za vsak dostop do tajnega podatka stopnje tajnosti ZAUPNO ali višje v sistemu mora obstajati možnost rekonstrukcije oziroma se mora zagotavljati revizijska sled iz katere je možno rekonstruirati dogodke in dostope uporabnikov do tajnih podatkov v sistemu. Tudi ostali dogodki kot so izvedbeni in kontrolni posegi morajo biti evidentirani in dokumentirani. V členu je določeno hranjenje le teh podatkov za zagotavljanje dokazov v morebitnih delovno pravnih in kazenskih postopkih.

K 61. členu

Člen določa, da je v primeru povezovanja sistemov med organi ali organizacijami določeno, da le ti morajo pridobiti soglasje skrbnikov posameznega sistema in da mora povezovanje biti izvedeno v skladu z Navodilom za povezovanje komunikacijsko informacijskih sistemov (Priloga 9 te uredbe).

XI. VARNOSTNO VREDNOTENJE SISTEMOV

K 62. členu

Nacionalni varnostni organ, na podlagi prejete vloge organa ali organizacije za izdajo varnostnega dovoljenja za delovanje sistema, v katerem se varujejo tajni podatki, prične s postopkom, ki ga vodi v skladu z zakonom ki ureja upravni postopek. Varnostno vrednotenje sistema nacionalni varnostni organ opravi na podlagi pregleda in ocene varnostne dokumentacije ter varnostnega vrednotenja sistema na lokaciji organa ali organizacije, s katerim preveri izpolnjevanje ukrepov in postopkov za zagotovitev varnega delovanja sistema v skladu s to uredbo in drugimi zakonskimi in podzakonskimi predpisi s področja varovanja tajnih podatkov.

K 63. členu

V skladu z 58. členom nacionalni varnosti organ opravi tudi postopke in varnostno vrednotenje sistemov tujih držav ali mednarodnih organizacij, v katerih se obravnavajo tajni podatki. Po končanem postopku nacionalni varnostni organ izda izjavo o skladnosti, ki jo posreduje pristojnemu organu tuje države ali mednarodne organizacije.

K 64. členu

Člen določa, da je potrebno v postopku varnostnega vrednotenja s strani organa ali organizacije izdelati varnostno dokumentacijo, ki je priloga vloge za pridobitev varnostnega dovoljenja za delovanje sistema, v katerem se varujejo tajni podatki do določene stopnje tajnosti. Varnostno dokumentacijo (načrt varovanja sistema, ocena varnostnih tveganj, varnostna navodila za delo) in drugo relevantno dokumentacijo (poročilo o izvedenih meritvah zaščite prostorov pred neželenim elektromagnetnim sevanjem, potrdilo o varnostni ustreznosti kriptografske rešitve, potrdila o zaščiti sestavin sistema pred neželenim elektromagnetnim sevanjem) je v postopku varnostnega vrednotenja sistema potrebno posredovati oziroma dati na vpogled nacionalnemu varnostnemu organu. V kolikor se v sistemu obravnavajo tajni potki stopnje tajnosti ZAUPNO ali višje je varnostno dokumentacijo potrebno minimalno označiti s stopnjo tajnosti INTERNO. Izjema so operativna varnostna navodila za delo uporabnikov v sistemu.

K 65. členu

V tem členu je določeno katere ključne sestavine vsebuje načrt varovanja in jih je potrebno zajeti v dokumentu in sicer opis sistema, načrt sestavin in povezav sistema, varnostne zahteve sistema, varnostna okolja, varnostne protiukrepe in varnostno upravljanje sistema. V prilogi 10 te uredbe je nadalje razdelana struktura vsebine načrta varovanja sistema, ki se izdela v začetni fazi načrtovanja in izgradnje ter dopolnjuje skozi celoten življenjski cikel sistema.

K 66. členu

V tem členu je določeno katere ključne sestavine vsebuje ocena varnostnih tveganj in jih je potrebno zajeti v dokumentu in sicer prepoznavanje in oceno tveganj in njihovih posledic, načrtovanje ukrepov in odgovornosti za varnostna tveganja ter spremljanje in poročanje o obvladovanju varnostnih tveganj. V prilogi 11 te uredbe je nadalje razdelana struktura vsebine ocene varnostnih tveganj, ki se izdela v začetni fazi načrtovanja in izgradnje ter dopolnjuje skozi celoten življenjski cikel sistema. Prav tako

je določeno, da se preostala varnostna tveganja, ki jih ni mogoče odpraviti ali zmanjšati po izvedbi vseh ukrepov, potrebno dosledno upravljati. Nacionalni varnostni organ v sodelovanju z organom pristojnim za kibernetsko varnost vodi seznam groženj in ranljivosti sistemov.

K 67. členu

V tem členu je določeno katere ključne sestavine vsebujejo varnostna navodila za delo v sistemu in jih je potrebno zajeti v dokumentu in sicer določitev varnostnega upravljanja in organiziranost varnosti sistema, načrtovanje ukrepov ob nepredvidenih dogodkih, upravljanje in spreminjanje konfiguracije/nastavitev sistema. Varnostna navodila za delo v sistemu se pripravijo za uporabnike in upravljavce sistema. Podrobneje je vsebina razdelana v Prilogi 12 te uredbe.

K 68. členu

Člen določa, da nacionalni varnosti organ pred izdajo dovoljenja za delovanje sistema v katerem se varujejo tajni podatki, opravi varnostno vrednotenje sistema na organu ali organizaciji. Varnostni pregled, se opravi ob navzočnosti vodje informacijskega sistema in vodje informacijske varnosti organa oz. organizacije in drugih oseb, odgovornih za varnost sistema (skrbnik sistema, upravljavec sistema, skrbnik kriptografskega materiala itd.), s katerim se preveri izpolnjevanje vseh ukrepov in postopkov za zagotovitev varnega delovanja sistema v skladu s predloženo varnostno dokumentacijo in zakonskimi ter podzakonskimi predpisi s področja varovanja tajnih podatkov in drugimi relevantnimi zakonskimi in podzakonskimi predpisi.

K 69. členu

Člen določa, da organ ali organizacija mora izvesti ponovni postopek varnostne odobritve sistema v primeru spremembe sistema, ki bi imela posledice za varnost v sistemu obravnavanih tajnih podatkov (dodajanje, zamenjava ključne programske oziroma strojne opreme, sprememba lokacije, vdor v sistem, sum kibernetskega napada na sistem….) oziroma kadar sistem več ne izpolnjuje minimalnih pogojev za varnostno delovanje sistema. Le to mora sporočiti nacionalnemu varnostnemu organu in posredovati vlogo za ponovni postopek pridobitve varnostnega dovoljenja za delovanje sistema.

XII. NEŽELENO ELEKTROMAGNETNO SEVANJE

K 70. členu

Člen določa, da vse sestavine sistemov, v okviru katerih se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje, morajo biti zaščitene proti neželenemu elektromagnetnemu sevanju (TEMPEST). Le-to se pojavlja v obliki elektromagnetnega valovanja, ki ga oddajajo komunikacijsko-informacijske naprave med obratovanjem. Ti moteči signali omogočajo nenadzorovano odtekanje tajnih podatkov iz sistema, zato je treba vse elemente sistemov, v okviru katerih se obravnavajo podatki stopnje tajnosti ZAUPNO, TAJNO in STROGO TAJNO, zaščititi proti temu neželenemu elektromagnetnemu sevanju. Člen tudi določa, da Ministrstvo za obrambo, Policija, Slovenska obveščevalno varnostna agencija ali drugi organ, ki ga pooblasti nacionalni varnostni organ, opravlja meritve neželenega elektromagnetnega sevanja.

XIII. KRIPTOGRAFIJA

K 71. členu

Člen opredeljuje celotni življenjski cikel kriptografske rešitve namenjene varovanju tajnih podatkov. Pobude za zasnovo kriptografske rešitve dajejo državni organi glede na svoje potrebe. Pri razvoju in nadgradnjah kriptografskih rešitev nacionalni varnostni organ sodeluje z državnimi organi in z zunanjimi izvajalci. Za varovanje tajnih podatkov v sistemih je dovoljeno uporabljati kriptografske rešitve, za katere je bilo izdano potrdilo o varnostni ustreznosti. Za varovanje drugih občutljivih podatkov (osebni podatki, davčna tajnost, …) v sistemih pa je take kriptografske rešitve dovoljeno uporabljati le izjemoma s predhodno odobritvijo nacionalnega varnostnega organa. Člen uvaja periodični nadzor nad varnostno ustreznost kriptografskih rešitev glede na stopnjo tajnosti tajnih podatkov v sistemih. Varnostna ustreznost se lahko v nekaterih primerih (na primer v primeru varnostnih incidentov, naknadno ugotovljenih varnostnih ranljivosti in podobno) preveri tudi pred iztekom v členu določenih obdobij.

K 72. členu

Podan je natančen opis dveh skupin kriptografskih algoritmov.

K 73. členu

Člen določa organe pristojne za izdajo potrdil o varnostni ustreznosti kriptografske rešitve ter obliko potrdila. Hkrati s potrdilom o varnostni ustreznosti mora pristojni organ izdati tudi minimalne varnostne zahteve za označevanje, distribucijo in uporabo kriptografske rešitve.

K 74. členu

Člen podrobneje določa začetek postopka ugotavljanja ustreznosti kriptografske rešitve. Pristojni predlagatelj, v skladu z zakonom je to ministrstvo, pristojno za javno upravo, ministrstvo, pristojno za notranje zadeve, ministrstvo, pristojno za obrambo, ministrstvo, pristojno za zunanje zadeve ali Slovenska obveščevalno-varnostna agencija, poda pisno vlogo na obrazcu, katere vsebina je predpisana v Prilogi 15 te uredbe in v kateri predlagatelj izpolni del A. Vlogi je potrebno priložiti ustrezno število kosov predlagane kriptografske rešitve za namene ugotavljanja varnostne ustreznosti in dokumentacijo, ki je predpisana v Prilogi 16 te uredbe. Člen podrobneje predpiše obvezne dele dokumentacije za kriptografske rešitve v sistemih, v katerih se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višjih stopenj tajnosti.

K 75. členu

Člen podrobneje opredeli priznavanje potrdil o varnostni ustreznosti kriptografskih rešitev
tujih držav in mednarodnih organizacij. Če se bodo tuje kriptografske rešitve uporabile v sistemih za varovanje tajnih podatkov stopnje tajnosti INTERNO, lahko nacionalni varnostni organ izda potrdilo na podlagi enakovrednega potrdila o varnostni ustreznosti kriptografske rešitve drugega nacionalnega organa za komunikacijsko varnost države članice EU, zveze NATO ali mednarodnih organizacij, katerih članica je Republika Slovenija. Pri tem postopek ugotavljanja varnostne ustreznosti kriptografske rešitve ni

potreben. Če se bodo tuje kriptografske rešitve uporabile v sistemih za varovanje tajnih podatkov stopnje tajnosti ZAUPNO ali TAJNO, mora nacionalni varnostni organ izvesti postopek ugotavljanja varnostne ustreznosti kriptografske rešitve. V sistemih za varovanje tajnih podatkov stopnje tajnosti TAJNO izključno tujih kriptografskih rešitev ni dovoljeno uporabljati. Člen uvaja izjemo, ko je dovoljeno uporabljati tuje tajne rešitve za varovanje tajnih podatkov stopnje tajnosti TAJNO in sicer takrat, ko enakovredna nacionalna rešitev ne obstaja in ima tuja kriptografska rešitev potrdilo o varnostni ustreznosti za varovanje tajnih podatkov EU ali zveze NATO najmanj stopnje tajnosti enakovredne stopnji tajnosti TAJNO. Priznavanje potrdil o varnostni ustreznosti tujih kriptografskih rešitev v sistemih za varovanje tajnih podatkov stopnje tajnosti STROGO TAJNO ni opredeljeno, saj ni dovoljeno.

K 76. členu

Člen podrobneje opredeljuje postopek ugotavljanja ustreznosti kriptografske rešitve za varovanje tajnih podatkov glede na stopnjo tajnosti tajnih podatkov v sistemu. V tem členu je opredeljen tudi postopek ugotavljanja varnostne ustreznosti drugih rešitev, ki niso nujno kriptografske, a so ključne za zagotavljanje varnosti. V tem smislu člen govori o rešitvah na osnovi fizikalnih pojavov ali fizikalnih lastnostih (diode in podobno) ali o drugih neopredeljenih rešitvah.

K 77. členu

Člen podrobneje opredeljuje začetek postopka ugotavljanja ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve. Na predlog organa lahko proizvajalec izvede posodobitve kriptografske naprave ter tako zagotovi optimalno delovanje naprave v spreminjajočem se digitalnem svetu. Pred vsako spremembo kriptografske naprave mora pristojni organ podati predlog s katerim začne postopek ugotavljanja varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve za varovanje tajnih podatkov. Predlog poda na predpisanem obrazcu, katerega vsebina je predpisana v Prilogi 15 te uredbe in v katerem predlagatelj izpolni del B.

K 78. členu

Člen določa, da morajo biti kriptografske rešitve v sistemih za varovanje tajnih podatkov stopnje tajnosti TAJNO in STROGO TAJNO zasnovane ne samo na abstraktnem (logičnem) nivoju, temveč tudi na mehanskem (strojnem) nivoju.

K 79. členu

Člen opredeljuje priporočila, dolžnosti in naloge proizvajalca v življenjskem ciklu kriptografske rešitve.

K 80. členu

Člen opredeljuje uporabo kriptografskih algoritmov glede na stopnjo tajnosti podatkov v sistemu. V kriptografskih rešitvah za varovanje tajnih podatkov stopnje tajnosti INTERNO ali ZAUPNO se dovoli uporaba tistih kriptografskih algoritmov, za katere nacionalni varnostni organ presodi, da so primerni za uporabo. V kriptografskih rešitvah za varovanje tajnih podatkov stopnje tajnosti TAJNO je zahtevana uporaba kriptografskih algoritmov I. nivoja. Izključno v primeru, da ustrezna nacionalna

kriptografska rešitev ne obstaja, je moč odstopati od predhodne zahteve. V kriptografskih rešitvah za varovanje tajnih podatkov stopnje tajnosti STROGO TAJNO se zahteva uporaba kriptografskih algoritmov I. nivoja.

K 81. členu

Člen določa, da mora hkrati s potrdilom o varnostni ustreznosti pristojni organ za vsako kriptografsko rešitev izdati tudi minimalne varnostne zahteve za označevanje, distribucijo in uporabo kriptografske rešitve. Pri tem se upošteva tudi varnostne zahteve, ki izhajajo iz članstva Republike Slovenije v mednarodnih organizacijah oziroma jih je Republika Slovenija sprejela s sklenitvijo drugih mednarodnih pogodb in sporazumov.

K 82. členu

Člen podrobneje določa postopek drugega vrednotenja ugotavljanja varnostne ustreznosti kriptografskih rešitev. Pri tem gre predvsem za gospodarsko ekonomski vidik, saj imamo kot država članica EU in zveze NATO preko postopka drugega vrednotenja ugotavljanja varnostne ustreznosti kriptografskih rešitev pomembno možnost nacionalne rešitve predstaviti ostalim državam članicam EU in zveze NATO. Pri tem povečujemo tržišče našim nacionalnim proizvajalcem kriptografskih rešitev ter njihovo prepoznavnost na trgih EU in zveze NATO. Splošna praksa večine držav članic EU in zveze NATO na tem področju je, da se za drugo vrednotenje ugotavljanja varnostne ustreznosti kriptografskih rešitev ne uporabijo enake rešitve, kot se uporabljajo v sistemih RS Slovenije, marveč le rešitve s pomembno spremenjenimi varnostnimi parametri. Zaradi obrambe nacionalne suverenosti RS Slovenije se enako določilo sprejme tudi v tem členu (četrti odstavek). Ravno tako se v fazi razvoja kriptografske rešitve lahko uporabljajo testni algoritmi določene družine algoritmov, razvite v državah članicah EU ali zvezi NATO, katere se pred dejansko uporabo kriptografske rešitve v sistemih za varovanje tajnih podatkov zamenja z netestno različico algoritma.

XIV. PREGLED TAJNIH PODATKOV

K 83. členu

Organ najmanj enkrat letno opravi inventuro prejetih in hranjenih tajnih podatkov EU in zveze NATO stopnje tajnosti TAJNO in STROGO TAJNO. Ob inventuri se preveri ali je dejansko stanje enako stanju zapisanem v evidenci ter ali se tajni podatki hranijo v ustreznem prostoru.

K 84. členu

Pred zaključkom delovnega razmerja mora vsak uslužbenec poskrbeti za varno predajo vseh dokumentov, ki so mu bili dodeljeni v obravnavo, pristojni osebi organa/organizacije oziroma pristojni organizacijski enoti v organu ali organizaciji.

S tem členom se zagotavlja da so nosilci tajnih podatkov pravočasno in ustrezno vrnjeni pristojnim osebam v organu/organizaciji.

XV. NAČRTI VAROVANJA

K 85., 86. in 87. členu

Členi določajo, da mora vsak organ in organizacija izdelati načrt varovanja tajnih podatkov v varnostnem območju ali skupini varnostnih območij, s katerim glede na vrsto in stopnjo tajnosti podatkov ter oceno ogroženosti podrobneje predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov v varnostnem območju. Ukrepi, ki morajo biti zajeti so taksativno našteti v tretjem odstavku 83. člena. Organ ali organizacija mora določiti odgovorno osebo za izdelavo načrta varovanja - nosilca načrta varovanja in njegovega namestnika, katerega naloga je tudi, da najmanj enkrat letno načrt pregleda in ga po potrebi popravi ali dopolni.

XVI. IZGUBA IN NEPOOBLAŠČENO RAZKRITJE TAJNEGA PODATKA

K 88. členu

Ta člen v skladu z varnostnimi politikami EU in zveze NATO predpisuje ukrepe in postopke ob primerih zlorabe tajnega podatka (uničenje, odtujitvijo ali drugi dogodek, ki kaže na zlorabo tajnega podatka). Zelo pomembno je, da je lastnik tajnega podatka ob eventualni zlorabi le tega obveščen, saj s pravočasno obveščenostjo lahko prepreči škodo, ki bi sicer lahko nastala, če o tem ne bi bil obveščen.

K 89. členu

V tem členu je določeno, katere podatke mora vsebovati obvestilo o zlorabi tajnega podatka.