

Uradni list Republike Slovenije



Internet: www.uradni-list.si

e-pošta: info@uradni-list.si

Št. **50** Ljubljana, ponedeljek **11. 4. 2022**

ISSN **1318-0576** Leto **XXXII**

VLADA

1070. Uredba o varovanju tajnih podatkov

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, 60/11 in 8/20) Vlada Republike Slovenije izdaja

UREDBO o varovanju tajnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

(vsečina 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 in organizacije pri obravnavanju tajnih podatkov (organizacijski ukrepi) ter ukrepov varovanja tajnih podatkov, varovanih prostorov ali objektov s tehničnimi sredstvi v skladu s to uredbo (tehnični ukrepi) vzpostavi sistem postopkov in ukrepov varovanja tajnih podatkov, ki ustreza stopnji tajnosti tajnih podatkov in stopnji tajnosti informacijskih sistemov ter onemogoča njihovo razkritje nepooblaščenim osebam.

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

3. člen

(pomen izrazov)

Izrazi, uporabljeni v tej uredbi, pomenijo:

1. javni prostor je prostor, dostopen vsem, v katerem se dogaja 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; sestavljajo ga programska, strojna, komunikacijska ter 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 sistemih zajema določanje in uporabo ukrepov varovanja tajnih podatkov, ki se obravnavajo prek 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. nosilec podatka je vsak medij, na katerem so zapisani podatki v fizični ali elektronski obliki;

6. 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, USB-ključ, CD/DVD-nosilec podatkov, zunanji disk in drugi);

7. 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 sestavine;

8. iznos podatka iz sistema pomeni tiskanje, shranjevanje na elektronski nosilec podatkov (USB-ključ, CD/DVD-nosilec podatkov, zunanji disk in drugi) ali izmenjavo z drugim sistemom prek medsebojne povezave sistemov;

9. neželeno elektromagnetno sevanje je sevanje, ki se nenadzorovano razširja in omogoča nepooblaščen seznanitev s tajnimi podatki;

10. 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 zmožljivostjo, rekonstrukcijo dogodkov in analizo;

11. razvid je namensko in sistematično spremljanje, beleženje ali vodenje podatkov;

12. preostalo tveganje je tveganje, ki v sistemu ostane tudi po izvajanju varnostnih ukrepov;

13. kriptografija je znanstvena veda, ki se ukvarja s konstrukcijo in analizo kriptografskih prvin in protokolov, ki pripomorejo k zagotavljanju zaupnosti, celovitosti, pristnosti in nezatajljivosti podatkov;

14. kriptografski algoritem je končno zaporedje pravil ali ukazov, ki sosledje bitov, kar pomeni čistopis, pretvori v drugo sosledje, ki je neberljivo sporočilo;

15. kriptografske prvine so osnovni sestavni deli kriptografske rešitve;

16. overjanje je preverjanje pristnosti entitete;
 17. incident je vsak dogodek, ki bi lahko imel škodljiv učinek na varovanje tajnih podatkov v sistemih.

II. DOLOČANJE IN OZNAČEVANJE TAJNIH PODATKOV

4. člen

(določanje tajnih podatkov)

Pooblaščen oseba, določena v 10. členu zakona, s pisno oceno, glede na možne škodljive posledice, podatkom določi ustrezno stopnjo tajnosti. V pisni oceni se opredelijo razlogi 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 v skladu z rokom hrambe tajnega podatka pri organu, ki je določil stopnjo tajnosti.

6. člen

(označevanje tajnih podatkov)

(1) Vsak dokument, nosilec podatkov in ključna sestavina sistema morajo biti ob določitvi stopnje tajnosti vidno označeni s predpisanimi oznakami stopnje tajnosti. Vsi dokumenti morajo imeti na vseh straneh dokumenta, v glavi in nogi označeno stopnjo tajnosti vključno z zunanji strani 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, natisnjena, 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 naslov označi v skladu z 8. členom te uredbe.

(3) Če spremni dopis ne vsebuje tajnih podatkov, se praviloma 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 ovojju, mora biti ta označen z ustrezno stopnjo tajnosti.

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

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

(7) Če je tajnost podatka določil organ, ki ni skrbnik sistema, mora imeti prikaz oznako tega organa.

(8) Vsi dokumenti, ki vsebujejo tajne podatke, morajo poleg oznak, določenih v tem členu, vsebovati sklic na dokument in datum dokumenta iz 4. 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;
- število morebitnih prilog.

(10) Vsi dokumenti, označeni s stopnjo tajnosti STROGO TAJNO, se poleg oznak, določenih 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. Poleg izvirne oznake se lahko na dokument vpiše tudi primerljiva stopnja tajnosti tajnega podatka v slovenskem jeziku.

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 dela besedila;

– se v prostor za dodatne oznake vpiše, da so odstavki ali deli odstavkov ali posamezne besede označeni z različno stopnjo tajnosti.

(2) Pooblaščen 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 preklicuje, se na dokumentu ali nosilcu podatkov, ki vsebuje tajni podatek, prečrtajo prvotne oznake tajnosti, pod staro oznako ali nad njo pa se navede nova oznaka stopnje tajnosti ali preklic stopnje tajnosti. Poleg navedenih oznak se na dokumentu navede še sklic na pisno obrazložitev spremembe ali preklica stopnje tajnosti. Namenski program 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, označenih 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) Pooblaščen 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 napišejo 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 pooblaščen oseba organa, ki je določila stopnjo tajnosti, izloči te podatke iz dokumenta.

(2) Iz dokumenta, iz katerega so bili v skladu s prejšnjim odstavkom izločeni tajni podatki, se odstranijo oznake stopenj tajnosti.

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

(4) Izločanje oziroma odstranjevanje tajnih podatkov iz dokumentov pomeni, da se besedilo prekrije in se ohrani originalna oblika dokumenta.

III. OBRAVNAVA IN HRAMBA TAJNIH PODATKOV

12. člen

(obravnavanje tajnih podatkov)

(1) Tajni podatki stopnje tajnosti INTERNO se obravnava v upravnem območju. Tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti se obravnava v varnostnem območju, ki je glede na način obravnavanja tajnih podatkov uvrščen v varnostno območje I. ali II. stopnje.

(2) Ne glede na prejšnji odstavek se lahko tajni podatki stopnje tajnosti ZAUPNO in TAJNO obravnava v upravnem območju pod pogoji, določenimi s to uredbo.

(3) Ne glede na prvi in drugi odstavek tega člena se tajni podatki do vključno stopnje tajnosti TAJNO lahko obravnava tudi izven varnostnega in upravnega območja pod pogoji, določenimi s to uredbo.

(4) Kadar je tajni podatek do vključno stopnje tajnosti TAJNO zaradi izvedbe točno določene naloge treba izjemoma obravnava 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, določeni s to uredbo.

(5) Kadar začasnega upravnega ali varnostnega območja iz tehničnih, organizacijskih in drugih razlogov ni mogoče vzpostaviti, se tajni podatki lahko obravnava pod pogoji, določenimi v 15. členu te uredbe.

13. člen

(vzpostavitev začasnega upravnega območja)

(1) Predstojnik organa ali oseba, ki jo ta pooblasti, mora za vzpostavitev začasnega upravnega območja izdelati dokument, v katerem se opredelijo:

- obseg začasnega upravnega območja;
- način varovanja;
- režim vstopa in izstopa;
- drugi potrebni ukrepi ob izrednih dogodkih (za primer požara, vloma, potresa ipd.).

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

14. člen

(vzpostavitev začasnega varnostnega območja)

(1) Predstojnik organa ali oseba, ki jo ta pooblasti, mora za vzpostavitev začasnega varnostnega območja izdelati dokument, v katerem se opredelijo:

- obseg začasnega varnostnega območja;
- način varovanja;
- režim vstopa in izstopa;
- ocena varnostnih tveganj obravnave tajnih podatkov;
- drugi potrebni ukrepi ob izrednih dogodkih (za primer požara, vloma, potresa ipd.).

(2) Zagotoviti je treba 24-urno neposredno in neprekinjeno fizično varovanje začasnega varnostnega območja in okolice ter kontrolo vstopa oziroma preverjanje identitete vsto-

pajočih. Fizično varovanje se lahko dopolni s prvinami tehničnega varovanja.

(3) Pred vzpostavitvijo začasnega varnostnega območja se opravi protiprisluškovalni pregled prostorov.

(4) Tajni podatki stopnje tajnosti ZAUPNO ali višje se hranijo v skladu s to uredbo.

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

15. člen

(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 obravnava le pod pogoji, določenimi v tem členu. Predstojnik organa ali oseba, ki jo ta pooblasti, določi, da se za izvedbo določenih nalog ali dogodkov tajni podatki stopnje tajnosti INTERNO, ZAUPNO in TAJNO obravnava izven upravnega in varnostnega območja.

(2) Tajnih podatkov ni dovoljeno obravnava na javnem prostoru oziroma na poti. Izjemoma se lahko tajni podatek do vključno stopnje tajnosti TAJNO obravnava izven upravnega in varnostnega območja, pri čemer je treba zagotoviti, da se s tajnim podatkom ne seznanijo nepooblaščen osebe ter da ima oseba tajni podatek ves čas pod nadzorom.

(3) Obravnavanje tajnih podatkov v sistemih 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.

(4) Vsak iznos ali vnos nosilca tajnega podatka zunaj upravnega in varnostnega območja se evidentira. Oseba, ki prevzame nosilec tajnega podatka, to potrdi s podpisom ter s tem prevzame odgovornost in skrb za varnost tajnih podatkov.

16. člen

(hramba tajnih podatkov)

(1) Tajni podatki stopnje tajnosti INTERNO se hranijo v upravnem območju v zaklenjenih pisarniških ali kovinskih omarah, ključki se hranijo ločeno. 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 v skladu z roki, določenimi s predpisi, ki urejajo poslovanje z dokumentarnim in arhivskim gradivom. Po preteku roka hrambe se izločijo in uničijo v skladu s 50. členom te uredbe.

(3) Ne glede na prejšnji odstavek centralna registra EU in Nata hranita tajne podatke največ dve leti od prejema. Po preteku omenjenega časa tajne podatke uničita v skladu s 50. členom te uredbe.

(4) Organizacije tajne podatke hranijo, dokler jih potrebujejo za opravljanje delovnih nalog. Po uporabi tajne podatke uničijo v skladu s 50. členom 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 varujejo tajni podatki stopnje tajnosti ZAUPNO ali višje stopnje tajnosti tako, da lahko že sam vstop v varnostno območje omogoča dostop do teh podatkov. V varnostnem območju I. stopnje se izvajajo najmanj naslednji varnostni postopki in ukrepi:

- jasno določen in varovan obseg območja, v katerem se zagotavlja nadzor nad vstopom ali izstopom oseb in vozil v

to območje, dovoljuje vstop samo osebam, ki imajo dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti in imajo dovoljenje za vstop v to območje;

– vodenje razvida tajnih podatkov, ki se v varnostnem območju hranijo na način, da se oseba z njimi seznani že ob samem vstopu v to območje;

– prepoved vnosa mehanskih, elektronskih in magnetno optičnih sestavnih delov, s katerimi je mogoče tajne podatke nepooblaščenoma posneti, odnesti ali prenesti, oziroma kakršnihkoli 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 je varnostno območje, 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) Okoli varnostnega območja I. stopnje ali na poti, ki vodi v tako varnostno območje, se vzpostavi upravno območje.

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

(4) Predstojnik organa določi osebe, ki lahko samostojno vstopajo v varnostno območje I. stopnje.

(5) 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 prejšnjega odstavka. Oseba iz prejšnjega odstavka mora pred vstopom osebe brez ustreznega dovoljenja poskrbeti, da bodo tajni podatki umaknjeni oziroma da bo preprečeno, da bi se oseba brez ustreznega dovoljenja seznanila s tajnim podatkom.

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 omogočata 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:

a) jasno določen in varovan obseg območja, v katerem se zagotavlja nadzor nad vstopom in izstopom oseb in vozil in dovoljuje vstop v to območje samo osebam, ki imajo dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti in imajo dovoljenje za vstop v to območje;

b) 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 četrtega odstavka tega člena;

c) organiziranost 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;

d) druge osebe organa ali organizacije, ki niso na seznamu iz četrtega odstavka tega člena, vstopajo v varnostno območje samo v spremstvu oseb iz četrtega 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;

e) 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 je varnostno območje;

f) prepoved vnosa mehanskih, elektronskih in magnetno optičnih sestavnih delov, s katerimi je mogoče tajne podatke nepooblaščenoma posneti, odnesti ali prenesti, oziroma kakršnihkoli naprav, s katerimi je mogoča zloraba tajnih podatkov. Izjemoma vnos in uporabo takih naprav odobri oseba, odgovorna za varnost varnostnega območja;

g) 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) Okoli varnostnega območja II. stopnje ali na poti, ki vodi v takšno varnostno območje, se vzpostavi upravno območje.

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

(4) Predstojnik organa določi osebe, 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 se zagotavlja, 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 EU in Nata)

(1) Centralna registra EU in Nata sta pristojna za varovanje tajnih podatkov EU in Nata stopnje tajnosti ZAUPNO in višje. Centralna registra EU in Nata varujeta tudi tajne podatke EU in Nata stopnje tajnosti INTERNO, če 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 Nata predstojnik organa določi pooblaščenega nadzorno osebo (Cosmic Control Officer /CCO/). Njene naloge so določene v varnostni politiki Nata.

21. člen

(podregistri EU in Nata ter kontrolne točke Nata)

(1) Podregistri in kontrolne točke so pristojni za varovanje tajnih podatkov EU in Nata stopnje tajnosti ZAUPNO in višjih stopenj tajnosti znotraj posameznih organov. Podregistri in kontrolne točke lahko varujejo tudi tajne podatke EU in Nata stopnje tajnosti INTERNO, če 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 predhodnega ogleda, ki ga opravi nacionalni varnostni organ. Nacionalni varnostni organ opravi ogled na podlagi vloge, v kateri je treba predložiti tudi načrt varovanja. Z ogledom se preveri, ali postopki in ukrepi tehničnega in fizičnega varovanja ter organiziranost 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 organiziranost 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 Nata, ki je vzpostavljena za varovanje tajnih podatkov do vključno stopnje tajnosti STROGO TAJNO, predstojnik organa določi pooblaščenega nadzornega osebo (Cosmic Control Officer CCO). Njene naloge so določene v varnostni politiki Nata.

22. člen

(oprema varnostnega in upravnega območja)

Oprema varnostnega in upravnega območja ter preostali pogoji, ki jih morajo izpolnjevati upravna in varnostna območja, so določeni 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 organiziranost 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 organiziranost varovanja, ki mora biti določena v načrtu varovanja, načrt pa mora biti izdelan pred ogledom. Pri vzpostavitvi upravnega območja v organih ogled ni potreben.

(3) Organ ali organizacija mora pred določitvijo varnostnega območja pridobiti soglasje 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 predhodnega ogleda, ki ga opravi v ta namen.

25. člen

(označevanje varnostnih in upravnih območij)

(1) Oseba, ki vstopi v varnostno območje, mora biti o tem nedvoumno in jasno obveščena še pred vstopom.

(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 obve-

stila, 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, zadošča, da je območje oziroma stavba ali okoliš, v katerem je območje, označena s tablamami o imenu organa ali organizacije ter obvestilom 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 določen v Prilogi 3, ki je sestavni del te uredbe.

26. člen

(nadzor vhoda in izhoda v varnostna in upravna območja)

(1) Samostojen vstop pooblaščenih oseb v varnostno območje se nadzira z ugotavljanjem identitete vstopajoče osebe. Fizični ali videonadzor 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 prepoznavna 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 nadzora ter omejitve vstopa in gibanja v varnostnem in upravnem območju, kadar to zahteva ocena ogroženosti ali to določajo spremenjene varnostne razmere.

27. člen

(varovanje opreme)

(1) Varnostnotehnična oprema, nameščena v upravnih in varnostnih območjih, mora biti zavarovana tako, da je ne morejo uporabljati nepooblaščen 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, nameščene v upravno ali varnostno območje.

(2) Ne glede na prejšnji odstavek se ključne sestavine sistema lahko uporabljajo 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 preostali 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,
- pri spremembi zaposlenih v območju, če to zahteva ocena ogroženosti,
- po odločitvi predstojnika,
- najmanj vsakih 24 mesecev ali
- ob vzpostavitvi začasnega varnostnega območja.

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

(3) Ne glede na prejšnji odstavek protiprisluškovalni pregled varnostnih območij v Ministrstvu za obrambo ter organizacijah, ki zanj izvajajo naročila, izvede pristojna organizacijska enota Ministrstva za obrambo, v Slovenski obveščevalno-varnostni agenciji ter organizacijah, ki zanj izvajajo naročilo, pa notranja 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 vsaki od njih, 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 njej, in mora biti s tako stopnjo tajnosti tudi označena.

32. člen

(nastavitev kombinacij ključavnic za blagajne)

(1) Število oseb, seznanjenih s posameznimi kombinacijami ključavnic, mora biti čim manjše. Predstojnik organa ali organizacije oziroma oseba, ki jo ta pooblasti, to zagotovi z razporedom delovne naloge.

(2) Nastavitev 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, prepisuje ali skenira (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 izdelavo kopij, ki imajo lastnosti elektronske naprave, morajo izpolnjevati pogoje, ki 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 EU in Nata stopnje tajnosti ZAUPNO ali TAJNO se lahko kopira le v pristojnem registru ali podregistru ali kontrolni točki, ki je tajne podatke prejel, 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 pooblaščen oseba organa, v katerem mu je bila določena stopnja tajnosti. Izjema je tajni podatek Nata stopnje tajnosti STROGO TAJNO, katerega kopiranje lahko odobri pooblaščen oseba v centralnem registru.

34. člen

(prevajanje)

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

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

(3) 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. Poleg izvirne oznake se na dokument vpiše tudi prevedena primerljiva stopnja tajnosti tajnega podatka.

35. člen

(iznos tajnih podatkov iz sistema)

(1) Za vsak iznos tajnega podatka iz sistema je treba voditi ustrezní razvid, ki zagotavlja beleženje iznosa.

(2) Ne glede na prejšnji odstavek 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. Delovanje sistema mora zagotavljati, da lahko tajne podatke iz sistema iznaša le pooblaščen oseba.

VI. EVIDENTIRANJE

36. člen

(evidentiranje tajnih podatkov v registrskem sistemu)

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

(2) V evidenco iz prejšnjega odstavka se vpisujejo naslednji podatki, razen če jih tajni podatek ne vsebuje:

- a) evidenčna številka;
- b) datum dokumenta;
- c) številka dokumenta;
- d) naslov ali vrsta dokumenta (vabilo, zaprosilo, zapisnik, poročilo ipd.);
- e) stopnja tajnosti;
- f) številka kopije;
- g) datum prejema ali odpreme dokumenta;

- h) naslovnik (pri odpremi dokumenta);
- i) število strani;
- j) število prilog.

(3) Evidenca iz prvega odstavka tega člena se lahko nadomesti z evidenco iz 37. člena te uredbe.

37. člen

(evidentiranje tajnih podatkov)

(1) V evidenco tajnih podatkov se vpisujejo naslednji podatki, razen če jih tajni podatek ne vsebuje:

- a) evidenčna številka;
- b) datum dokumenta;
- c) številka dokumenta;
- d) naslov ali vrsta dokumenta (vabilo, zaprosilo, zapisnik, poročilo ipd.);
- e) stopnja tajnosti;
- f) številka kopije;
- g) subjekt dokumenta (pošiljatelj);
- h) prejemnik dokumenta (signirni znak) ali naslovnik (pri odpremi);
- i) datum prejema ali odpreme dokumenta;
- j) število strani;
- k) število prilog.

(2) Pri spremembi ali preklicu stopnje tajnosti mora biti z 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 dokumenti, ki so označeni s stopnjo tajnosti, ne skenirajo v sistem za evidentiranje tajnih podatkov.

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

38. člen

(seznam vpogledov)

(1) Vsak organ in organizacija, 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 ali 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 drugi odstavek 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 morajo biti razvidni:

- uporabniško ime;
- datum in čas seznanitve.

(5) Seznam vpogledov v sistemih se vodi 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 osebam, ki imajo dovoljenje za dostop do tajnih podatkov in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog.

(2) Če iz naslova ni možno razbrati posameznega prejemnika tajnega podatka, distribucijo tajnega podatka znotraj organa ali organizacije odredi predstojnik organa oziroma organizacije 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 oziroma organizaciji 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 v skladu z rokom hrambe tajnega podatka. Distribucijski seznam, oblikovan za dokumente, ki sodijo v skupno vsebinsko področje, se hrani trajno.

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

(4) Distribucijski seznam vsebuje vsaj naslednje podatke:

- oznako organa ali organizacijske enote ali centralnega registra ali organizacije,
- vsebinsko področje ali številko dokumenta in
- prejemnika 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. 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 do vključno stopnje tajnosti TAJNO zunaj upravnega območja lahko zunanjo ovojnico nadomesti zaklenjen ali zapečaten kovček, škatla ali torba.

(3) Pri prenosu tajnih podatkov stopnje tajnosti STROGO TAJNO zunaj upravnega območja mora biti notranja ovojnica v zaprtem kovčku, škatli ali torbi z zapiranjem na ključ ali šifrirno kombinacijo. Prenos opravi 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 oziroma organizacija mora določiti, kje se sprejemajo nosilci tajnih podatkov in kdo jih sprejema. Naslovnik ali oseba, pooblaščen za sprejem nosilcev tajnih podatkov, potrdi njihov prejem z vpisom v dostavno ali kurirsko knjigo oziroma na drug način potrdi prejem tajnega podatka.

(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 Republike Slovenije)

(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 se lahko prenašajo s kurirsko službo ali po lastni prenosni mreži (organa ali naročnika). Izjemoma se lahko opravi osebni prenos tajnega podatka do vključno stopnje tajnosti TAJNO, če ima oseba dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti in ob upoštevanju pogojev iz 46. člena te uredbe. Tak osebni prenos odobri predstojnik organa, če kurirska služba ni na voljo ali bi uporaba te službe

povzročila zamudo, ki bi imela škodljive posledice za delovanje države.

(2) Za prenos tajnih podatkov Nata stopnje tajnosti ZAU-PNO 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 pod pogoji iz prvega odstavka tega člena in ob upoštevanju pogojev iz 46. člena te uredbe. 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 ZAU-PNO 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 pod pogoji iz prvega odstavka tega člena in ob upoštevanju pogojev iz 46. člena te uredbe. Tajni podatki stopnje tajnosti INTERNO se lahko prenašajo s kurirsko službo, po lastni prenosni mreži 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 obveznosti, določenih v 41. členu 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 mednarodnem 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 kurirjem posameznih organov izdajo predstojniki teh organov. Obrazec kurirskega certifikata je objavljen na spletni strani nacionalnega varnostnega organa.

(4) Izjemoma je mogoč osebni mednarodni prenos tajnega podatka do vključno stopnje tajnosti TAJNO, in sicer s kurirskim certifikatom in pod pogoji iz prvega odstavka 42. člena ter ob upoštevanju pogojev iz 46. člena te uredbe.

44. člen

(kurirski prenos)

(1) Kurirji ter osebe, ki v organu opravljajo naloge lastne prenosne mreže (v nadaljnjem besedilu: 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 prenos 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 postopki 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 določen v Prilogi 5, ki je sestavni del te uredbe.

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

(3) Usposabljanji iz prvega in drugega odstavka tega člena izvajata Ministrstvo za obrambo in Policija, za kurirje Slovenske obveščevalno-varnostne agencije pa 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, 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 in bi prenos s kurirjem povzročil zamudo, ki bi imela škodljive posledice za delovanje države, se lahko izven upravnega ali varnostnega območja do vključno stopnje tajnosti TAJNO izjemoma opravi osebni prenos tajnega podatka.

(2) Osebni prenos lahko izvede oseba pod pogoji iz prvega odstavka 42. člena te uredbe.

(3) Pri osebnem prenosu skrb za varnost tajnega podatka prevzame oseba, ki prenaša tajne podatke.

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

(5) Ovojnice, v kateri se prenašajo tajni podatki, v času prenosa ni dovoljeno odpirati, prav tako tajnih podatkov v času prenosa 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, ki je v Prilogi 6, ki je sestavni del te uredbe.

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

48. člen

(pomoč drugih organov)

(1) Pooblaščen uradne osebe morajo osebi, ki prenaša tajne podatke in se izkaže z veljavnim pooblastilom, na njeno zaprosilo zagotoviti pomoč v obliki in obsegu, ki omogoča varovanje tajnih podatkov pred odtujitvijo, poškodovanjem ali uničenjem.

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

49. člen

(prenos tajnih podatkov v sistemih)

(1) Prenos tajnih podatkov v 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 nacionalni varnostni organ.

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) Če 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 mm². Za uničevanje tajnih podatkov stopnje tajnosti TAJNO in STROGO TAJNO v papirni obliki se uporablja rezalnik papirja, ki zagotavlja razrez papirja velikosti največ 5 mm².

(3) Če rezalnik papirja ne ustreza zahtevanim standardom iz prejšnjega odstavka, je treba zagotoviti nadaljnje uničenje razrezanih delcev, pri čemer se uporabijo metode, ki zagotovijo dokončno uničenje do neprepoznavnosti (npr. sežig, sulfadni postopek ali izdelava celuloze). Če se ta proces izvaja izven varnostnega oziroma upravnega območja, je treba zagotoviti, da je pri prevozu in dokončnem uničenju tajnih podatkov ves čas prisotna pooblaščen oseba.

(4) Organizacije tajne podatke, z izjemo tajnih podatkov tuje države, uničijo v skladu z določbami te uredbe. Če ne morejo zagotoviti ustreznih pogojev za uničevanje tajnih podatkov, tajne podatke vrnejo pošiljatelju.

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

(6) Kopije in dodatni izvodi dokumentov, ki vsebujejo tajne podatke in niso del zadeve organa, se izločijo in uničijo takoj po opravljeni delovni nalogi, za katero so bili izdelani, oziroma najpozneje ob predaji dokumentov v tekočo zbirko.

(7) Kopije dokumentov na nosilcih, ki vsebujejo tajne podatke in so namenjene izključno prenosu tajnih podatkov, se uničijo takoj po opravljeni delovni nalogi po postopku, določenem v Prilogi 9, ki je sestavni del te uredbe.

(8) Tajni podatki se hranijo v skladu z roki, določenimi s predpisi, ki urejajo poslovanje z dokumentarnim in arhivskim gradivom. Po preteku roka hrambe se izločijo in uničijo, razen če so v skladu s predpisi, ki urejajo poslovanje z dokumentarnim in arhivskim gradivom, določeni kot arhivsko gradivo. Pri izročitvi arhivskega gradiva s tajnimi podatki pristojnemu arhivu se upoštevajo predpisi, ki urejajo področje arhivske dejavnosti.

(9) Tajni podatki se izločajo in uničujejo komisijsko. Komisijo imenuje predstojnik organa oziroma organizacije ali oseba, ki jo predstojnik organa oziroma organizacije 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.

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

(11) Seznam vpogledov iz 38. člena te uredbe se priloži zapisniku o uničenju tajnega podatka.

(12) Kadar 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 ali prepisovanja ali fizično uničiti. Za opremo sistema, v katerem so se obravnavali tajni podatki stopnje tajnosti ZAUPNO ali višje, ponovna uporaba v druge namene ni možna.

(13) Uničenje tajnih podatkov v sistemih se izvaja s fizičnim uničenjem elektronskih nosilcev podatkov. Postopek fizičnega uničenja elektronskih nosilcev podatkov je določen v Prilogi 9 te uredbe.

(14) 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 naslednje odgovorne osebe za varovanje tajnih podatkov v sistemih:

- skrbnika sistema,
- 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 iz prvega odstavka tega člena obvesti nacionalni varnostni organ.

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

52. člen

(skrbnik sistema)

Skrbnik sistema:

- a) izvede postopek varnostne odobritve sistema,
- b) pripravi varnostno dokumentacijo,
- c) odloča o spremembah in dopolnitvah sistema,
- d) odloča, kdo in kako sme uporabljati sistem,
- e) odloča o uvedbi, upravljanju in vzdrževanju sistema,
- f) usmerja in izdaja navodila upravljavcu sistema za delovanje sistema,
- g) skrbi za obvladovanje varnostnih tveganj in obvladovanje preostalih tveganj,
- h) določa ukrepe za zaščito proti neželenemu elektromagnetnemu sevanju,
- i) izvaja nadzor nad pravilnim delovanjem sistema in
- j) spremlja vse posege v sistem.

53. člen

(upravljavec sistema)

(1) Upravljavec sistema:

- a) namešča, vzdržuje, konfigurira, integrira ter zagotavlja delovanje in razpoložljivost sistema,
- b) nudi pomoč uporabnikom sistema,
- c) spremlja varnostne dogodke in zaznava incidente v sistemu,
- d) poroča vodji informacijske varnosti sistema o zaznanih incidentih,
- e) skrbniku sistema poroča o vseh posegih v sistem in
- f) izvaja 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:

- načrtovanje ukrepov in postopkov varovanja tajnih podatkov v sistemih in njihov nadzor,
- obravnavo zaznanih incidentov v sistemih ter 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 kriptografskega materiala v skladu 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 državne 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 obveščevalne in varnostne 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 je pristojna Slovenska obveščevalno-varnostna agencija.

(4) Usklajevanje 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 treba 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 pravice po vedenju.

(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) Kadar 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 določa 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 ipd.).

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.

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 (npr.: prekinitve delovnega razmerja, premestitev in podobno) mora biti varnostna shema ustrezno popravljena in sprememba ustrezno dokumentirana.

60. člen

(spremljanje in nadzor vstopa v sistem in dostopa do tajnih podatkov)

(1) Spremljanje in nadzor vstopa v sistem 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 določijo način nadzora in spremljanja vseh izvedbenih in kontrolnih posegov v sistem ter pooblaščenosti izvajalci 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) Zapis o posegih v sistem se morajo hraniti dokler se sistem uporablja za varovanje tajnih podatkov.

(5) Vsak vstop v sistem, v katerem se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje, mora biti zabeležen (revizijska sled). Čas hrambe revizijske sledi se določi na podlagi predpisov, ki urejajo področje ravnanja z dokumentarnim gradivom. 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 v skladu s postopki in merili za povezovanje sistemov, v katerih se varujejo tajni podatki, ki so določeni v Prilogi 10, 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 pregleda 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 predpisi s 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, določeni v Prilogah 11, 12 in 13, ki so sestavni deli te uredbe.

(3) Postopek varnostnega vrednotenja sistema obsega:

- pregled in oceno varnostne dokumentacije,
- pregled sistema na lokaciji organa ali organizacije in
- izdajo 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 predloži pristojnemu organu tuje države ali mednarodne organizacije.

64. člen

(dokumenti, potrebni za izvedbo varnostnega vrednotenja sistema)

(1) Pred postopkom varnostnega vrednotenja sistema in izdaje varnostnega dovoljenja organ ali organizacija izdela varnostno dokumentacijo, v kateri opiše sistem, opredeli varnostne zahteve, oceni varnostna tveganja sistema, določi varnostne ukrepe za njegovo zaščito ter določi odgovorne osebe za varno delovanje sistema.

(2) Varnostna dokumentacija obsega:

- načrt varovanja sistema,
- oceno varnostnih tveganj in
- varnostna navodila za delo v sistemu.

(3) V postopku varnostnega vrednotenja sistema je treba nacionalnemu varnostnemu organu poslati ali dati na vpogled tudi drugo dokumentacijo, ki jo potrebuje (npr. 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, na podlagi ustrezne ocene možnih škodljivih posledic označi vsaj s stopnjo tajnosti INTERNO. Varnostna navodila za delo so lahko brez stopnje tajnosti.

(5) Ne glede na drugi odstavek 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, določena 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 procesu 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 ter njihovih posledic, načrtovanje 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 metodologija, določena v Prilogah 11, 12 in 13 te uredbe.

(3) Preostala 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 skrbno načrtovana in vodena.

(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 ter nastavitve 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 v organu ali organizaciji, s katerim preveri izpolnjevanje vseh ukrepov in postopkov za zagotovitev varnega delovanja sistema v skladu s predloženo varnostno dokumentacijo in predpisi s področja varovanja tajnih podatkov in drugimi predpisi.

(2) V okviru varnostnega vrednotenja se opravi varnostni pregled sistema, s katerim se preveri izvajanje 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 ter drugih oseb, odgovornih za varnost sistema (skrbnik sistema, upravljavec sistema, skrbnik kriptografskega materiala itn.).

69. člen

(ponovni postopek varnostnega vrednotenja sistema)

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

(2) Ponovni postopek varnostnega vrednotenja sistema se izvede ob vsaki spremembi sistema, ki povzroča ali bi lahko povzročila posledice glede varnosti v sistemu obravnavanih tajnih podatkov. Upravljavec ali skrbnik sistema sporoči nacionalnemu varnostnemu organu spremembo in predloži vlogo za ponovni postopek varnostnega vrednotenja sistema.

(3) Ob ugotovitvi upravljavca, skrbnika sistema ali nacionalnega varnostnega organa, da sistem več ne izpolnjuje minimalnih fizičnih, organizacijskih in tehničnih ukrepov ter postopkov za varovanje tajnih podatkov do določene stopnje tajnosti, se izvede ponovni 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 elektromagnetnemu sevanju.

(2) Ukrepi za zaščito pred neželenim elektromagnetnim sevanjem morajo zajemati izbor in način namestitve vseh sestavin sistema glede na stopnjo tajnosti podatkov v sistemu

in glede na rezultate opravljenih meritev elektromagnetnega sevanja iz prostorov, kjer so ali bodo sestavine nameščene. Postopki za zaščito pred neželenim elektromagnetnim sevanjem so v Prilogi 8, ki je sestavni del te uredbe. Vlada podrobneje predpiše merila in navodila za zaščito pred neželenim elektromagnetnim sevanjem v sistemih.

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

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

(5) Stopnjo ogroženosti prostorov z vidika izvajanja zaščite proti neželenemu elektromagnetnemu sevanju določijo organi, določeni v prejšnjem odstavku.

XIII. KRIPTOGRAFIJA

71. člen

(razvoj, uporaba in preverjanje ustreznosti 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, namenjenih varovanju tajnih podatkov.

(3) Za varovanje tajnih podatkov v sistemih je dovoljeno uporabljati kriptografske rešitve, za katere je izdano potrdilo o varnostni ustreznosti. Izjemoma se lahko kriptografske rešitve, za katere je izdano potrdilo o varnostni ustreznosti, uporabljajo tudi v druge namene, vendar je predhodno treba pridobiti soglasje nacionalnega varnostnega organa.

(4) Nacionalni varnostni organ obdobjno 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.

(5) Varnostna ustreznost se lahko preveri tudi pred iztekom obdobja iz prejšnjega odstavka.

72. člen

(klasifikacija kriptografskih algoritmov)

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

(2) Kriptografski algoritmi I. ravni 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. ravni so tudi algoritmi, pridobljeni na podlagi mednarodnih sporazumov. Kriptografski algoritmi I. ravni se uporabljajo za varovanje tajnih podatkov stopnje tajnosti TAJNO ali STROGO TAJNO.

(3) Kriptografski algoritmi II. ravni so 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 so predlagane kriptografske rešitve ustrezne. 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.

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, ki je v Prilogi 16, ki je sestavni del te uredbe. Vlogo predlagatelj na podlagi ocene možnih škodljivih posledic označi z ustrežno stopnjo tajnosti.

(2) Sestavna dela vloge iz prejšnjega odstavka sta:

- ustrežno število kosov predlagane kriptografske rešitve za namen ugotavljanja varnostne ustreznosti in
- dokumentacija o predlagani kriptografski rešitvi, ki jo predlagatelj na podlagi ocene možnih škodljivih posledic označi z ustrežno stopnjo tajnosti.

(3) Vsebinska dokumentacije iz druge alineje prejšnjega odstavka je določena v Prilogi 17, ki je sestavni del te uredbe.

(4) Pri ugotavljanju ustreznosti kriptografskih rešitev v sistemih, ki obravnavajo tajne podatke stopnje tajnosti ZAU-PNO ali višjih stopenj tajnosti, so obvezni del dokumentacije 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, Nata 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 kriptografskih rešitev iz prvega odstavka tega člena ni dovoljeno uporabljati.

(5) Ne glede na prejšnji odstavek se kriptografska rešitev iz prvega odstavka tega člena v sistemih, ki obravnavajo tajne podatke stopnje tajnosti TAJNO, izjemoma lahko uporabi, če nacionalna kriptografska rešitev ne obstaja in ima kriptografska rešitev potrdilo o varnostni ustreznosti za varovanje tajnih podatkov EU ali Nato najmanj stopnje tajnosti, enakovredne stopnji tajnosti TAJNO.

(6) V sistemih, ki obravnavajo tajne podatke stopnje tajnosti STROGO TAJNO, se smejo 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 njihovo izvedbo 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 izvedbe 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 podajo vlogo na predpisanem obrazcu, ki je v Prilogi 16 te uredbe.

77. člen

(postopek ugotavljanja varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve)

Postopek ugotavljanja varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve se izvede na predlog organa, če 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, ki je v Prilogi 16 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 kriptografske rešitve mora skrbeti za varnost dobavne verige tako, da se zmanjša verjetnost kompromitacije varnostno pomembnih strojnih in programskih komponent.

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

(3) Proizvajalec kriptografske rešitve mora spremljati strokovna dognanja o morebitnih ranljivostih uporabljenih algoritmov in njihovega izvajanja. To vključuje tako kriptografske kot preostale strojne in programske komponente. O morebitnih ranljivostih nemudoma poroča 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. ravni.

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

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

(3) 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 Nata. Podlaga za izvedbo drugega vrednotenja je potrdilo o varnostni ustreznosti kriptografskih rešitev za varovanje tajnih podatkov in pisni predlog 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 dejansko stanje začeti postopek ugotavljanja ustreznosti kriptografske rešitve za varovanje tajnih podatkov EU ali Nata.

(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, lahko opravi tudi nacionalni varnostni organ.

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

(4) Pisni predlog za postopek drugega vrednotenja pri pristojnih organih EU ali Nata 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 tajnih podatkov EU in Nata)

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

(2) Centralna registra EU in Nata vsako leto do 1. februarja pozove vse podregistre in kontrolne točke, da jima poročajo

o številu prejetih in uničenih tajnih podatkov 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 organizacijski enoti, ki je pristojna za hrambo tajnih podatkov, 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, izdelata 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 izdelata 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:

a) opis in značilnosti varnostnega območja;

b) ukrepe fizičnega varovanja (zunanje in notranje fizično varovanje, varnostne točke z opisi nalog izvajalcev);

c) ukrepe tehničnega varovanja (zunanje in notranje tehnično varovanje, nadzor nad vstopom in izstopom, alarmni sistem in postopki ob sprožitvah posameznih stopenj alarmov, dokumentiranje);

d) postopke ob nasilnem vstopu in nepredvidenem dogodku: požaru, potresu, povodnji in drugih naravnih nesrečah;

e) postopke in ukrepe ob izgubi, razkritju ali odtujitvi tajnega podatka;

f) podatke o drugih ukrepih in postopkih varovanja tajnih podatkov (opravljanje vzdrževalnih in drugih del v varnostnih območjih);

g) podatke o nosilcu načrta varovanja – osebi, ki je odgovorna za izdelavo načrta varovanja;

h) podatke o preventivnih varnostnih ukrepih za osebe, ki dostopajo do tajnih podatkov (evidence usposabljanj, postopki ob zaznavah groženj, notranji nadzor);

i) ukrepe in postopke poostrenega nadzora oziroma omejitev vstopa in gibanja v varnostnem in upravnem območju, kadar to zahteva ocena ogroženosti ali to določajo spremenjene varnostne razmere.

(4) Vsak organ ali organizacija določi 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 se stalno dopolnjuje, najmanj enkrat letno pa pregleda in preveri 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 razkritjem tajnih podatkov, njihovim uničenjem, izgubo, odtujitvijo, poškodovanjem ali kakršnikoli drugim dogodkom, ki kaže na zlorabo tajnih podatkov (v nadaljnjem besedilu: zloraba tajnega podatka), je treba takoj seznaniti predstojnika organa oziroma organizacije ali osebo, ki jo ta pooblasti, in zagotoviti vse ukrepe za preprečitev nadaljnje zlorabe tajnega podatka in izsleditev 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 oceni morebitna škoda za interese Republike Slovenije oziroma za delovanje organa. V preiskavi se določijo ukrepi, ki jih je treba izvesti za odpravo škodljivih posledic in preprečitev vnovične zlorabe.

(5) Če zloraba tajnega podatka kaže na sum storitve kazniviga 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 EU in Nata ter pristojni inšpektorat v Republiki Sloveniji.

89. člen

(obvestilo o zlorabi tajnega podatka)

Obvestilo o zlorabi tajnega podatka iz prejšnjega člena 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, organ, 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;

– podatke o tem, ali je bil organ, ki je podatek določil za tajnega, obveščen;

– postopke in ukrepe, ki so bili izvedeni za preprečitev nadaljnje zlorabe tajnih podatkov.

XVII. PREHODNE IN KONČNE DOLOČBE

90. člen

(uskladitev obstoječih kriptografskih rešitev)

Obstoječe kriptografske rešitve, ki imajo veljavno dovoljenje za obravnavanje tajnih podatkov stopnje tajnosti TAJNO

in STROGO TAJNO, se v petih letih od uveljavitve te uredbe uskladijo s 75. členom te uredbe.

91. člen

(uskladitev načrtov varovanja)

Organi in organizacije načrte varovanja, izdelane v skladu z 32. členom Uredbe o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11, 24/11), uskladijo s to uredbo v enem letu od njene uveljavitve.

92. člen

(uničenje tajnih podatkov v centralnih registrih EU in Nata)

Centralna registra EU in Nata tajne podatke, ki jih ob uveljavitvi te uredbe hranita več kot dve leti, uničita v skladu s to uredbo v enem letu od uveljavitve te uredbe.

93. člen

(uskladitev evidenc tajnih podatkov)

Evidence tajnih podatkov se uskladijo s 36. in 37. členom te uredbe v enem letu od uveljavitve te uredbe.

94. člen

(distribucijski seznam centralnih registrov EU in Nata)

Distribucijski seznam centralnih registrov EU in Nata iz tretjega odstavka 40. člena te uredbe določi vlada v šestih mesecih od uveljavitve te uredbe.

95. člen

(prilagoditev upravnih in varnostnih območij)

Pogoji, ki jim mora ustrezati varnostno-tehnična oprema upravnih in varnostnih območij iz 22. člena te uredbe, morajo biti vzpostavljeni v dveh letih od uveljavitve te uredbe.

96. člen

(izpolnjevanje pogojev za uporabo naprav za izdelavo kopij)

Naprave za izdelavo kopij, ki imajo lastnosti elektronske naprave iz 33. člena te uredbe, morajo izpolnjevati pogoje za varovanje tajnih podatkov v dveh letih od uveljavitve te uredbe.

97. člen

(določitev odgovornih oseb sistema)

Predstojnik določi odgovorne osebe iz 51. člena te uredbe v šestih mesecih od uveljavitve te uredbe.

98. člen

(določitev meril in navodil za zaščito pred neželenim elektromagnetnim sevanjem)

Do sprejetja meril in navodil za zaščito pred neželenim elektromagnetnim sevanjem v sistemih iz drugega odstavka 70. člena te uredbe se uporabljajo predpisi EU ali Nata.

99. 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, iz 80. člena te uredbe v šestih mesecih od uveljavitve te uredbe.

100. člen

(sprejetje sklepa o varovanju kriptografskega materiala)

Vlada sprejme sklep o varovanju kriptografskega materiala iz 55. in 56. člena te uredbe v enem letu od uveljavitve te uredbe.

101. člen

(prenehanje veljavnosti)

Z dnem uveljavitve 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).

102. člen

(začetek veljavnosti)

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

Št. 00701-31/2021

Ljubljana, dne 7. aprila 2022

EVA 2021-1535-0001

Vlada Republike Slovenije

Janez Janša
predsednik

Priloga 1: Vzorci oznak stopnje tajnosti INTERNO, ZAUPNO, TAJNO IN STROGO TAJNO

INTERNO

Ocena možnih škodljivih posledic:
[Vnesite besedilo]



REPUBLIKA SLOVENIJA
NAZIV ORGANA

ulica, kraj

T:
F:
E:

[Naslovnik]

— Številka: *[številka]*
Datum: *[datum]*

Zadeva: *[zadeva]*

[Besedilo]

S spoštovanjem.

Pripravil/a:
[Ime in priimek]
[naziv]

[Ime in priimek]
[naziv]

ZAUPNO

Ocena možnih škodljivih posledic:
[Vnesite besedilo]



REPUBLIKA SLOVENIJA
NAZIV ORGANA

T:
F:
E:

[Naslovník]

Številka: [številka]
Datum: [datum]

Zadeva: [zadeva]

[Besedilo]

S spoštovanjem.

Pripravi/a:
[Ime in priimek]
[naziv]

[Ime in priimek]
[naziv]

Ocena možnih škodljivih posledic – pri dokumentu organa, ki je podatku določil stopnjo tajnosti

ZAUPNO

Številka izvoda: [št]
Število prilog: [št]
Ocena možnih škodljivih posledic:
[Vnesite besedilo]

TAJNO



REPUBLIKA SLOVENIJA
NAZIV ORGANA

ulica, kraj

T:
F:
E:

[Naslovnik]

Številka: [številka]
Datum: [datum]

Zadeva: [zadeva]

[Besedilo]

S spoštovanjem.

Pripravi/a:
[Ime in priimek]
[naziv]

[Ime in priimek]
[naziv]

Številka izvoda: [št]
Število prilog: [št]
Ocena možnih škodljivih posledic:
[Vnesite besedilo]

STROGO TAJNO

REPUBLIKA SLOVENIJA
NAZIV ORGANA

ulica, kraj

T:
F:
E:

[Naslovnik]

[zadeva]

Številka: [številka]

Datum: [datum]

Zadeva: [zadeva]

[Besedilo]

S spoštovanjem.

Pripravil/a:

[Ime in priimek]

[naziv]

[Ime in priimek]

[naziv]

Priloga 2: Pogoji za upravna in varnostna območja v organih in organizacijah**MINIMALNI POGOJI, KI JIM MORA USTREZATI VARNOSTNO-TEHNIČNA
OPREMA UPRAVNEGA OBMOČJA****Sistem protivlomnega varovanja**

Če objekt oziroma kompleks, v katerem so prostori upravnega območja, ni neposredno in neprekinjeno fizično varovan, morajo biti prostori upravnega območja, kadar se v njih ne nahajajo zaposleni, varovani s sistemom za samodejno zaznavanje gibanja oseb, ki mora ustrezati najmanj standardu SIST EN 50131 razreda 2 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Sistemi za prenos alarmnega signala

Alarmni signal se mora prenašati po nadzorovani naročniški liniji. Čas prenosa od nastanka do prikaza alarma v varnostno-nadzornem centru mora ustrezati najmanj standardu SIST EN 50136 razreda M 3 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Sistem za prenos alarmnega signala mora omogočati periodično preverjanje zaznave napake med naročniškim modulom in nadzornim centrom najmanj v skladu s standardom SIST EN 50136 razred T4 ali drugim primerljivim standardom, katerega skladnost preverja nacionalni varnostni organ.

Če se upravno območje vzpostavlja v tujini, se uporablja predpisani standard, če je to tehnično izvedljivo, če ni, se uporablja rešitev, ki zagotavlja podobne možnosti prenosa alarmnega signala na pooblaščen varnostno-nadzorni center v državi gostiteljici.

Sistem kontrole pristopa

Na vhodu ali izhodu upravnega območja se izvaja identifikacija zaposlenih oseb in vozil. Obiskovalce je ob vstopu treba ustrezno evidentirati. Obiskovalci se v upravnem območju lahko gibajo samo v spremstvu stalno zaposlenega osebja.

Če se nadzor vstopa in izstopa izvaja izključno s sistemom elektronske pristopne kontrole, mora ustrezati najmanj standardu SIST EN 50133 razreda 3, kategorija pristopa B ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Vrata

Na vhodu v upravno območje ali v prostor znotraj upravnega območja, kjer se hranijo tajni podatki stopnje tajnosti INTERNO, morajo biti nameščena masivnejša vrata, ki se zaklepajo (polna lesena vrata, kovinska vrata ipd.). V primeru zasteklitve mora biti steklo neprebojno, ojačeno s kovinsko mrežo ali protivlomno folijo. Ustreznost vrat po potrebi preverja nacionalni varnostni organ.

MINIMALNI POGOJI, KI JIM MORA USTREZATI VARNOSTNO-TEHNIČNA OPREMA VARNOSTNEGA OBMOČJA

Sistem protivlomnega varovanja

Prostori varnostnega območja se, kadar se v njih ne nahaja stalno zaposleno osebje, opremijo s sistemom za samodejno zaznavanje gibanja oseb, ki mora ustrezati najmanj standardu SIST EN 50131 razreda 3 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ, in mora biti vključen vedno, ko v prostoru ni pooblaščenih oseb.

Sistemi za prenos alarmnega signala

Alarmni signal se mora prenašati po nadzorovani naročniški liniji. Čas prenosa od nastanka do prikaza alarma v varnostno-nadzornem centru mora ustrezati najmanj standardu SIST EN 50136 razreda M 4 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Sistem za prenos alarmnega signala mora omogočati občasno preverjanje prenosne poti in zaznavo napake med naročniškim modulom in nadzornim centrom najmanj v skladu s standardom SIST EN 50136 razred T 5 ali drugim primerljivim standardom, katerega skladnost preverja nacionalni varnostni organ.

Če se varnostno območje vzpostavlja v tujini, se uporablja predpisani standard, če je to tehnično izvedljivo, če ni, se uporablja rešitev, ki zagotavlja podobne možnosti prenosa alarmnega signala na pooblaščen varnostno-nadzorni center v državi gostiteljici.

Sistem kontrole pristopa

Sistem pristopne kontrole na vhodu v varnostno območje mora ustrezati najmanj standardu SIST EN 60839-11-1 oziroma SIST EN 60839-11-2 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Zidovi

Zunanji zidovi varnostnega območja morajo biti iz armiranega betona debeline 150 mm ali drugega materiala enake mehanske trdnosti. Če je varnostno območje vzpostavljeno v 2. nadstropju ali višje, je debelina zunanjih zidov varnostnega območja lahko 100 mm armiranega betona ali drugega materiala enake mehanske trdnosti. Če je zagotovljeno neposredno in neprekinjeno fizično varovanje varnostnega območja ali objekta, v katerem se varnostno območje nahaja, so lahko zidovi nižje mehanske trdnosti.

Notranji zidovi varnostnega območja (ki mejijo na upravno območje) morajo biti iz armiranega betona debeline 100 mm ali drugega materiala enake mehanske trdnosti. Če je zagotovljeno neposredno in neprekinjeno fizično varovanje varnostnega območja ali objekta, v katerem se varnostno območje nahaja, so lahko zidovi nižje mehanske trdnosti.

Dele zunanjih zidov varnostnega območja, za katerimi je prostor, ki ga organ ali organizacija, ki vzpostavlja varnostno območje, ne upravlja oziroma ga ne nadzira, je treba opremiti s tipali alarmne naprave, ki zaznavajo tresenje in ustrezajo najmanj standardu SIST EN 50131 razreda 3 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Protivlomna vrata

Protivlomna vrata morajo imeti vsaj tritočkovno zapiranje in morajo ustrezati standardu SIST EN 1627 stopnje 4. Če je zagotovljeno neposredno in neprekinjeno fizično varovanje varnostnega območja ali objekta, v katerem se varnostno območje nahaja, se lahko vgradijo protivlomna vrata, ki ustrezajo standardu SIST EN 1627 najmanj stopnje 2 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Varnostna ključavnica

Zunanji del protivlomnih vrat se opremi s slepo kljuko in protivlomno zaščito ključavnice.

Na protivlomnih vratih se namesti cilindrični vložek za ključavnico po standardu SIST EN 1303, ki mora ustrezati mehanski odpornosti stopnje 2 ali drugemu primerljivemu standardu, katerega skladnost preverja nacionalni varnostni organ.

Samodejno zapiralo

Protivlomna vrata se opremijo s samodejnim zapiralom, ki zagotavlja, da se zapirajo za vsakim posameznim odpiranjem.

Okna

Okna morajo biti opremljena tako, da preprečujejo nepooblaščen vpogled v prostor.

Na okna varnostnega območja, ki mejijo na nenadzorovano površino, se do višine 5,5 m namestijo varnostne rešetke, tako, da so vzdane ali pritrjene z notranje strani oken. Izdelane morajo biti iz jeklenih elementov premera najmanj 20 mm ali drugega materiala enake mehanske trdnosti. Razmik med elementi rešetk ne sme biti večji od 150 mm. Zasteklitev se prelepi s protivlomno folijo debeline vsaj 200 mikronov. Namesto varnostnih rešetk se lahko vgradijo protivlomna okna z zasteklitvijo po standardu SIST EN 356 razreda P 8 B ali drugem primerljivem standardu, katerega skladnost preverja nacionalni varnostni organ, ali pa se na zunanji strani oken namestijo aktivni fotoelektrični IR-detektorji.

Če so okna od zunaj nedostopna in več kot 5,5 m nad nenadzorovano površino, se uporabi protivlomna folija debeline vsaj 200 mikronov.

Če je zunanost objekta z varnostnim območjem fizično varovana, se do višine 5,5 m nad terenom okno zaščiti z jekleno varnostno rešetko z elementi premera vsaj 12 mm, uporabijo se protivlomna okna z zasteklitvijo po standardu SIST EN 356 razreda P 6 B ali drugem primerljivem standardu, katerega skladnost preverja nacionalni varnostni organ ali pa se na zunanji strani oken namestijo aktivni fotoelektrični IR-detektorji. Zasteklitev se prelepi s protivlomno folijo debeline vsaj 175 mikronov.

Prezračevanje in zajem zraka

Površina s prezračevalnim oziroma klimatizacijskim sistemom povezanih odprtin za prezračevanje, ki sega iz varnostnega območja, ne sme biti večja od 200 cm². Če so odprtine za prezračevanje večje, je treba nanje namestiti varnostno rešetko, ki mora biti privarjena ali pritrjena z notranje strani, odprtine varnostne rešetke pa ne smejo biti večje od 200 cm².

Odprtina za zajem zraka se izdelata ali zavaruje tako, da se nepooblaščenim osebam onemogoči dostop. Odprtina se zaščiti z varnostno mrežo, katere odprtine ne smejo biti večje od 200 cm².

Klimatska naprava

Zunanji del klimatske naprave za zajem zraka in izpust vode mora biti ustrezno zavarovan tako, da se onemogoči nepooblaščen dostop do naprave in prenos zvoka iz varnostnega območja.

Zvočna izolacija prostora

Če se v prostoru obravnavajo tajni podatki tudi v zvočni obliki (sestanki, videokonference, telefonski pogovori ipd.), je treba prostor ustrezno zvočno izolirati (zvočno tesnjenje oz. dušenje vrat, oken, prezračevalnega sistema).

Blagajne in varnostne ključavnice

Tajni podatki stopnje tajnosti ZAUPNO in TAJNO se v varnostnem območju II. stopnje, in po potrebi v varnostnem območju I. stopnje, hranijo v blagajnah po standardu SIST EN 1143 protivlomne stopnje 2 ali drugem primerljivem standardu, katerega skladnost preverja nacionalni varnostni organ.

Tajni podatki stopnje tajnosti STROGO TAJNO se v varnostnem območju II. stopnje, in po potrebi v varnostnem območju I. stopnje, hranijo v blagajnah po standardu SIST EN 1143 protivlomne stopnje 3 ali drugem primerljivem standardu, katerega skladnost preverja nacionalni varnostni organ.

Na blagajnah mora biti nameščena elektronska ali mehanska ključavnica po standardu SIST EN 1300 razreda B ali drugem primerljivem standardu, katerega skladnost preverja nacionalni varnostni organ.

Blagajne za hrambo ključev

Ključki varnostnega območja se hranijo v posebni blagajni po standardu vsaj SIST EN 1143 protivlomne stopnje 1 ali drugem primerljivem standardu, katerega skladnost preverja nacionalni varnostni organ, ki mora biti nameščena v upravnem območju ali prostoru, ki je neprekinjeno fizično ali tehnično varovan.

Na blagajni iz prejšnjega odstavka mora biti nameščena elektronska ključavnica po standardu SIST EN 1300 razreda B ali drugem primerljivem standardu, katerega skladnost preverja nacionalni varnostni organ.

Za shranjevanje ključev varnostnih območij se lahko namesto blagajn uporabi elektronski sistem za shranjevanje ključev (ključar), ki mora biti nameščen v upravnem območju ali prostoru, ki je neprekinjeno fizično ali tehnično varovan.

Rezalnik papirja

Za uničevanje tajnih podatkov stopnje tajnosti INTERNO in ZAUPNO v papirni obliki se uporablja rezalnik papirja, ki ustreza varnostnemu razredu SIST EN 15713, in zagotavlja razrez v skladu z drugim odstavkom 50. člena te uredbe. Za uničevanje tajnih podatkov stopnje tajnosti TAJNO in STROGO TAJNO v papirni obliki se uporablja rezalnik papirja, ki ustreza varnostnemu razredu SIST EN 15713, in zagotavlja razrez v skladu z drugim odstavkom 50. člena te uredbe.

Prostor za odlaganje elektronskih naprav in prtljage

Ob vhodu v varnostno območje I. stopnje in varnostno območje II. stopnje je treba namestiti omarice za shranjevanje mobilnih aparatov, torb in drugih naprav, ki se v varnostno območje ne smejo vnašati.

Detektorska vrata za odkrivanje nevarnih stvari

Ob vhodu v varnostno območje I. stopnje morajo biti nameščena detektorska vrata za odkrivanje orožja, kovin in mehanskih, elektronskih in magnetno optičnih sestavnih delov, s katerimi je mogoče tajne podatke nepooblaščenno posneti, odnesti ali prenesti.

Namesto z detektorskimi vrati se pregledi lahko opravljajo z ročnimi detektorji.

Če so detektorska vrata nameščena ob vhodu v objekt in osebo stalno spremljajo zaposleni, detektorskih vrat pred vhodom v I. varnostno območje ni treba nameščati.

Videonadzor in hramba videoposnetkov

Videonadzor mora pokrivati vse vhode in izhode v varnostna območja in mora zagotavljati ustrezno kakovost posnetka v vseh pogojih snemanja.

Snemalna naprava mora zagotavljati neprekinjeno snemanje in mora biti nameščena v varnostnem ali upravnem območju, do katerega imajo dostop samo za to pooblaščen osebe.

Posnetki videonadzora se hranijo najmanj trideset (30) dni. Do posnetkov imajo dostop samo za to pooblaščen osebe.

Priloga 3: Vzorec napisov za varnostno območje

Vzorec napisov za varnostno območje

VSTOPATE V VARNOSTNO OBMOČJE I. STOPNJE. IZVAJAJO SE PREDPISANI UKREPI. ENTERING CLASS I SECURITY AREA. OBLIGATORY SAFETY PROCEDURES AND MEASURES ARE BEING CARRIED OUT.
--

VSTOPATE V VARNOSTNO OBMOČJE II. STOPNJE. IZVAJAJO SE PREDPISANI UKREPI. ENTERING CLASS II SECURITY AREA. OBLIGATORY SAFETY PROCEDURES AND MEASURES ARE BEING CARRIED OUT.
--

Priloga 5: Program usposabljanja kurirjev

1. ZAKONODAJA – predstavitev zakonskih aktov ter internih predpisov, navodil in drugih vsebin, ki se nanašajo na varovanje in prenos podatkov
2. SPECIALNI DEL (teorija):
 - varnostna kultura,
 - samozaščitni ukrepi,
 - načini prenosa pošte,
 - prenos pošte za lastno uporabo (npr. udeležba na sestankih),
 - načrt varovanja prenosa pošte,
 - opredelitev postopkov in preventivnih ukrepov za prenos pošte,
 - komunikacija z uradnimi osebami drugih organov (npr. policija),
 - prenos pošte v tujino,
 - sredstva in oprema za prenos pošte,
 - ukrepi ob zlorabi podatkov,
 - najbolj pogoste napake pri prenosu pošte,
 - primeri iz prakse.
3. PRAKTIČNI DEL:
 - simulacija prenosa pošte (peš ali z vozilom),
 - spremstvo prenosa pošte (peš ali z vozilom),
 - ugotavljanje in preprečevanje sledenja (peš ali z vozilom),
 - izvajanje samozaščitnih ukrepov,
 - ukrepi in postopki ob zlorabi podatkov, fizičnem napadu na kurirja,
 - obveščanje, ravnanje s komunikacijskimi sredstvi,
 - osnove samoobrambe.
4. VARNA VOŽNJA:
 - vizualni varnostni pregled vozila,
 - pregled vozila s tehničnimi pripomočki,
 - odpravljanje osnovnih napak na vozilu,
 - osnove varne vožnje,
 - ukrepi ob nesrečah, napadu na vozilo ipd.

Priloga 6: Pooblastilo za prenos (OBR-KU)

<Glava organa/organizacije>

Številka: [številka]

Datum: [datum]

Na podlagi drugega odstavka 47. člena Uredbe o varovanju tajnih podatkov (Uradni list RS, št. 50/22) izdajam osebi:

ime: _____

priimek: _____

datum rojstva: _____

POOBLASTILO ZA PRENOS TAJNIH PODATKOV

Imenovani/a je v skladu z 22. členom Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20) varnostno preverjen/a in ima dovoljenje za dostop do tajnih podatkov stopnje tajnosti _____ številka _____, ki ga je izdalo _____ z veljavnostjo od _____ do _____.

Pooblastilo za prenos tajnih podatkov do stopnje tajnosti _____ velja do _____.

OPOZORILO:

Policisti morajo osebi, ki prenaša tajne podatke in se izkaže s tem pooblastilom, na njeno zaprosilo zagotoviti pomoč v obliki in obsegu, ki omogoča varovanje tajnih podatkov pred odtujitvijo, poškodovanjem ali uničenjem.

Pooblaščen delavci iz prejšnjega odstavka nimajo pravice do vpogleda v vsebino tajnih podatkov. Cariniki pri postopkih, ki jih izvajajo v skladu s svojimi pooblastili, nimajo pravice do vpogleda v vsebino tajnih podatkov, ko se oseba izkaže s tem pooblastilom.

Predstojnik organa

Priloga 7: Pooblastilo za prenos (OBR-OP)

<Glava organa/organizacije>

Številka: [številka]

Datum: [datum]

Na podlagi tretjega odstavka 47. člena Uredbe o varovanju tajnih podatkov (Uradni list RS, št. 50/22) izdajam osebi:

ime: _____

priimek: _____

datum rojstva: _____

POOBLASTILO ZA PRENOS TAJNIH PODATKOV

Imenovani/a je v skladu z 22. členom Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20) varnostno preverjen/a in ima dovoljenje za dostop do tajnih podatkov stopnje tajnosti _____ številka _____, ki ga je izdalo _____ z veljavnostjo od _____ do _____.

Pooblastilo velja za prenos tajnih podatkov št. _____ stopnje tajnosti _____.

OPOZORILO:

Policisti morajo osebi, ki prenaša tajne podatke in se izkaže s tem pooblastilom, na njeno zaprosilo zagotoviti pomoč v obliki in obsegu, ki omogoča varovanje tajnih podatkov pred odtujitvijo, poškodovanjem ali uničenjem.

Pooblaščen delavci iz prejšnjega odstavka nimajo pravice do vpogleda v vsebino tajnih podatkov. Cariniki pri postopkih, ki jih izvajajo v skladu s svojimi pooblastili, nimajo pravice do vpogleda v vsebino tajnih podatkov, ko se oseba izkaže s tem pooblastilom.

Predstojnik organa

Priloga 8: Postopki za zaščito pred neželenim elektromagnetnim sevanjem v sistemih

Pomen izrazov

Izrazi, uporabljeni v tej prilogi, pomenijo:

- neželeno elektromagnetno sevanje je sevanje naprav, ki so del sistema, in se nenadzorovano razširja in tako omogoča odtekanje tajnih podatkov,
- zaščita pred neželenim elektromagnetnim sevanjem je vrsta ukrepov, s katerimi se preprečuje ali bistveno zmanjšuje neželeno elektromagnetno sevanje,
- pojem zaščita pred neželenim elektromagnetnim sevanjem zajema raziskave in preučevanje neželenega elektromagnetnega sevanja, pa tudi vrste ukrepov za njegovo preprečevanje oziroma zmanjšanje,
- gradnik je vsaka naprava, priprava ali del instalacije, ki je sestavni del sistema, v katerem se obravnava tajni podatki stopnje tajnosti ZAUPNO ali višje.

Uporaba in dostop do meril in navodil

Do sprejetja ustreznih nacionalnih meril in navodil se uporabljajo dokumenti EU ali Nata.

Pri uporabi meril in navodil je treba zagotoviti, da:

- imajo dostop do teh navodil samo tisti, ki jih nujno potrebujejo za izvajanje svoje naloge po načelu »potrebe po seznanitvi«,
- imajo uporabniki ali prejemniki navodil ustrezno dovoljenje za dostop do tajnih podatkov,
- je vzpostavljeno ustrezno upravno ali varnostno območje.

Označevanje opreme

Vsa delujoča oprema razen kriptografske, za varovanje tajnih podatkov stopnje tajnosti ZAUPNO ali višje v elektronski obliki mora imeti ustrezno potrdilo o zaščiti pred neželenim elektromagnetnim sevanjem in biti ustrezno označena z nalepko, na kateri je navedena stopnja te zaščite.

Označevanje opreme in izdajanje potrdil o zaščiti pred neželenim elektromagnetnim sevanjem je v pristojnosti za to pooblaščenih laboratorijev. Pri nabavi te opreme mora skrbnik ali upravljavec sistema (naročnik) opozoriti izvajalca naročila, da mu obvezno predloži potrdilo o zaščiti pred neželenim elektromagnetnim sevanjem.

Potrdila o zaščiti pred neželenim elektromagnetnim sevanjem so del dokumentacije, na podlagi katere se pridobiva varnostno dovoljenje za delovanje sistema.

Če je nalepka, s katero se preprečuje nedovoljen poseg v to opremo, poškodovana, potrdilo o zaščiti pred neželenim elektromagnetnim sevanjem ni več veljavno in opremo ni več dovoljeno uporabljati za varovanje tajnih podatkov stopnje tajnosti ZAUPNO ali višje.

Dolžnost izvajanja varnostnih postopkov ravnanja z opremo

Upravitelj sistema mora uporabnike sistema in tehnično osebje, odgovorno za upravljanje in vzdrževanje sistema in infrastrukture, seznaniti z varnostnimi postopki ravnanja z opremo, zaščiteni pred neželenim elektromagnetnim sevanjem.

Vsak uporabnik sistema, vodje projektov in izvajalci del pri projektih, nosilci upravljanja in vzdrževanja sistemov, upravljavci in vzdrževalci elektroenergetske in druge infrastrukture, povezane z informacijsko-komunikacijsko infrastrukturo za prenos tajnih podatkov, morajo izvajati varnostne postopke ravnanja z opremo.

Pristojnost spreminjanja sestave in gradnikov informacijskega sistema

Sestave informacijskega sistema oziroma premeščanja gradnikov, ki imajo potrdilo o zaščiti pred neželenim elektromagnetnim sevanjem, ni dovoljeno spreminjati. Prav tako niso dovoljeni drugi posegi v to opremo, ki bi lahko povečali ogroženost na področju zaščite pred neželenim elektromagnetnim sevanjem.

Ob morebitni potrebi po spremembi sestave sistema in posameznih njegovih gradnikov lahko dovoli spremembo vodja informacijske varnosti za sistem ali oseba, ki jo pooblasti, ali v njegovi odsotnosti upravitelj sistema.

Vsaka sprememba mora biti ustrezno dokumentirana v tehnični dokumentaciji.

Priloga 9: Navodilo za uničenje in ponovno uporabo elektronskih nosilcev tajnih podatkov

Fizično uničenje elektronskih nosilcev tajnih podatkov

Fizično uničenje elektronskega nosilca pomeni, da rekonstrukcija tajnih podatkov z elektronskega nosilca ne sme biti mogoča.

Fizično uničenje elektronskih nosilcev tajnih podatkov opravi organ ali organizacija sama. Če nima ustreznih pogojev za uničenje, jih fizično uniči na komisijskem uničevanju blaga pri ustreznih ponudnikih storitev.

Elektronski nosilci tajnih podatkov se uničujejo komisijsko. Komisijo imenuje predstojnik organa ali oseba, ki jo predstojnik organa za to pooblasti. V komisiji so najmanj tri osebe, med katerimi mora biti oseba, odgovorna za varovanje tajnih podatkov. O uničenju tajnih podatkov komisija pripravi zapisnik. Zapisnik se hrani trajno.

Elektronski nosilci podatkov, ki so dotrajani ali v okvari oziroma kakor koli drugače poškodovani, se fizično uničijo.

Metode fizičnega uničenja elektronskih nosilcev tajnih podatkov

Z metodami fizičnega uničenja elektronskih nosilcev tajnih podatkov se uničijo vsi elektronski nosilci ne glede na strukturo medija (magnetni trakovi, diskete, trdi disk idr.).

Za fizično uničenje posameznega nosilca elektronskih podatkov mora biti izbrana ustrezna metoda uničenja, s katero rekonstrukcija tajnih podatkov z elektronskega nosilca podatkov ni mogoča.

Metode fizičnega uničenja elektronskih nosilcev podatkov so:

- diskete: odstranitev nosilca iz ohišja, čemur sledi razrez v namenskem rezalniku,
- trdi diski: fizično uničenje v mlinu za kovine, zažig ali kemično uničenje,
- USB-ključ, SSD: lomljenje, uničenje v mlinu, zažig ali kemično uničenje,
- BD, DVD, CD, CD-RW, CD-R, CD-ROM: razrez z namenskim rezalnikom,
- magnetni trakovi: zažig ali kemično uničenje,
- razmagnetenje magnetnega medija.

Ponovna uporaba elektronskih nosilcev podatkov

Ponovna uporaba elektronskih nosilcev podatkov je dovoljena samo za elektronske nosilce podatkov, na katerih so se varovali tajni podatki stopnje tajnosti INTERNO.

Ponovna uporaba elektronskih nosilcev podatkov iz prejšnjega odstavka je dovoljena tudi izven organa.

Ponovna uporaba elektronskih nosilcev tajnih podatkov stopnje tajnosti ZAUPNO in višjih stopenj tajnosti izven organa ni dovoljena, znotraj organa pa je dovoljena v sistemih, za katere je bilo izdano varnostno dovoljenje, in se lahko ponovno uporabi za varovanje tajnih podatkov, kot mu je bilo v osnovi izdano varnostno dovoljenje.

Postopek uničenja tajnih podatkov na elektronskih nosilcih, namenjenih ponovni uporabi

Pred ponovno uporabo nosilca tajnih podatkov znotraj organa se podatki na elektronskih nosilcih uničijo s standardnimi postopki brisanja, ki jih omogočajo sistemi, na katerih se nosilci uporabljajo (brisanje, formatiranje ipd.).

Pred ponovno uporabo nosilca izven organa je treba za brisanje tajnih podatkov uporabiti namensko opremo ali postopke, ki večkratno prepišejo/izbrišejo podatke na elektronskih nosilcih in tako zagotavljajo, da podatkov ni možno rekonstruirati. Vsak sektor elektronskega nosilca je prepisan najmanj trikrat z različnimi bitnimi vzorci.

Tajni podatki na elektronskih nosilcih, namenjenih ponovni uporabi, se uničujejo komisijsko. Komisijo imenuje predstojnik organa ali oseba, ki jo predstojnik organa za to pooblasti. V komisiji so najmanj tri osebe, med katerimi mora biti oseba, odgovorna za varovanje tajnih podatkov. O uničenju tajnih podatkov komisija pripravi zapisnik. Zapisnik se hrani trajno.

Priloga 10: Postopki in merila za povezovanje sistemov

Pri povezovanju sistemov na mednarodni ravni se upoštevajo tudi navodila, ki se uporabljajo na podlagi mednarodnih pogodb ali sprejetih mednarodnih obveznosti.

Ti postopki in merila ne zajemajo izmenjave informacij z uporabo izmenljivih elektronskih nosilcev podatkov.

Pomen izrazov, uporabljenih v tej prilogi

Izrazi, uporabljeni v tej prilogi, pomenijo:

- OSI – (Open System Interconnection) je referenčni model oziroma nabor internetnih protokolov, opredeljenih v standardu ITU-T X.200;
- SMZ – storitev mejne zaščite (angl. Boundary Protection Service – BPS) je varnostna storitev na vseh OSI plasteh, ki zmanjšuje varnostna tveganja zaradi povezovanja sistemov. SMZ je praviloma sestavljen iz večjega števila EMZ;
- EMZ – prvina mejne zaščite (angl. Boundary Protection Component – BPC) na vseh OSI plasteh je programska ali strojna rešitev, ki zagotavlja SMZ. Primeri EMZ, ki ga je odobril pristojni organ, so antivirusni program, požarna pregrada, usmerjevalnik, kriptografska rešitev, enosmerna podatkovna dioda in podobni;
- enosmerna podatkovna dioda – tako podatki kot tok podatkov prek te rešitve potekajo izključno enosmerno (vključno s potrditvenim signalom ACK, ki ga pri tej povezavi ni);
- VPN (angl. Virtual Private Network) – navidezno zasebno omrežje;
- izjava o skladnosti – izjava upraviteljev sistemov o skladnosti povezave sistemov z varnostnimi zahtevami;
- varnostno dovoljenje za delovanje povezave – potrdilo o izvajanju vseh ukrepov in postopkov za zagotovitev varnega delovanja povezave sistemov;
- uporabnik je oseba, ki ima v enem od sistemov uporabniški račun.

Zahteva za povezavo

Za povezavo dveh ali več sistemov je predhodno potreben tehten poslovni ali operativni razlog, ki mora biti pisno opredeljen v Operativni zahtevi za povezavo (v nadaljnjem besedilu: OZP).

V OZP se opredelijo poslovne, operativne in tehnične zahteve, ki vsebujejo:

- razloge za takšno povezavo in pričakovane koristi,
- zahtevo po izmenjavi informacij,
- ravni in načine povezave na vseh OSI plasteh za potrebe opredelitve SMZ in EMZ,
- obstoječo infrastrukturo, pomembno za medsebojno povezovanje
- stopnje tajnosti varovanih tajnih podatkov,
- skupnost uporabnikov in
- privilegije uporabnikov.

V OZP (za vsak sistem posebej ali enoten za vse sisteme, ki se povezujejo) se posebej opredelijo odgovornosti in pristojnosti upravitelja SMZ.

OZP mora biti pregledana s strani vodij informacijske varnosti in upraviteljev prihodnjih povezanih sistemov ter odobrena s strani predstojnikov organov ali organizacij.

O vseh spremembah zahtev, opredeljenih v OZP, je treba obvestiti vse preostale upravitelje povezanih sistemov. Če pride do sprememb ali novih povezav z drugimi sistemi v enem od povezanih sistemov, je treba o tem obvestiti upravitelje preostalih povezanih sistemov.

Načrtovanje povezave

Ravni in načini povezave na vseh OSI plasteh, ki niso opredeljeni v OZP, niso dovoljeni in jih mora SMZ onemogočati.

Vsak sistem mora poskrbeti za lastno zaščito nasproti drugemu. Pri tem mora sistem, s katerim se povezuje, obravnavati kot potencialno varnostno grožnjo.

Za izbiro, namestitve in upravljanje povezovalnih prvin posameznega sistema sta odgovorna upravljavca sistemov.

Vsaka zahteva, postavljena drugemu sistemu, mora biti dokumentirana v izjavi o skladnosti.

Upravljevec mora upravljati in vzdrževati svoj del povezave tako, da se zagotovi njeno pravilno in varno delovanje.

Upravljavca se morata med seboj predhodno obveščati o spremembah posameznih sistemov, ki bi lahko vplivale na varnostna tveganja ali delovanje povezave. V takih primerih je treba obnoviti postopke iz operativnih zahtev za povezavo.

Varnost pretoka podatkov se zagotavlja s SMZ, ki še zagotavlja najnižje dopustno sprejemljivo tveganje za povezane sisteme.

Z medsebojno povezavo se lahko namestijo, konfigurirajo in uporabljajo le protokoli, mrežne storitve in toki podatkov, potrebni za izvajanje OZP.

Povezovanje sistemov

Povezovanje sistemov je dovoljeno le v eni nadzorovani in varovani vstopno-izstopni točki, skozi katero potekajo vsi servisi in storitve.

Povezovanje sistemov, v katerem se varujejo tajni podatki, z drugim sistemom, je dovoljeno le, če je mednju nameščen SMZ.

SMZ in njegove nastavitve se določijo na podlagi Ocene varnostnih tveganj, da se tveganje zmanjša na najnižjo možno stopnjo.

V sistemu, kjer se varujejo tajni podatki različnih stopenj tajnosti, mora biti zagotovljeno, da podatki višje stopnje tajnosti ne morejo prehajati v sistem z nižjo stopnjo tajnosti.

Če sistem zagotavlja le komunikacijsko infrastrukturo za prenos tajnih podatkov in so podatki kriptirani s kriptografsko rešitvijo, za katero je bilo izdano potrdilom o varnostni ustreznosti v skladu s to uredbo, se takšna povezava ne šteje za medsebojno povezavo.

V postopku izdaje varnostnega dovoljenja za povezavo sistemov morajo upravljavci posameznih sistemov, v katerih se varujejo tajni podatki, pripraviti:

- oceno varnostnih tveganj,
- načrt varovanja povezave z opisom SMZ in EMZ.

V dokumentih morajo biti opisani tudi pogoji, pod katerimi se lahko povezava začasno odklopi ali se omeji njene storitve ter ukine povezava.

V okviru dokumentacije je treba obravnavati tudi vse že vzpostavljene povezave med sistemi.

Povezave med sistemi

Povezave med posameznimi sistemi glede na stopnjo tajnosti:

- sistemi, ki se povezujejo, so istih stopenj tajnosti,
- sistemi, ki se povezujejo, so različnih stopenj tajnosti,
- sistemi, brez stopenj tajnosti se povezujejo s sistemi s stopnjami tajnosti.

O medsebojni povezavi sistemov govorimo v primerih, ko se sistema razlikujeta najmanj v eni od naslednjih lastnosti:

- najvišja stopnja varovanih tajnih podatkov,
- varnostni način delovanja,

- upravitelj sistema in organ za varnostno odobritev sistema,
- varnostne zahteve in veljavna varnostna politika,
- drugi varnostni parametri (potreba po seznanitvi oz. interesni skupnosti, omejitve, posebni protokoli, stopnja fizične zaščite, vrsta nosilnega omrežja, lastništvo podatkov, ki se izmenjujejo).

Dodajanje novih komponent (npr. nova delovna postaja, nova omrežna oprema) že vzpostavljenemu sistemu, ki hkrati ne vplivajo na katero od lastnosti, naštetih v prejšnjem odstavku, se ne štejejo kot povezovanje sistemov.

Modeli medsebojne povezave

Medsebojno povezavo sistemov opisujeta dva parametra:

- varnostni pogoji, ki se določajo na podlagi lastnosti in opredeljujejo medsebojno povezavo dveh sistemov, ter
- vloge, ki opisujejo vlogo sistema v medsebojni povezavi.

Vloge sistemov v medsebojni povezavi opredeljujejo:

- smer toka podatkov s stališča sistema in
- zagotavljanje storitev, vlogo sistema v zagotavljanju ali uporabi storitev, ki jo zagotavlja medsebojna storitev.

Vrednosti vloge iz posamezne lastnosti iz prejšnjega odstavka so podane v spodnji preglednici.

Lastnost	Vrednost	Opis
smer toka podatkov	prejemanje	sistem prejema podatke iz drugega sistema
	pošiljanje	sistem pošilja podatke drugemu sistemu
	pošiljanje/prejemanje	sistem pošilja in prejema podatke
zagotavljanje storitev	uporaba (uporabnik storitev)	sistem uporablja storitve, ki jih zagotavlja drugi sistem – odjemalec
	zagotavljanje (ponudnik storitev)	sistem zagotavlja storitve za drugi sistem – strežnik
	uporaba/zagotavljanje	sistem zagotavlja storitve drugemu sistemu in uporablja njegove storitve

Vrednosti vlog iz prejšnjega odstavka je treba natančno opredeliti v OPZ.

Pogoji glede določanja toka ali storitev:

	določitev toka podatkov ali storitev	dovoljeno	izjema
povezovanje sistemov istih stopenj tajnosti	Vsak tok ali storitev iz OZP mora biti natančno določena.		
povezovanje sistemov različnih stopenj tajnosti	Vsak tok ali storitev iz OZP mora biti natančno določena.	Dovoljen je samo enosmerni tok iz sistema nižje stopnje tajnosti v sistem za višjo stopnjo tajnosti.	Podatkovni tok iz sistema višje stopnje tajnosti v sistem nižje stopnje tajnosti – samo pod pogojem, da so podatki natančno varnostno označeni (labelirani) in se na EMZ/SMZ izvaja nadzor pretoka podatkov.
povezovanje s sistemom brez stopnje tajnosti	Vsak tok ali storitev iz OZP mora biti natančno določena.	Sistem z najvišjo stopnjo tajnosti podatkov za kontrolirano dvosmerno	Sistemi za višje stopnje tajnosti se lahko z medomrežjem (internetom) povezujejo samo enosmerno iz medomrežja oziroma sistema nižje stopnje

		povezovanje je INTERNO.	tajnosti v sistem z višjo stopnjo tajnosti. Pri tovrstnem načinu je obvezna uporaba enosmerne podatkovne diode.
--	--	-------------------------	---

Dostop in nadzor izmenjave podatkov

Nadzorni mehanizmi povezanih sistemov morajo biti taki, da se dostop do tajnih podatkov omogoči samo uporabnikom, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov in se morajo s tajnimi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog.

Izmenjava podatkov med povezanimi sistemi je dovoljena pooblaščenim uporabnikom ali odobrenim procesom.

Nadzor nad izmenjavo izvršljivih datotek (npr. makro, JavaScript, ActiveX controls) se izvaja v skladu z načrtom varovanja sistema.

Skladno z oceno tveganja se uporabijo primerni mehanizmi za zaznavanje in preprečevanje zlonamernih aktivnosti prek SMZ (nenadzorovan pretok podatkov, pretok zlonamerne kode, zaznavanje nepredvidenih aktivnosti itn.).

Priloga 11: Načrt varovanja sistema

<Glava organa / organizacije>

NAČRT VAROVANJA SISTEMA
»dolgo ime sistema«
(kratko ime sistema)

Številka:

Datum:

Različica:

Izdelal:	Soglašala in predlaga:	Izdano mnenje UVTP o ustreznosti:
		Številka dokumenta:
		Datum:

- 1 **ZGODOVINA DOKUMENTA**
- 2 **SLOVAR POJMOV**
- 3 **VIRI**
- 4 **KRATEK POVZETEK DOKUMENTA**
- 5 **UVOD**
 - 5.1 Ime sistema
 - 5.2 Kratek opis sistema
 - 5.3 Najvišja stopnja tajnih podatkov v sistemu
 - 5.4 Lokacija sistema
 - 5.5 Uporabniki sistema
 - 5.6 Varnostni način delovanja sistema
- 6 **OPIS SISTEMA**
 - 6.1 Namen sistema
 - 6.2 Opis podatkov/informacij sistema
 - 6.3 Uporabniki sistema po vlogah
 - 6.4 Konfiguracija sistema
 - 6.5 Splošni opis topologije sistema
 - 6.6 Entitete v sistemu
 - 6.7 Uporabnost sistema
 - 6.8 Komunikacije
 - 6.9 Kriptografska oprema
 - 6.10 Strojna oprema
 - 6.11 Programska oprema
- 7 **NAČRT SESTAVIN IN POVEZAV SISTEMA**
 - 7.1 Skice sistema do stopnje tajnosti
 - 7.2 Skice povezav z drugimi sistemi
- 8 **VARNOSTNE ZAHTEVE SISTEMA**
 - 8.1 Varen začetni zagon
 - 8.2 Varna obnova sistema, ki sledi prekinitvi systemske operacije
 - 8.3 Varna zaustavitev sistema
 - 8.4 Varnostne naloge
 - 8.5 Identifikacija in overjanje
 - 8.6 Nadzor dostopa (fizičen, logičen)
 - 8.7 Označevanje stopenj tajnosti
 - 8.8 Nadzor nad celovitostjo
 - 8.9 Nadzor nad tajnostjo
 - 8.10 Nadzor nad razpoložljivostjo
 - 8.11 Nadzor nad komunikacijami
 - 8.12 Fizično in postopkovno nadzorstvo osebja, dokumentacije, programske opreme, podatkov in opreme
- 9 **VARNOSTNO OKOLJE**
 - 9.1 Širše varnostno okolje sistema (v nadaljevanju ŠVO)
 - 9.2 Ožje varnostno okolje sistema (v nadaljevanju OVO)
 - 9.3 Elektronsko varnostno okolje sistema (v nadaljevanju EVO)
- 10 **VARNOSTNI PROTIUKREPI**
 - 10.1 Identifikacija in overjanje
 - 10.1.1 Politika
 - 10.1.2 Varnostno tveganje in preostalo tveganje
 - 10.1.3 Protiukrepi ŠVO
 - 10.1.4 Protiukrepi OVO
 - 10.1.5 Protiukrepi EVO

- 10.2 Nadzor nad dostopom
 - 10.2.1 Politika
 - 10.2.2 Varnostno tveganje in preostalo tveganje
 - 10.2.3 Protiukrepi ŠVO
 - 10.2.4 Protiukrepi OVO
 - 10.2.5 Protiukrepi EVO
- 10.3 Označevanje in ravnanje z informacijami
 - 10.3.1 Politika
 - 10.3.2 Varnostno tveganje in preostalo tveganje
 - 10.3.3 Protiukrepi ŠVO
 - 10.3.4 Protiukrepi OVO
 - 10.3.5 Protiukrepi EVO
- 10.4 Podatkovne komunikacije
 - 10.4.1 Politika
 - 10.4.2 Varnostno tveganje in preostalo tveganje
 - 10.4.3 Protiukrepi ŠVO
 - 10.4.4 Protiukrepi OVO
 - 10.4.5 Protiukrepi EVO
- 10.5 Celovitost tajnosti in razpoložljivosti
 - 10.5.1 Politika
 - 10.5.2 Varnostno tveganje in preostalo tveganje
 - 10.5.3 Protiukrepi ŠVO
 - 10.5.4 Protiukrepi OVO
 - 10.5.5 Protiukrepi EVO

11 VARNOSTNO UPRAVLJANJE SISTEMA

- 11.1 Organiziranost varnosti
- 11.2 Nadzor konfiguracije/nastavitev in spremembe strojne ter programske opreme
- 11.3 Vzdrževanje sistema
- 11.4 Dokumentacija sistema
- 11.5 Varnostna odobritev sistema
- 11.6 Odpis opreme
- 11.7 Poročanje o incidentih in njihova preiskava

Priloga 12: Ocena varnostnih tveganj sistema

<Glava organa / organizacije>

OCENA VARNOSTNIH TVEGANJ V SISTEMU
»dolgo ime sistema«
(kratko ime sistema)

Številka:

Datum:

Različica:

Izdelal:	Soglaša in predlaga:	Izdano mnenje UVTP o ustreznosti:
		Številka dokumenta:
		Datum:

- 1 ZGODOVINA DOKUMENTA
- 2 VIRI
- 3 SLOVAR POJMOV
- 4 KRATEK POVZETEK DOKUMENTA
- 5 UVOD
 - 5.1. Ime sistema (dolgo, kratko)
 - 5.2. Kratek opis sistema
 - 5.3. Najvišja stopnja v sistemu
 - 5.4. Razlaga stopenj ocene tveganj
 - 5.4.1. Lestvica kritičnosti

Posamezna varnostna tveganja so v tej oceni razvrščena po verjetnosti negativnega dogodka in lestvici kritičnosti na delovanje sistema "primer" v naslednje stopnje:

Lestvica kritičnosti	Lestvica verjetnosti negativnega dogodka				
	zelo visoka	visoka	zmerna	nizka	zelo nizka
zelo visoka	zelo visoko	zelo visoko	visoko	zmerno	nizko
visoka	zelo visoko	visoko	visoko	zmerno	nizko
zmerna	Visoko	visoko	zmerno	nizko	nizko
nizka	Zmerno	zmerno	nizko	nizko	zelo nizko
zelo nizka	Nizko	nizko	nizko	zelo nizko	zelo nizko

Lestvica kritičnosti:

- **zelo visoka**, kar pomeni, da organizacija ne more izpolnjevati osnovnega namena delovanja brez uporabe sistema ali podatkov, ki jih obravnava;
- **visoka**, kar pomeni, da organizacija ne more učinkovito izpolnjevati dela osnovnega namena delovanja brez uporabe sistema ali podatkov, ki jih obravnava;
- **zmerna**, kar pomeni, da je delovanje organizacije resno ogroženo, vendar lahko osnovni namen delovanja izpolni drugače z zmernimi stroški;
- **nizka**, kar pomeni, da bi bil ob izgubi ali razpadu sistema ali podatkov, ki jih obravnava, učinek na izpolnjevanje osnovnega namena organizacije majhen;
- **zelo nizka**, kar pomeni, da sistem ali podatki, ki jih obravnava, niso pomembni za izpolnjevanje osnovnega namena delovanja organizacije.

5.4.2. Lestvica verjetnosti negativnega dogodka

Lestvica verjetnosti negativnega dogodka:

- **zelo visoka**, kar pomeni, da se bo dogodek skoraj zagotovo zgodil;
- **visoka**, kar pomeni, da se bo dogodek verjetno zgodil;
- **zmerna**, kar pomeni, da se bo dogodek mogoče zgodil;
- **nizka**, kar pomeni, da se dogodek mogoče ne bo zgodil;
- **zelo nizka**, kar pomeni, da se dogodek skoraj zagotovo ne bo zgodil.

Priporočljiva sprejemljiva tveganja so: **zelo nizka in nizka**. Priporočljiva pogojno sprejemljiva tveganja so: **zmerna in visoka**. Nesprejemljiva tveganja so: **zelo visoka**.

- 6 OCENA TRENUTNEGA STANJA SISTEMA Z OCENO STOPNJE TVEGANJA
 - 6.1. Nesreče iz okolja
 - 6.1.1 Požari
 - 6.1.2 Potresi
 - 6.1.3 Poplave
 - 6.1.4 Neurja
 - 6.1.5 Epidemije
 - 6.1.6 Ocena za stopnje tveganja za nesreče iz okolja

Ocena varnostnih tveganj v (kratko ime sistema)

- 6.1.7 Opis zagotavljanja celovitosti sistema ob nesrečah iz okolja
- 6.1.8 Opis zagotavljanja razpoložljivosti in dostopnosti sistema ob nesrečah iz okolja
- 6.1.9 Opis zagotavljanja tajnosti sistema ob nesrečah iz okolja
- 6.2. Organizirano in/ali načrtno poškodovanje sistema
 - 6.2.1 Opis tveganj ob organiziranem in/ali načrtnem poškodovanju, kot je teroristični napad, vojno ali izredno stanje, sabotaža, kraja, požig, nezadovoljni zaposleni ipd.
 - 6.2.2 Ocena stopnje tveganj za organizirano in/ali načrtno poškodovanje sistema oziroma podatkov v njem
 - 6.2.3 Opis zagotavljanja celovitosti sistema ob organiziranem in/ali načrtnem poškodovanju
 - 6.2.4 Opis zagotavljanja razpoložljivosti in dostopnosti sistema ob organiziranem in/ali načrtnem poškodovanju
 - 6.2.5 Opis zagotavljanja tajnosti sistema ob organiziranem in/ali načrtnem poškodovanju
- 6.3. Izguba storitev javne infrastrukture
 - 6.3.1 Opis tveganja ob prekinitvi električne napetosti
 - 6.3.2 Opis tveganja ob prekinitvi telekomunikacijskih povezav
 - 6.3.3 Ocena stopnje tveganja ob izgubi storitev javne infrastrukture
- 6.4. Opis zagotavljanja celovitosti sistema ob izgubi storitev javne infrastrukture
 - 6.4.1 Opis zagotavljanja razpoložljivosti in dostopnosti sistema ob izgubi storitev javne infrastrukture
 - 6.4.2 Opis zagotavljanja tajnosti sistema ob izgubi storitev javne infrastrukture
- 6.5. Strojne in sistemske napake
 - 6.5.1 Opis tveganj ob strojnih in sistemskih napakah
 - 6.5.2 Ocena stopnje tveganja ob strojnih in sistemskih napakah
 - 6.5.3 Opis zagotavljanja celovitosti sistema ob strojnih in sistemskih napakah
 - 6.5.4 Opis razpoložljivosti in dostopnosti sistema ob strojnih in sistemskih napakah
 - 6.5.5 Opis zagotavljanja tajnosti sistema ob strojnih in sistemskih napakah
- 6.6. Varnostno in poslovno nepredvidljivi dogodki
 - 6.6.1 Opis tveganja ob varnostno in poslovno nepredvidljivih dogodkih, kot so kibernetični napadi, izguba, poškodovanje ter razkritje podatkov
 - 6.6.2 Ocena stopnje tveganja ob varnostno in poslovno nepredvidljivih dogodkih
 - 6.6.3 Opis zagotavljanja celovitosti sistema ob varnostno in poslovno nepredvidljivih dogodkih
 - 6.6.4 Opis zagotavljanja razpoložljivosti in dostopnosti sistema ob varnostno in poslovno nepredvidljivih dogodkih
 - 6.6.5 Opis zagotavljanja tajnosti sistema ob varnostno in poslovno nepredvidljivih dogodkih

7 KONČNA SKUPNA OCENA

Priloga 13: Varnostno navodilo za delo v sistemu

<Glava organa / organizacije>

VARNOSTNO NAVODILO ZA DELO V SISTEMU
»dolgo ime sistema«
(kratko ime sistema)

Številka:

Datum:

Različica:

Izdelal:	Soglaša in predlaga:	Izdano mnenje UVTP o ustreznosti:
		Številka dokumenta:
		Datum:

- 1 ZGODOVINA DOKUMENTA**
- 2 SLOVAR POJMOV**
- 3 VIRI**
- 4 KRATEK POVZETEK DOKUMENTA**
- 5 UVOD**
 - 5.1 Ime sistema
 - 5.2 Kratak opis sistema
 - 5.3 Najvišja stopnja tajnih podatkov v sistemu
- 6 VARNOSTNO UPRAVLJANJE IN ORGANIZIRANOST VARNOSTI SISTEMA**
 - 6.1 Odgovornost za varnost sistema
 - 6.2 Dodeljevanje pravic uporabnikom
 - 6.3 Prijavljanje varnostnih incidentov
 - 6.4 Seznanjanje z varnostnimi postopki sistema
 - 6.5 Fizična varnost
 - 6.6 Varnost, povezana z osebjem
 - 6.7 Pravice dostopa uporabnikov do prostorov (fizični dostop)
 - 6.8 Pravice za delo s sistemom (logični dostop)
 - 6.9 Dokumentacijska varnost
 - 6.9.1 Označevanje stopnje tajnosti na dokumentih in elektronskih nosilcev podatkov
- 7 INFORMACIJSKA VARNOST**
 - 7.1 Varnost strojne opreme
 - 7.2 Varnost programske opreme
 - 7.3 Protivirusna zaščita
 - 7.4 Zaščita lokalnega omrežja z uporabo požarnih pregrad in sistema za zaznavanje/preprečevanje vdorov
 - 7.5 Šifrirno varovanje podatkov
- 8 NAČRTOVANJE UKREPOV OB NEPREDVIDENIH NELJUBIH DOGODKIH**
 - 8.1 Varnostne kopije
 - 8.2 Ukrepi ob uporabi varnostnih kopij
 - 8.3 Ukrepi ob izpadu električnega omrežja
 - 8.4 Odpis opreme
- 9 UPRAVLJANJE IN SPREMINJANJE KONFIGURACIJE SISTEMA**
 - 9.1 Postopki za spreminjanje konfiguracije/nastavitve sistema
 - 9.2 Nameščanje programske opreme uporabnikov
 - 9.3 Spremembe strojne opreme
 - 9.4 Spremembe programske opreme
- 10 SPLOŠNA VARNOSTNA NAVODILA**
 - 10.1 Sporočanje napak pri delovanju sistema
 - 10.2 Ravnanje s sistemom in upoštevanje varnostnih navodil
- 11 NADZOR**
- 12 ODGOVORNO OSEBJE**

Priloga 14: Varnostno navodilo za delo v sistemu INTERNO

<Glava organa / organizacije>

**VARNOSTNO NAVODILO ZA DELO V SISTEMU
»dolgo ime sistema«
(kratko ime sistema)**

Številka:

Datum:

Različica:

Izdelal:	Soglašja in predlaga:	Izdano mnenje UVTP o ustreznosti:
		Številka dokumenta:
		Datum:

IME SISTEMA		STOPNJA TAJNOSTI SISTEMA	
Dolgo ime: Krajše ime: 		(izberite možnosti) ☐ INTERNO ☐ RESTREINT UE/EU RESTRICTED (EU INTERNO) ☐ NATO RESTRICTED (NATO INTERNO)	
OPIS SISTEMA			
ODGOVORNE OSEBE ZA VARNOST SISTEMA			
Vodja informacijske varnosti	Ime:		
	Priimek:		
	Številka in datum sklepa:		
	Telefon:		
	Elektronska pošta:		
Upravljalavec sistema	Ime:		
	Priimek:		
	Številka in datum sklepa:		
	Telefon:		
	Elektronska pošta:		
Odgovorna oseba za notranji nadzor	Ime:		
	Priimek:		
	Številka in datum sklepa:		
	Telefon:		
	Elektronska pošta:		

FIZIČNA VARNOST	
Sistem za varovanje tajnih podatkov stopnje tajnosti INTERNO je nameščen v upravnem območju.	Številka in datum sklepa:
Minimalni pogoji, ki jim mora ustrezati varnostno-tehnična oprema upravnega območja.	Alarmni sistem ☐ DA ☐ NE Prenos alarmnega signala ☐ DA ☐ NE Nadzor vstopa in gibanja ☐ DA ☐ NE
Organ ali organizacija ima sprejet akt iz 38. člena Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20; v nadaljnjem besedilu: ZTP)	☐ DA ☐ NE
VARNOST, POVEZANA Z OSEBJEM	
Osebe se pred dostopom do tajnih podatkov udeležijo osnovnega usposabljanja s področja varovanja tajnih podatkov.	☐ DA ☐ NE
Osebe pred dostopom do tajnih podatkov podpišejo izjavo, da so seznanjene z zakonom in predpisi, ki urejajo varovanje tajnih podatkov, in z varnostnim navodilom za delo v sistemu.	☐ DA ☐ NE
Osebe do tajnih podatkov v sistemu dostopajo po načelu potrebe po vedenju.	☐ DA ☐ NE
Upravljaivec ali vodja informacijske varnosti ali pooblaščen oseba dodeljuje pravice uporabnikom za vstop v sistem na podlagi potrebe po vedenju.	☐ DA ☐ NE
DOKUMENTACIJSKA VARNOST	
Dokumenti, ki nastajajo v sistemu in jim je določena stopnja tajnosti INTERNO in/ali RESTREINT UE/EU RESTRICTED (EU INTERNO) oziroma NATO RESTRICTED (NATO INTERNO), so označeni v skladu z ZTP in predpisi, sprejetimi na njegovi podlagi ali mednarodnimi sporazumi.	☐ DA ☐ NE
Vse ključne sestavine sistema (računalnik, monitor, tiskalnik/multifunkcijska naprava, tipkovnica, USB-ključ ipd.) so označene s stopnjo tajnosti INTERNO in/ali RESTREINT UE/EU RESTRICTED (EU INTERNO) oziroma NATO RESTRICTED (NATO INTERNO), v skladu z ZTP in predpisi, sprejetimi na njegovi podlagi ali mednarodnimi sporazumi.	☐ DA ☐ NE

UPRAVLJANJE IN SPREMINJANJE KONFIGURACIJE SISTEMA	
Za spreminjanje/konfiguracijo sistema je predstojnik pooblastil upravljavca sistema in vodjo informacijske varnosti.	☐ DA ☐ NE Sklep/pooblastilo št.
Za nameščanje nove programske opreme sta s pooblastilom predstojnika določena upravljavca sistema in vodja informacijske varnosti.	☐ DA ☐ NE Sklep/pooblastilo št.
Za zamenjavo strojne opreme sta s pooblastilom predstojnika določena upravitelj sistema in vodja informacijske varnosti.	☐ DA ☐ NE Sklep/pooblastilo št.
O vseh posegih se vodi evidenca opravljenih dostopov in posegov.	☐ DA ☐ NE
Sistem je zaščiten s protivirusno zaščito (samostojna programska rešitev, integrirana programska rešitev v sklopu operacijskega sistema ipd.)	☐ DA ☐ NE
VARNOSTNA NAVODILA UPORABNIKOM ZA DELO V SISTEMU	
– opis splošnih varnostnih navodil za delo v sistemu, – sporočanje napak pri delovanju sistema, – ravnanje s sistemom in upoštevanje varnostnih navodil.	

Priloga 15: Potrdilo o varnostni ustreznosti kriptografske rešitve

<Glava organa / organizacije>

Številka:

Datum:

Nacionalni varnostni organ na podlagi odločbe številka _____ z dne _____ izdaja

POTRDILO O VARNOSTNI USTREZNOSTI

za kriptografsko rešitev

<ime kriptografske rešitve>

podjetja <ime podjetja>, ki se uporablja za varovanje tajnih podatkov
vključno do stopnje tajnosti

<stopnja tajnosti>.

Varnostno potrdilo velja ob upoštevanju minimalnih varnostnih zahtev za označevanje, distribucijo in uporabo kriptografske rešitve <ime kriptografske rešitve>
(dok. št. _____ z dne _____, <stopnja tajnosti>).

Potrdilo velja do _____.

Ime in priimek predstojnika

Podpis predstojnika

Žig

Priloga 16: Vloga za začetek postopka ugotavljanja ustreznosti kriptografske rešitve**VNESITE STOPNJO TAJNOSTI**

<Glava organa / organizacije>

**VLOGA ZA ZAČETEK
POSTOPKA UGOTAVLJANJA USTREZNOSTI KRIPTOGRAFSKE REŠITVE****PREDLAGATELJ****Državni organ:** (ustrezno označite)

- ☐ ministrstvo, pristojno za javno upravo
- ☐ ministrstvo, pristojno za notranje zadeve
- ☐ ministrstvo, pristojno za obrambo
- ☐ ministrstvo, pristojno za zunanje zadeve
- ☐ Slovenska obveščevalno-varnostna agencija
- ☐ Urad Vlade Republike Slovenije za varovanje tajnih podatkov

Naslov: _____**Ime in priimek kontaktne osebe:** _____

Telefonska številka kontaktne osebe: _____**Elektronski naslov kontaktne osebe:** _____**KRIPTOGRAFSKA REŠITEV****Ime kriptografske rešitve:** _____**Stopnja tajnosti:** (ustrezno označite)

- ☐ INTERNO
- ☐ ZAUPNO
- ☐ TAJNO
- ☐ STROGO TAJNO

- ☐ RESTREINT UE/EU RESTRICTED (EU INTERNO)
- ☐ CONFIDENTIEL UE/EU CONFIDENTIAL (EU ZAUPNO)
- ☐ SECRET UE/EU SECRET (EU TAJNO)
- ☐ TRES SECRET UE/EU TOP SECRET (EU STROGO TAJNO)

- ☐ NATO RESTRICTED (NATO INTERNO)
- ☐ NATO CONFIDENTIAL (NATO ZAUPNO)
- ☐ NATO SECRET (NATO TAJNO)
- ☐ COSMIC TOP SECRET (NATO STROGO TAJNO)

VNESITE STOPNJO TAJNOSTI

<Glava organa / organizacije>

Kratek opis delovanja oziroma namen uporabe kriptografske rešitve: _____

VRSTA POSTOPKA: (ustrezno označite)

[A] ugotavljanje varnostne ustreznosti nove kriptografske rešitve

[B] ugotavljanje varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve

[C] ostalo: _____
(navedite)

PROIZVAJALEC

Ime podjetja: _____

Sedež podjetja: _____

V/Na _____, dne _____

Ime in priimek predstojnika

Podpis kontaktne osebe v organu

Podpis predstojnika

Žig

Priloga 17: Vsebina dokumentacije za začetek postopka ugotavljanja ustreznosti kriptografske rešitve

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

**DOKUMENTACIJA K PREDLOGU
ZA UVEDBO POSTOPKA UGOTAVLJANJA USTREZNOSTI KRIPTOGRAFSKE REŠITVE ZA
VAROVANJE TAJNIH PODATKOV**

PROIZVAJALEC

Ime podjetja: _____

Sedež podjetja: _____

Odgovorna oseba: _____

Kontaktna oseba (navedite osebo, s katero bo nacionalni organ v tem postopku sodeloval):

Ime in priimek kontaktne osebe: _____

Delovno mesto kontaktne osebe: _____

Telefonska številka kontaktne osebe: _____

Elektronski naslov kontaktne osebe: _____

KRIPTOGRAFSKA REŠITEV

Ime kriptografske rešitve: _____

Kratek opis delovanja kriptografske rešitve, vključno s predvidenim namenom uporabe:

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

VRSTA POSTOPKA: (ustrezno označite)

[A] ugotavljanje varnostne ustreznosti nove kriptografske rešitve

[B] ugotavljanje varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve

[C] ostalo: _____
(navedite)Če ste označili točko **[A]**, priložite zahtevano dokumentacijo
(glej **[A] NOVA KRIPTOGRAFSKA REŠITEV; ZAHTEVANA DOKUMENTACIJA**).Če ste označili točko **[B]**, priložite zahtevano dokumentacijo
(glej **[B] NADGRADNJA VARNOSTNO USTREZNE KRIPTOGRAFSKE REŠITVE; ZAHTEVANA DOKUMENTACIJA**).

ter navedite številko in datum potrdila o varnostni ustreznosti že potrjene kriptografske rešitve:

Datum potrdila: _____ Številka potrdila: _____

Če ste označili točko **[C]**, priložite zahtevano dokumentacijo
(glej **[C] OSTALO; ZAHTEVANA DOKUMENTACIJA**).

V/Na _____, dne _____

Ime in priimek odgovorne osebe_____
Podpis kontaktne osebe_____
Podpis odgovorne osebe

Žig

VNESITE STOPNJO TAJNOSTI

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

[A] NOVA KRIPTOGRAFSKA REŠITEV**ZAHTEVANA DOKUMENTACIJA** (dokumentacija mora biti zapisana v slovenskem jeziku)

1. Opis kriptografske rešitve (modula), in sicer:
 - a) podroben opis delovanja kriptografske rešitve, vseh njenih načinov uporabe, vključno z njeno namembnostjo. Če gre za bolj zapleteno rešitev, lahko proizvajalec pripravi osebno predstavitev;
 - b) podroben opis vseh kriptografskih mehanizmov, ki izvajajo varnostne funkcije. Običajno so to šifrirni algoritmi, generatorji naključnih števil, razni kriptografski protokoli, kriptografski ključi (tajni in javni), podatki za overitev in drugi varnostno pomembni parametri, katerih razkritje bi lahko ogrozilo varnost kriptografske rešitve. Možna je uporaba drugih mehanizmov, ki zagotavljajo ustrezno zaščito tajnih podatkov.
2. Opis vlog in funkcij pooblaščenih uporabnikov kriptografske rešitve ter opis mehanizmov overjanja, in sicer:
 - a) opis vseh vlog, ki jih podpira kriptografska rešitev;
 - b) opis vseh funkcij, servisov in operacij, ki jih lahko določene vloge opravljajo;
 - c) opis mehanizmov overjanja, overitvenih podatkov in inicializacije.
3. Opis modela končnih stanj:
 - a) opis modela vseh končnih stanj kriptografskega modula;
 - b) opis prehodov med različnimi končnimi stanji kriptografskega modula.
4. Opis fizične varnosti:
 - a) opis fizične materialne zaščite;
 - b) poročilo o ustrezni zaščiti pred neželenim elektromagnetnim sevanjem (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
 - c) opis postopka brisanja varnostno pomembnih parametrov;
 - d) opis okoliških parametrov (temperatura, vlažnost, napajanje ...) delovanja.
5. Opis delovnega okolja:
 - a) opis delovnega okolja glede na možnost spreminjanja in dostopa do delovnega okolja;
 - b) opis delovnega okolja glede na možnost spreminjanja in dostopa do že delujoče kriptografske rešitve;
 - c) tip operacijskega sistema in razčlenitev neprizeto nastavljenih parametrov.
6. Opis upravljanja kriptografskih ključev:
 - a) opis vseh kriptografskih ključev ali sestavnih delov, s pomočjo katerih ključi nastajajo;
 - b) podroben opis vseh generatorjev naključnih števil;
 - c) opis načinov za generiranje kriptografskih ključev;
 - d) opis načinov za vzpostavljanje kriptografskih ključev;
 - e) opis postopka vnosa in iznosa kriptografskih ključev;
 - f) opis načinov shranjevanja kriptografskih ključev;

VNESITE STOPNJO TAJNOSTI

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

- g) opis postopka brisanja kriptografskih ključev.
7. Opis samopreizkušanja:
- a) opis postopka samopreizkušanja, vključno s preizkušanjem pri zagonu in vsemi pogojnimi preizkusi;
 - b) opis stanj, ko samopreizkušanje ni uspešno, in postopek za vzpostavitev ponovnega normalnega operativnega delovanja;
 - c) opis vseh varnostno kritičnih funkcij, ki se pri zagonu kriptografske rešitve preverijo;
 - d) opis mehanizma izključitve varnostnih funkcij kriptografske rešitve, če ta obstaja.
8. Opis življenjskega cikla kriptografske rešitve:
- a) opis postopkov za varno generiranje, namestitve in zagon kriptografske rešitve, vključno z morebitno nadgradnjo z novimi različicami;
 - b) bločna predstavitev posameznih varnostno pomembnih programskih podsklopov z izvlečki izvirne programske kode (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
 - c) izvirna programska koda (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
 - d) opis strojne, programske oziroma strojno-programске opreme in bločna predstavitev posameznih varnostno pomembnih strojnih, programskih ali strojno-programskih podsklopov (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
 - e) opis (za vse programske, strojne in strojno-programске sestavne dele) vhodnih parametrov, vseh funkcij, ki se izvedejo na podlagi vhodnih parametrov, ter pričakovanih rezultatov, ko se te funkcije izvedejo;
 - f) opis fizičnih vhodov/izhodov in logičnih vmesnikov z določenimi vhodnimi/izhodnimi potmi;
 - g) opis ročnih in logičnih kontrol kriptografskih rešitev, opis fizičnih in logičnih kazalnikov statusa.
9. Opis postopka razdelitve kriptografske rešitve avtoriziranim skrbnikom kriptografskega materiala:
- a) opis administrativnih funkcij, varnostnih dogodkov, varnostnih parametrov, fizičnih in logičnih vmesnikov, ki jih bo uporabljal;
 - b) postopek za varno upravljanje kriptografske rešitve;
 - c) varnostno pomembne domneve glede na ravnanje uporabnika kriptografske rešitve.
10. Navodila za uporabnika (uporabniški priročnik):
- a) odobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal;
 - b) naloge, ki zagotavljajo varno delovanje kriptografske rešitve.
11. Opis razvojnega okolja in razvojnih procesov (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna):
- a) opis razvojnega okolja;
 - b) navedba in opis testov, ki ste jih izvedli v fazah razvoja kriptografske rešitve za:
 - i. preverjanje pravilnosti delovanja kriptografske rešitve;

VNESITE STOPNJO TAJNOSTI

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

- ii. preverjanje robustnosti strojne opreme;
 - iii. varnostno analizo kriptografske rešitve, možnosti kompromitacij;
 - c) navedba načinov testiranja varnosti tega protokola (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji ipd.);
 - d) priprava testnih orodij, ki jih bo nacionalni varnostni organ potreboval pri testiranju, in morebitne dodatne opreme za izvedbo postopka.
12. Opis dobavne verige varnostno pomembnih gradnikov kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna).

[B] NADGRADNJA VARNOSTNO USTREZNE KRIPTOGRAFSKE REŠITVE**ZAHTEVANA DOKUMENTACIJA** (dokumentacija mora biti zapisana v slovenskem jeziku)

1. Natančen opis spremenjenih ali novih funkcionalnosti nadgradnje kriptografske rešitve (modula).
2. Opis razvojnega okolja in razvojnih procesov nadgradnje kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna):
 - a) opis razvojnega okolja;
 - b) navedba in opis testov, ki so bili izvedeni v fazah razvoja nadgradnje kriptografske rešitve za:
 - i. preverjanje pravilnosti delovanja kriptografske rešitve;
 - ii. preverjanje robustnosti strojne opreme;
 - iii. varnostno analizo kriptografske rešitve, možnosti kompromitacij;
 - c) navedba načinov testiranja varnosti tega protokola (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji ipd.);
 - d) priprava testnih orodij, ki jih bo nacionalni varnostni organ potreboval pri testiranju, in morebitne dodatne opreme za izvedbo postopka.
3. Specifikacija navodil za uporabnika (uporabniški priročnik):
 - a) odobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal;
 - b) naloge, ki zagotavljajo varno delovanje kriptografske rešitve.
4. Opis postopka razdelitve kriptografske rešitve avtoriziranim skrbnikom kriptografskega materiala:
 - a) opis administrativnih funkcij, varnostnih dogodkov, varnostnih parametrov, fizičnih in logičnih vmesnikov, ki jih bo uporabljal;
 - b) postopek za varno upravljanje kriptografske rešitve;
 - c) varnostno pomembne domneve glede na ravnanje uporabnika kriptografske rešitve.

VNESITE STOPNJO TAJNOSTI

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

5. Opis dobavne verige varnostno pomembnih gradnikov nadgradnje kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna).

[C] OSTALO _____
ZAHTEVANA DOKUMENTACIJA (dokumentacija mora biti zapisana v slovenskem jeziku)

1. Podroben (matematični) opis delovanja nekriptografske rešitve (oz. sistema, sheme, mehanizma ...) in dokaz pravilnosti delovanja nekriptografske rešitve (oz. sistema, sheme, mehanizma ...).
2. Opis razvojnega okolja in razvojnih procesov nadgradnje kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna):
 - a) opis razvojnega okolja;
 - b) navedba in opis testov, ki ste jih izvedli v fazah razvoja nekriptografske rešitve za:
 - i. preverjanje pravilnosti delovanja;
 - ii. preverjanje robustnosti delovanja;
 - iii. varnostno analizo nekriptografske rešitve, možnosti kompromitacij;
 - c) navedba načinov testiranja varnosti tega protokola (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji ipd.);
 - d) priprava testnih orodij, ki jih bo nacionalni varnostni organ potreboval pri testiranju, in morebitne dodatne opreme za izvedbo postopka.
3. Opis dobavne verige varnostno pomembnih gradnikov nekriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna).

VNESITE STOPNJO TAJNOSTI

1071. Uredba o določitvi nalog kontaktne točke za spodbujanje rabe obnovljivih virov energije

Na podlagi desetega odstavka 51. člena Zakona o spodbujanju rabe obnovljivih virov energije (Uradni list RS, št. 121/21 in 189/21) Vlada Republike Slovenije izdaja

U R E D B O
o določitvi nalog kontaktne točke
za spodbujanje rabe obnovljivih virov energije

I. SPLOŠNE DOLOČBE**1. člen**

(vsebina)

Ta uredba določa način dela, področje uporabe in naloge kontaktne točke, vzpostavitev in vodenje informacijskega sistema, sodelovanje s pristojnimi organi in poročanje ter obveščanje kontaktne točke kot del dejavnosti centra za podpore, kot jo določa 51. člen Zakona o spodbujanju rabe obnovljivih virov energije (Uradni list RS, št. 121/21 in 189/21; v nadaljnjem besedilu: ZSROVE).

2. člen

(pomen izrazov)

(1) Izrazi, uporabljeni v tej uredbi, pomenijo:

1. »kontaktna točka« je dejavnost centra za podpore, kot jo opredeljuje 51. člen ZSROVE;

2. »vlagatelj« je pravna ali fizična oseba, ki namerava kot investitor vlagati v napravo ter katere vlogo za pridobitev dovoljenj in drugih aktov usmerja kontaktna točka;

3. »upravni in drug pristojni organ« je prvostopenjski upravni organ, kot ga opredeljuje zakon, ki ureja upravni postopek, oziroma zanj velja subsidiarna uporaba zakona, ki ureja upravni postopek;

4. »upravni in drugi postopki« so postopki, kot so urejeni v Zakonu o splošnem upravnem postopku (Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07, 65/08, 8/10, 82/13, 175/20 – ZIUOPDVE in 3/22 – ZDeb) oziroma zanje velja subsidiarna uporaba zakona, ki ureja upravni postopek;

5. »proizvodna naprava« je sklop opreme in napeljav, ki pretvarja obnovljive vire energije v električno energijo, toploto za ogrevanje in hlajenje ali v pogonska tekoča in plinasta biogoriva ter lahko obratuje samostojno;

6. »program podpore« je vsak instrument, program ali mehanizem, ki ga uporabi država članica ali skupina držav članic in spodbuja uporabo energije iz obnovljivih virov z zmanjševanjem stroškov te energije, povečanjem cene, po kateri se lahko prodaja, ali povečanjem količine nabavljene energije na podlagi obveznosti glede obnovljive energije ali drugače, kamor med drugim spadajo finančni instrumenti, naložbena pomoč, davčne oprostitve ali olajšave, vračilo davkov, programi podpore, ki zavezujejo k uporabi obnovljive energije, vključno s programi, ki uporabljajo zelene certifikate, in neposredni programi zaščite cen, vključno s tarifami za dovajanje energije in spremenljivimi ali fiksnimi plačili premij;

7. »informacijski sistem« je računalniški sistem, ki ga upravlja center za podpore ter zagotavlja ustrezno informacijsko podporo za integrirano izvajanje poslovnih in upravnih procesov;

8. »Agencija za energijo« je v skladu z zakonom ustanovljen nacionalni regulativni organ Republike Slovenije na področju trga z energijo.

(2) Drugi izrazi imajo enak pomen, kot ga določajo predpisi s področja energetike.

II. OBSEG IN ZAGOTAVLJANJE NALOG JAVNE SLUŽBE**3. člen**

(področje uporabe)

(1) Kontaktna točka opravlja dejavnost iz 4. člena te uredbe na področju javnih in zasebnih vlaganj za:

- proizvodnjo električne energije iz obnovljivih virov energije;
- proizvodnjo toplote za ogrevanje in hlajenje iz obnovljivih virov energije;
- proizvodnjo plinastih goriv, vključno z vodikom, iz obnovljivih virov energije;
- proizvodnjo pogonskih tekočih in plinastih biogoriv;
- proizvodnjo drugih tekočih biogoriv;
- soproizvodnjo z visokim izkoristkom;
- uporabo odvečne toplote v sistemih daljinskega ogrevanja;
- hranilnike električne energije, povezane z izgradnjo proizvodne naprave.

(2) Kontaktna točka je na voljo vsem vlagateljem ne glede na nazivno moč ali namembnost proizvodne naprave, vključno s samooskrbo.

4. člen

(temeljne naloge kontaktne točke)

(1) Kontaktna točka usmerja vlagatelja pri postopkih pridobivanja dovoljenj in drugih aktov, ki se po nacionalnem pravu zahtevajo za proizvodne naprave ter so potrebni za gradnjo, rekonstrukcijo, obnovo ali obratovanje proizvodne naprave in njihovo priključitev na omrežje ter v postopkih programov podpore.

(2) Kontaktna točka vlagatelja pregledno vodi skozi postopek predložitve vlog za izdajo dovoljenj in drugih aktov, od vložitve zahteve do izdaje dokončne odločitve o tej zahtevi, ter mu zagotavlja vse potrebne informacije.

(3) Kontaktna točka lahko opravlja vse naloge v zvezi s pomočjo vlagatelju v upravnih in drugih postopkih ter postopkih programov podpore, vendar pa v teh postopkih ne nastopa kot zastopnik ali pooblaščenec vlagatelja.

(4) Dovoljenja in drugi akti iz prvega in drugega odstavka tega člena so vsa dovoljenja in drugi posamični akti, prostorski akti, licence, registracije in upravna dejanja, ki so potrebni za gradnjo, rekonstrukcijo, obnovo ali obratovanje proizvodne naprave ter za pridobitev podpore v postopkih programov podpore (v nadaljnjem besedilu: dovoljenja in drugi akti).

(5) Dovoljenja in drugi akti iz tega člena vključujejo zlasti:

- a) prijavo na javni razpis za podpore v skladu z zakonom, ki ureja spodbujanje obnovljivih virov energije;
- b) odločbo o sklenitvi podpore in sklenitev pogodbe o njej;
- c) spremembo oziroma sprejetje prostorskega izvedbenega akta;
- č) lokacijsko preveritev;
- d) gradbeno dovoljenje;
- e) vodno dovoljenje;
- f) celovito dovoljenje;
- g) uporabno dovoljenje;
- h) soglasje za priključitev na prenosni ali distribucijski sistem in druge dokumente, ki so potrebni za priključitev proizvodne naprave oziroma, kjer je predvideno, za hranilnik energije;
- i) priključitev na omrežje;
- j) okoljevarstvena in druga soglasja ali dovoljenja, če so potrebna;
- k) vsako drugo dovoljenje, ki se nanaša na proizvodno napravo oziroma hranilnik energije ter je potrebno za gradnjo ali rekonstrukcijo in za začetek obratovanja proizvodne naprave;
- l) prijavo na druge javne razpise, javne pozive in druge oblike povabil za podpore za spodbujanje rabe obnovljivih virov energije.

(6) Kontaktna točka brezplačno ter neodvisno od proizvajalcev in dobaviteljev opreme in storitev informira in svetuje o postopku in izvedbi investicije v proizvodno napravo, vendar ne

izvaja izbire konkretne tehnologije ali tehnike, izbire izvajalca, izračunov ekonomike projekta ter sorodnih vsebinskih in pravnih parametrov projekta. Kontaktna točka v sklopu informiranja ponuja seznam oziroma nabor izvajalcev, ki opravljajo tovrstne storitve, ter seznam ustreznih proizvodnih naprav.

(7) Kontaktna točka lahko opravlja druga administrativna opravila za potrebe postopkov, na primer usmerja vlagatelja pri pridobivanju soglasij solastnikov, pridobivanju služnosti oziroma pravice graditi ter v drugih podobnih primerih, ter sodeluje z občinami, če je za izvedbo investicijske namere treba sprejeti ali spremeniti prostorski izvedbeni akt.

5. člen

(prijava vlagatelja)

(1) Kontaktna točka usmerja vlagatelja na podlagi prijave, ki jo lahko odda osebno ali prek pooblaščenca na lokaciji kontaktne točke, lahko jo pošlje pisno po pošti ali jo odda elektronsko prek spletnega portala kontaktne točke.

(2) Center za podpore za kontaktno točko na lokaciji vzpostavi fizični prostor, ki mora biti dostopen vsem ljudem skladno s pravilnikom, ki ureja univerzalno graditev in uporabo objektov.

(3) Center za podpore za kontaktno točko za potrebe oddaje elektronske prijave vzpostavi spletni portal, kjer vlagatelj z oddajo prijave izrazi interes za sodelovanje s kontaktno točko.

(4) Vlagatelj hkrati z vlogo v postopku za pridobitev dovoljenja oziroma drugega akta obvesti upravni in drug pristojni organ, da predmetni postopek usmerja kontaktna točka.

(5) Če postopek vlagatelja za pridobitev dovoljenja oziroma drugega akta pred upravnim in drugim pristojnim organom že teče, kontaktna točka obvesti upravni in drug pristojni organ, da je predmetni postopek začela usmerjati kontaktna točka.

6. člen

(sodelovanje vlagatelja s kontaktno točko)

Kkontaktna točka sodeluje z vlagateljem in usmerja njegovo vlogo v postopkih, ko vlagatelj s kontaktno točko aktivno sodeluje, tako da na poziv kontaktne točke posreduje potrebne podatke ali izvede potrebne aktivnosti.

7. člen

(informacijski sistem in izmenjava podatkov)

(1) Center za podpore za kontaktno točko z namenom zagotovitve elektronskega poslovanja z vlogami vzpostavi informacijski sistem, s katerim zagotavlja ustrezno informacijsko podporo za integrirano izvajanje poslovnih in upravnih procesov.

(2) V informacijski sistem se povezujejo naslednji podatki:

a) osnovni podatki o vlagatelju, razvidni iz njegove prijave;

b) podatki v postopku za pridobitev dovoljenja in drugega akta, ki jih na zahtevo kontaktne točke zagotovijo upravni in drugi pristojni organi oziroma druge osebe;

c) podatki oziroma informacije, ki jih na zahtevo kontaktne točke zagotovijo upravni in drugi pristojni organi oziroma druge osebe tudi za postopke, za katere ni bila vložena prijava, pri čemer se osebni podatki, razen identifikatorja prevzemno-predajnega mesta in z njim povezanih enoličnih identifikatorjev merilnih točk ter naziv in naslov prevzemno-predajnega mesta oziroma drugih identifikatorjev proizvodne naprave, ne predajo;

č) podatki o dejanskem obratovanju proizvodne naprave in drugih okoliščinah, ki so lahko podlaga za oceno učinkovitosti v skladu s tretjim odstavkom 19. člena ZSROVE, in sicer za čas od začetka obratovanja proizvodne naprave do izteka časa izvajanja podpore v skladu z 20. členom ZSROVE ter ne glede na morebitno pridobitev podpore ali naložbene pomoči oziroma vključenosti v mehanizme po IV. poglavju ZRSROVE.

8. člen

(vzpostavitev in vodenje javne evidence)

(1) Center za podpore za kontaktno točko vzpostavi in vodi javno dostopno uradno evidenco (v nadaljnjem besedilu: javna evidenca).

(2) V javni evidenci se vodijo naslednji podatki, ki jih na zahtevo kontaktne točke zagotovijo upravni in drugi pristojni organi ter druge osebe iz 9. člena te uredbe:

– podatki o prejetih popolnih oziroma nepopolnih vlogah v postopku pri posameznem upravnem in drugem pristojnem organu ter drugi osebi iz 9. člena te uredbe;

– podatki o fazah v postopku pri obdelavi vlog pri posameznih osebah iz prejšnje alineje, vključno z zamudami;

– podatki o končnih odločitvah pri obdelavi vlog pri posameznih osebah iz prve alineje tega odstavka, vključno s podatki o priključenih proizvodnih napravah.

9. člen

(sodelovanje s pristojnimi organi)

(1) Upravni in drugi pristojni organi, ki odločajo v postopkih za izdajo dovoljenj in drugih aktov, ter druge osebe, ki v teh postopkih sodelujejo (v nadaljnjem besedilu: upravni in drugi pristojni organi), so dolžni kontaktni točki neodplačno predati podatke oziroma informacije iz 10. člena te uredbe.

(2) Upravni in drugi pristojni organi so na zahtevo kontaktne točke dolžni podatke oziroma informacije iz 10. člena te uredbe zagotoviti kontaktni točki kot informacijo v elektronski obliki najpozneje naslednji delovni dan po vloženi zahtevi.

10. člen

(podatki oziroma informacije, ki jih zagotovijo upravni in drugi pristojni organi)

(1) Za namen izvajanja nalog ima kontaktna točka pravico dostopa do naslednjih zbirk podatkov, ki jih zagotovijo upravni in drugi pristojni organi:

– zbirka podatkov o graditvi objektov,

– zbirka podatkov o prostorskih aktih in

– druge zbirke podatkov, ki se nanašajo na gradnjo, rekonstrukcijo, obnovo ali obratovanje proizvodne naprave in njihovo priključitev na omrežje ter na postopke programov podpore.

(2) V postopku iz četrtega in petega odstavka 5. člena te uredbe je upravni in drug pristojni organ dolžan kontaktni točki zagotoviti zlasti naslednje podatke oziroma informacije:

1. osnovne podatke (opravilna številka spisa, zadeve ali postopka, datum odprtja spisa, zadeve ali postopka (prejem prve vloge vlagatelja));

2. podatke postopka (tj. status vlagateljeve vloge – popolnost oziroma nepopolnost vloge, podatek o manjkajočih dokumentih oziroma dokazilih, ki jih je treba pridobiti za izdajo dokončne odločitve, rok obravnave vloge idr.);

3. druge podatke oziroma informacije, in sicer na zahtevo kontaktne točke.

11. člen

(poročanje)

(1) Center za podpore za kontaktno točko vsako leto do 1. marca tekočega koledarskega leta pošlje ministrstvu, pristojnemu za energijo, letno poročilo o izvajanju njenih nalog za obdobje od 1. januarja do 31. decembra preteklega koledarskega leta (v nadaljnjem besedilu: letno poročilo).

(2) Letno poročilo vsebuje najmanj podatke o:

– številu in vrsti prejetih prijav po prvem odstavku 51. člena ZSROVE ter drugih vlog po osmem odstavku 51. člena ZSROVE po posameznih proizvodnih napravah v skladu s 3. členom te uredbe;

– številu rešenih, zavrženih in zavrnjenih prijav in vlog;

– razlogih zavrženih in zavrnjenih vlog;

– podanih pritožbah;

– vsoti denarnih sredstev programov podpore;

– vrsti in priključni moči ter lokaciji proizvodne naprave;

– trajanju postopkov, ki so potrebni za gradnjo, rekonstrukcijo, obnovo ali obratovanje proizvodne naprave ter v postopku programov podpore.

(3) Letno poročilo mora vsebovati tudi zaznane ovire in predloge za njihovo odpravo, izpostaviti mora trende ter druge posebnosti glede investiranja v proizvodne naprave in predloge izboljšav storitev kontaktne točke.

(4) Letno poročilo oziroma izvleček letnega poročila center za podpore objavi na spletni strani kontaktne točke.

12. člen

(priročnik in obveščanje)

(1) Center za podpore za kontaktno točko pripravi in javno objavi priročnik o postopkih za vlagatelje na področju proizvodnje energije iz obnovljivih virov, ki posebej obravnava tudi majhne projekte ter projekte končnih odjemalcev s samoskrbo (v nadaljnjem besedilu: priročnik) in ga redno, vsaj enkrat letno, posodablja.

(2) Za javno objavo priročnika šteje objava na spletni strani kontaktne točke na način, ki omogoča brezplačen dostop in prenos pripravljenega priročnika. Poleg objave na spletni strani je priročnik dostopen tudi v prostorih kontaktne točke.

(3) Kontaktna točka obvešča glede spodbujanja rabe obnovljivih virov energije, vključevanja v sistem samooskrbe in oblikovanja skupnostne samooskrbe, pri čemer pripravlja gradiva, izobraževanja in dogodke za namen obveščanja glede spodbujanja rabe obnovljivih virov energije.

13. člen

(letni program dela za izvajanje nalog kontaktne točke)

(1) Center za podpore pripravi letni program dela za izvajanje nalog kontaktne točke, ki je del letnega programa dela in finančnega načrta iz šestega odstavka 18. člena ZSROVE (v nadaljnjem besedilu: letni program dela kontaktne točke).

(2) Letni program dela kontaktne točke vsebuje del, ki se nanaša na vsebino nalog kontaktne točke, finančni in kadrovski del kontaktne točke, način delovanja spletnega portala iz 5. člena te uredbe, strategijo sodelovanja z lokalnimi energetske organizacijami in drugimi subjekti, načrt usposabljanj, načrt obveščanja javnosti in druge vsebine, ki se nanašajo na delovanje kontaktne točke v prihodnjem letu.

14. člen

(sodelovanje z lokalnimi energetske organizacijami)

(1) Za izvajanje nalog kontaktne točke lahko center za podpore sodeluje z lokalnimi energetske organizacijami.

(2) Center za podpore sodelovanje iz prejšnjega odstavka uredi s pogodbo. S pogodbo center za podpore in lokalna energetska organizacija med drugim uredita tudi dostop do potrebnih podatkov za potrebe izvajanja pogodbenih nalog.

15. člen

(navodila za delovanje kontaktne točke)

(1) Z namenom ureditve delovanja, nalog, načina izmenjave podatkov in drugega v pristojnosti kontaktne točke, center za podpore pripravi podrobnejša navodila, ki jih objavi na spletni strani kontaktne točke (v nadaljnjem besedilu: navodila). Poleg objave na spletni strani so navodila dostopna tudi v prostorih kontaktne točke.

(2) V navodilih so podane zahteve za podrobnejšo opredelitev nabora podatkov in informacij ter podrobnejšo obličnost oziroma tehnične podrobnosti glede izmenjave podatkov z vlagatelji ter upravnimi in drugimi pristojni organi, kakor tudi obrazec prijave za fizično in elektronsko prijavo, protokoli oziroma koraki v digitalni in tekstualni obliki za postopke, ki so potrebni za priključitev in pridobitev pomoči proizvodnih naprav iz 3. člena te uredbe ter druge.

(3) Pred objavo navodil iz prvega odstavka tega člena mora center za podpore pridobiti soglasje ministra, pristojnega za energijo.

(4) Kontaktna točka o objavi in spremembi navodil pisno obvesti upravne in druge organe.

III. PREHODNA IN KONČNA DOLOČBA

16. člen

(prehodna določba)

Elektrooperater, operater sistema plina, distributer toplote in Agencija za energijo vzpostavijo povezavo z informacijskim sistemom za avtomatski prenos podatkov iz 7. člena te uredbe, najpozneje v roku 6 mesecev po sprejemu navodil iz 15. člena te uredbe, z namenom sledenja fazam posameznega postopka, vključno z zamudami in izdanimi končnimi odločitvami.

17. člen

(začetek veljavnosti)

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

Št. 00704-138/2022

Ljubljana, dne 7. aprila 2022

EVA 2021-2340-0158

Vlada Republike Slovenije

Janez Janša

predsednik

1072. Uredba o nadomestilu za izrabo prostora za proizvodno napravo na veter

Na podlagi osmega odstavka 21. člena Zakona o spodbujanju rabe obnovljivih virov energije (Uradni list RS, št. 121/21 in 189/21) Vlada Republike Slovenije izdaja

U R E D B O

o nadomestilu za izrabo prostora za proizvodno napravo na veter

1. člen

(predmet uredbe)

Ta uredba določa podrobnejša pravila za odmero in plačevanje nadomestila za izrabo prostora za proizvodno napravo na veter (v nadaljnjem besedilu: nadomestilo).

2. člen

(pomen izrazov)

(1) Izrazi, uporabljeni v tej uredbi, pomenijo:

1. »proizvajalec električne energije« je oseba, ki je bila investitor proizvodne naprave, jo upravlja in pridobiva prihodke od električne energije, proizvedene v tej proizvodni napravi;

2. »proizvodna naprava na veter« je sklop opreme in napeljav, ki pretvarjajo veter kot obnovljivi vir energije v električno energijo, ter lahko samostojno obratuje (v nadaljnjem besedilu: proizvodna naprava);

3. »fizična oseba« je oseba, ki opravlja dejavnost proizvodnje električne energije z eno proizvodno napravo z nazivno močjo do 50 kW in je vpisana v register fizičnih oseb, ki opravljajo dejavnost proizvodnje električne energije pri Agenciji Republike Slovenije za javnopravne evidence in storitve, ter ima veljavno deklaracijo za proizvodno napravo v skladu z zakonom, ki ureja spodbujanje rabe obnovljivih virov energije;

4. »višina podpore« je cena električne energije proizvodne naprave, ki jo Agencija za energijo določi v odločbi o dodelitvi podpore.

(2) Drugi izrazi, uporabljeni v tej uredbi, pomenijo enako kot izrazi, določeni v zakonu, ki ureja spodbujanje rabe obnovljivih virov energije.

3. člen

(zavezanec za plačilo nadomestila)

Zavezanec za plačilo nadomestila (v nadaljnjem besedilu: zavezanec) je proizvajalec električne energije.

4. člen

(izjema od obveznosti plačila nadomestila)

Ne glede na prejšnji člen obveznost plačila nadomestila ne velja za fizične osebe.

5. člen

(upravičenec do prejema nadomestila)

(1) Zavezanec plača nadomestilo občini, v kateri je proizvodna naprava na veter (v nadaljnjem besedilu: občina).

(2) Če proizvodna naprava, sestavljena iz več generatorjev (v nadaljnjem besedilu: vetrnice ali vetrne elektrarne), ki obratujejo povezano, stoji v več občinah, plača zavezanec tem občinam nadomestilo v sorazmerju z inštalirano močjo vetrnic na območju posamezne občine.

(3) Nadomestilo je javna dajatev, ki pripada občini.

6. člen

(osnova za nadomestilo)

(1) Osnova za nadomestilo je ocenjeni celoletni prihodek zavezanca, ki izvira iz proizvodnje električne energije iz vetrne energije njegovih posameznih proizvodnih naprav.

(2) V primeru proizvodnih naprav na veter, za katere je zavezanec na podlagi odločbe Agencije za energijo upravičen do podpore, se v letu, ko je zavezanec podporo prejemal, osnova za nadomestilo določi kot zmnožek letne proizvedene količine električne energije (izražene v MWh) in višine podpore (izražene v EUR/MWh).

(3) V primeru preostalih proizvodnih naprav na veter, za katere zavezanec ni upravičen do podpore, se osnova za nadomestilo določi kot zmnožek letne proizvedene količine električne energije (izražene v MWh) in referenčne cene električne energije (izražene v EUR/MWh), ki jo za posamezno leto določi in objavi Agencija za energijo v skladu z zakonom, ki ureja spodbujanje rabe obnovljivih virov energije.

(4) Ne glede na prejšnji odstavek se v primeru proizvodnih naprav na veter, za katere je zavezanec del proizvedene električne energije prodajal na podlagi pogodb o nakupu električne energije iz obnovljivih virov, veljavnih najmanj deset let, osnova za nadomestilo določi kot zmnožek po pogodbi o nakupu električne energije iz obnovljivih virov prodanih količin električne energije (izražene v MWh) in pogodbenih cen električne energije (izraženih v EUR/MWh).

7. člen

(obveznost plačila nadomestila)

(1) Nadomestilo je letna obveznost zavezanca in se odmeri za preteklo leto po tridstotni stopnji od vrednosti osnove iz prejšnjega člena.

(2) Obveznost plačila nadomestila nastopi prvi dan v mesecu, ki sledi mesecu, v katerem začne proizvodna naprava oddajati električno energijo v omrežje.

8. člen

(odločba o odmeri nadomestila)

(1) Nadomestilo zavezancu odmeri ministrstvo, pristojno za energijo, z odločbo, ki jo pošlje v vednost občini.

(2) Z odločbo o odmeri nadomestila se določi znesek nadomestila, ki ga je zavezanec dolžan plačati občini.

9. člen

(plačilni pogoji)

(1) Zavezanec poravnava z odločbo odmerjeno nadomestilo v enkratnem znesku v 30 dneh po vročitvi odločbe.

(2) Za neplačane zapadle obveznosti tečejo zakonite zamudne obresti.

10. člen

(posredovanje podatkov)

(1) Zavezanec je dolžan ministrstvu, pristojnemu za energijo, v skladu s predpisom, ki ureja sporočanje podatkov, ki so jih dolžni sporočati izvajalci energetskih dejavnosti, najpozneje do 15. aprila tekočega koledarskega leta za preteklo koledarsko leto predložiti naslednje podatke:

– podatek o letni proizvedeni električni energiji za posamezno vetrno elektrarno,

– podatek o inštalirani moči vetrnih elektrarn na območju posamezne občine.

(2) Če je prihodek iz proizvodnje električne energije preteklega koledarskega leta nastal po 31. marcu tekočega koledarskega leta, se ovrednoti za nadomestilo v naslednjem letu.

KONČNA DOLOČBA

11. člen

(začetek veljavnosti)

Ta uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije, uporabljati pa se začne 7. avgusta 2022.

Št. 00704-137/2022

Ljubljana, dne 7. aprila 2022

EVA 2022-2430-0010

Vlada Republike Slovenije

Janez Janša
predsednik

MINISTRSTVA**1073. Pravilnik o spremembah in dopolnitvah
Pravilnika o temeljnih kvalifikacijah za voznike
motornih vozil v cestnem prometu**

Na podlagi 43. člena Zakona o prevozih v cestnem prometu (Uradni list RS, št. 6/16 – uradno prečiščeno besedilo, 67/19 in 94/21) minister za infrastrukturo izdaja

P R A V I L N I K**o spremembah in dopolnitvah Pravilnika
o temeljnih kvalifikacijah za voznike motornih
vozil v cestnem prometu****1. člen**

V Pravilniku o temeljnih kvalifikacijah za voznike motornih vozil v cestnem prometu (Uradni list RS, št. 103/10, 63/12, 62/14 in 69/19) se v 7. členu za četrtim odstavkom doda nov peti odstavek, ki se glasi:

»(5) Vozilo za preskus vožnje iz tretjega odstavka tega člena in zmogljivi simulator iz prejšnjega odstavka morata biti opremljena s tahografom. Pri vožnji z vozilom in pri preskusu na zmogljivem simulatorju se uporablja voznikova kartica, katere imetnik je inštruktor vožnje. Preskusna vožnja se izvaja z uporabo tahografa po postopku iz priloge 12, ki je sestavni del tega pravilnika. Izpisi iz tahografa, nastali med preskusom vožnje, se priložijo zapisniku praktičnega preskusa iz priloge 14, ki je sestavni del tega pravilnika.«.

Dosedanji peti, šesti, sedmi, osmi, deveti in deseti odstavek postanejo šesti, sedmi, osmi, deveti, deseti in enajsti odstavek.

2. člen

V 12. členu se sedmi odstavek spremeni tako, da se glasi:

»(7) Za vsak izpitni rok pri posameznem pooblaščenem centru za usposabljanje predsednik komisije imenuje tričlansko izpitno komisijo. Če je na izpitnem roku 10 kandidatov ali manj, predsednik imenuje dvočlansko komisijo. Če je število kandidatov večje od 36, predsednik imenuje štiričlansko izpitno komisijo. O teoretičnem preskusu znanja komisija vodi zapisnik o teoretičnem preskusu znanja, določen v prilogi 15, ki je sestavni del tega pravilnika.«.

3. člen

V 13. členu se v tretjem odstavku za drugim stavkom doda besedilo, ki se glasi: »Usposabljanje z uporabo orodij informacijske in komunikacijske tehnologije (IKT) ne sme trajati več kot 12 ur. Pri taki obliki usposabljanja mora pooblaščen izpitni center zagotoviti ohranjanje ustrezne kakovosti usposabljanja, vključno z izbiro področja, kjer se lahko orodja IKT najbolj učinkovito uporabijo.«.

Za petim odstavkom se doda nov šesti odstavek, ki se glasi:

»(6) Pooblaščen centri morajo najkasneje v 20 minutah po začetku rednega usposabljanja ministrstvu poslati število udeležencev usposabljanja.«.

4. člen

V 17. členu se črta četrti odstavek.

5. člen

Priloga 12 se nadomesti z novo prilogo 12, ki je kot Priloga 1 sestavni del tega pravilnika.

6. člen

Za prilogo 13 se dodata novi priloga 14 in priloga 15, ki sta kot Priloga 2 in Priloga 3 sestavni del tega pravilnika.

PREHODNA IN KONČNA DOLOČBA**7. člen**

(1) Preskusna vožnja iz novega petega odstavka 7. člena pravilnika se začne izvajati dva meseca od uveljavitve tega pravilnika.

(2) Poročila iz četrtega odstavka 17. člena Pravilnika o temeljnih kvalifikacijah za voznike motornih vozil v cestnem prometu (Uradni list RS, št. 103/10, 63/12, 62/14 in 69/19) se ministrstvu posredujejo do 31. maja 2022.

8. člen

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

Št. 007-4/2022-32

Ljubljana, dne 24. marca 2022

EVA 2022-2430-0001

Jernej Vrtovec
minister
za infrastrukturo

Priloga 1**»Priloga 12: Postopek uporabe tahografa**

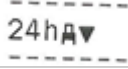
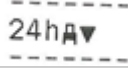
Preskusna vožnja se izvaja z vozilom ali na zmogljivem simulatorju (vožnja na zmogljivem simulatorju ali vadbeni progi traja maksimalno 30 minut), ki sta opremljena s tahografom. Preskusna vožnja skupaj traja 90 minut. V tem času kandidat prevoziti razdaljo najmanj 40 kilometrov. V primeru, da cestno prometne razmere ne omogočijo prevoziti te razdalje, se to navede v opombe zapisnika praktičnega preskusa.

Pri vožnji z vozilom ali na zmogljivem simulatorju se uporablja voznikova kartica katere imetnik je inštruktor – ocenjevalec vožnje. Izpisi iz tahografa, ki nastanejo tekom preskusne vožnje se priložijo zapisniku praktičnega preskusa.

Pri vozilih opremljeni z analognim tahografom se uporablja tahografski vložek, ki ga izpolni inštruktor – ocenjevalec vožnje. Izpolnjen tahografski vložek se priloži zapisniku praktičnega preskusa.

Preskusna vožnja se izvaja z uporabo tahografa po spodaj opisanem postopku. Pri uporabi analognega tahografa se preskusna vožnja izvaja smiselno s spodaj opisanim postopkom.

Št. kora ka	Zaporedje aktivnosti, nalog in opravil	Opis izvajanja aktivnosti, nalog in opravil	
010	Prihod do vozila	Vstavitve voznikove kartice v tahograf (kartica s katero razpolaga inštruktor – ocenjevalec). Tahograf se nastavi na področje izven veljavnosti. Nastavi se aktivnost drugo delo-	
011	Vnos aktivnosti za nazaj	Vnos aktivnosti voznika za nazaj. Vnese se aktivnosti od zadnjega izvzetja voznikove kartice (ali tahografskega vložka). Kandidat obrazloži: - Navodilo 2: Zapisovanje časa, ki ga voznik porabi za potovanje do kraja, ki ni običajni kraj prevzema ali predaje vozila, za katero velja področje uporabe Uredbe (ES) št 561/2006 in - Pojasnilo 7: Beleženje in nadzor obdobja dejavnosti in nedejavnosti voznikov, ko so oddaljeni od vozila Dokumenta sta dostopen na https://transport.ec.europa.eu/transport-modes/road/social-provisions/driving-time-and-rest-periods/guidance-notes-implementation-community-rules-driving-times-and-rest-periods-professional-drivers_en Kandidat obrazloži izvajanja 5. odstavka, 6. člena Uredbe 561/2006/EU. Po vnosu aktivnosti za nazaj se izdela dnevni izpis aktivnosti voznika iz voznikove kartice  in se na izpisu obkrožijo vnesene aktivnosti za nazaj. Kandidat na izpisu navede svoje podatke (ime in priimek), številko osebnega dokumenta in izpis podpiše.	
012	Oznaka države	Vnos oznake države, v kateri se dnevni delovni čas začne.	

020	Uporaba tahografa	Kandidat razloži delovanje tahografa. Kandidat razloži upravljanje preklopnega mehanizma, ki omogočajo ločen in razločen zapis naslednjih časovnih obdobj: »drugo delo«, ki pomeni vsako dejavnost, razen vožnje, kot je opredeljena v točki (a) člena 3 Direktive 2002/15/ES, in tudi vsako delo za istega ali drugega delodajalca v prevozniskem sektorju ali zunaj njega; »čas razpoložljivosti« in »čas odmora, počitka, letni ali bolniški dopust«.	
021	Menjava papirja	Kandidat prikaže postopek menjave papirja v tahografu.	
030	Začetek izvajanja vožnje	Vožnja se izvaja z vstavljenno voznikovo kartico.	
050	Zaključek vožnje	Voznika se seznani s postopki, ki jih mora izvesti po zaključku vožnje.	
055	Oznaka države	Vnos oznake države, v kateri se dnevni delovni čas konča.	
070	Dnevni izpis aktivnosti iz tahograf	Izdela se dnevni izpis aktivnosti iz tahografa.  Na izpisu se označijo (obkrožijo) aktivnosti, ki jih je kandidat izvedel v času praktičnega preizkusa vožnje. Na izpisu se obkroži podatek o času začetka izvajanja vožnje in času zaključka vožnje. Izračuna se razlika obeh časov in se ročno zapiše na izpis.	
072	Pregled podatkov na izpisu	Kandidat razloži podatke na izpisu, datum zadnje kalibracije tahografa, kdaj je potrebno izvesti novo kalibracijo? Kandidat razloži, kaj predstavljajo zapisi v zadnjih desetih vrsticah na izpisu?	
073	Okvara tahografa	Simulira se okvara tahografa. Kandidat izvede ročne zapise aktivnosti, ki jih je izvajal. Kandidat na hrbtni strani izpisa iz koraka 070 ročno vnese svoje aktivnosti, ki jih je izvajal od začetka izvajanja vožnje, do zaključka dnevnih aktivnosti. Zabeleži se tudi čas potovanja od/do vozila. Kandidat na izpisu navede svoje podatke, številko osebnega dokumenta in izpis podpiše.	
074	Okvara voznikove kartice	Simulira se okvara voznikove kartice. Kandidat obrazloži kako postopa v primeru izgube, kraje ali okvare voznikove kartice. Obrazložitev: Pred začetkom izvajanja dnevnih aktivnosti izdela izpis in vnese svoje podatke in ga podpiše.  Ob zaključku izvajanja dnevnih aktivnosti izdela izpis in vnese svoje podatke in ga podpiše. 	
075	Izpis diagramov iz tahografa	Če tip tahografa omogoča, se izdela izpis diagramov iz tahografa za tekoči dan: - diagram hitrosti;  - diagram aktivnosti voznika.  Kandidat obrazloži vsebino izpisanih diagramov.	
080	Arhiviranje izpisov	Izpisi iz tahografa, ki so nastali pod 011, 070 in 075 se priložijo Zapisniku praktičnega preizkusa.	

Priloga 2

»Priloga 14: Zapisnik praktičnega preskusa



REPUBLIKA SLOVENIJA
 MINISTRSTVO ZA INFRASTRUKTURO
 Komisija za opravljanje preskusa znanja
 za pridobitev temeljne kvalifikacije voznikov motornih vozil v cestnem prometu

ZAPISNIK PRAKTIČNEGA PRESKUSA

za pridobitev temeljne kvalifikacije voznikov motornih vozil v cestnem prometu

Pooblaščen center za usposabljanje: _____

Priimek in ime kandidata: _____ Kategorija: _____

1. Preskusna vožnja - Relacija izpitne vožnje: _____

Registrska oznaka vozila: _____

Datum preskusa: _____

Št. kilometrov na koncu vožnje: _____

Začetek preskusa ob: _____

Št. kilometrov na začetku vožnje: _____

Zaključek preskusa ob: _____

Razlika: _____ km

Razlika: _____ min

		1	1a	NAPAKE	OPOMBE
I. IZBOLJŠANJE RACIONALNE VOŽNJE TER ZAGOTAVLJANJE UDOBJA IN VARNOSTI POTNIKOV, PRIPRAVA NA VARNO VOŽNJO, UPRAVLJANJE VOZILA TER UPRAVLJANJE S SEKUNDARNIMI NAPRAVAMI ZA UPRAVLJANJE VOZILA	Preverjanje stanja pnevmatik, luči, odsevnikov, krmilnega in zavornega sistema, smernih utripalk in zvočnih opozorilnih naprav. Pravilna nastavitve sedeža, vzratnih ogledal. Pripnjanje z varnostnim pasom ter zaprtje vrat				
	Pravilno upravljanje z volanom, pedalom za plin, sklopko, ročno in nožno zavoro. Pravilno menjanje prestav				
	Zagon motorja in gladko speljevanje (po ravni površini, navkreber in navzdol).				
	Pospšejevanje do ustrezne hitrosti ob menjavanju prestav, pri čemer je potrebno obdržati ravno linijo				
	Prilagoditev hitrosti za zavijanje na levo ali desno (po možnosti na omejenem prostoru, pri čemer mora voznik ohraniti nadzor nad vozilom), prilagajanje vzdolžnega in bočnega gibanja				
	Vožnja vzvratno v ravni linij in vožnja vzvratno levo ali desno v ovinek, tako da vozilo ostane v pravilni smeri				
	Uporabljanje dovoljenih sredstev za komuniciranje z drugimi udeleženci v prometu, interakcija s potniki, upoštevanje pravil varne vožnje ob drugih vlogah voznika (spremljanje potnikov, vstop in izstop potnikov, ipd.)				
	Obračanje vozila v nasprotno smer z uporabo vožnje naprej in vzvratne vožnje.				
	Pravilno zaviranje za zaustavitev vozila in, če je potrebno, ustavitev v sili				
	Parkiranje vozila in zapustitev parkirnega prostora (vzporedna, poševna ali pod kotom) tako naprej, kot vzvratno, na ravni površini, navzdol in navkreber				
	Naprave za čiščenje, sušenje in odmrzovanje vetrobranskega stekla ter naprave za luči in klimatizacijo				

II. OBIČAJNA MANEVIRANJA , ZDRAVJE, VARNOST NA CESTI IN VAROVANJE OKOLJA, STORITEV, LOGISTIKA	Spremljanje in opazovanje (vključno z uporabo vzvratnih ogledal) poteka ceste, oznak, prometnih znakov in morebitnih ali dejanskih nevarnosti				
	Zmožnost preprečevanja kaznivih dejanj in tihotapljenje ilegalnih priseljencev: kandidat pokaže mesta na vozilu, kjer se lahko skriva in tihotapi nedovoljeno blago ali ilegalni priseljenci in pokaže preventivne ukrepe s katerimi se zmanjša ali prepreči takšna dejanja				
	Ustrezno predvidevanje in reagiranje v dejanskih nevarnih situacijah				
	Upoštevanje cestno prometnih predpisov in navodil pooblaščenih uradnih oseb, pristojnih za nadzor in urejanje cestnega prometa				
	Spoštovanje in upoštevanje udeležencev v prometu				
	Speljevanje iz robnika in/ali s parkirnega prostora, uporaba posebnih infrastruktur npr. rezervirani vozní pas				
	Pravilno usmerjanje svojega vozila in prilagoditev razmeram v prometu ter poteku in nagibu ceste				
	Ohranjanje primerne varnostne razdalje med vozili				
	Menjava prometnih pasov				
	Vožnja mimo parkiranih ali stoječih vozil in ovir				
	Srečanje z nasproti vozečimi vozili v ozkih mestih				
	Prehitevanje v različnih situacijah				
	Približevanje in prečkanje železniškega prehoda				
	Približevanje in prečkanje križišča				
	Zavijanje v križišču (desno ali levo) ali zapuščanje cestišča				
	Preprečevanje fizičnih tveganj za voznika: upoštevanje ergonomskih načel, pravilni gibi in drža pri vožnji, osebna zaščita, prepričanje o varnosti, ko voznik zapušča vozilo				
	Ravnanje z vozilom v sili, preprečevanje zapletov po nesreči, ravnanje v primeru požara, evakuacija potnikov, priprava poročila o nesreči				
III. SPOSOBNOST VARNEGA OBNAŠANJA NA RAZLIČNIH VRSTAH CEST IN V RAZLIČNIH POGOJIH VOŽNJE	Cesta zunaj naselja (makadam, asfalt).				
	Hitra cesta				
	Avtocesta				
	Vreme (dež, sneg)				
	Svetloba (sončno, noč)				
	Gostota prometa (tekoča, stoječa)				

OCENA: OPRAVIL - NI OPRAVIL Priimek in ime ocenjevalca: _____ Podpis: _____

1.a Vožnja na vadbeni progi ali simulatorju DA NE

Registrska oznaka vozila: _____

Datum preskusa: _____

Št. kilometrov na koncu vožnje: _____

Začetek preskusa ob: _____

Št. kilometrov na začetku vožnje: _____

Zaključek preskusa ob: _____

Razlika: _____ km

Razlika: _____ min (max 30)

Skupni čas preskusa 1 + 1a = _____ (minimalno 90 min)

OCENA: OPRAVIL - NI OPRAVIL Priimek in ime ocenjevalca: _____ Podpis: _____

2. Praktični preskus (1.4., 1.5., 1.6., 3.2., 3.3 in 3.5) Datum preskusa: _____ od – do: _____

OCENA: OPRAVIL - NI OPRAVIL Priimek in ime ocenjevalca: _____ Podpis: _____

Podpis kandidata in opombe:

_____ «.

Priloga 3**»Priloga 15: Zapisnik o teoretičnem preskusu znanja**

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA INFRASTRUKTURO
Komisija za opravljanje preskusa znanja
za pridobitev temeljne kvalifikacije voznikov motornih vozil v cestnem prometu

Pooblaščen center za usposabljanje:

ZAPISNIK
o teoretičnem preskusu znanja za pridobitev temeljne kvalifikacije
voznikov motornih vozil v cestnem prometu

Kandidat za pridobitev temeljne kvalifikacije:.....
(ime in priimek)

je opravljal teoretični preskus znanja za pridobitev temeljne kvalifikacije za:
(ustrezno obkroži)

- a) prevoz blaga
- b) prevoz potnikov

Datum izpita

Kraj izpita.....

OCENA PRESKUSA ZNANJA

kandidat JE opravil - NI opravil

teoretični preskus znanja za pridobitev temeljne kvalifikacije za prevoz:.....
(vpiši potnikov ali blaga)

OPOMBE:

(vpiše se, če kandidat ni pristopil k izpitu oziroma se mu zaradi kršenja izpitnih pravil ni dovolilo nadaljevati z opravljanjem izpita ali druge podobne opombe)

V..... dne

Predsednik izpitne komisije:

Člana izpitne komisije:«.

OBČINE

PREBOLD

1074. Zaključni račun proračuna Občine Prebold za leto 2021

Na podlagi tretjega odstavka 98. člena Zakona o javnih financah (Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13, 55/15 – ZFisP, 96/15 – ZIPRS1617, 13/18 in 195/20 – odl. US) in 15. člena Statuta Občine Prebold (Uradni list RS, št. 52/13 in 45/14) je občinski svet na 28. redni seji 7. aprila 2022 sprejel

ZAKLJUČNI RAČUN proračuna Občine Prebold za leto 2021

1. člen

Sprejme se Zaključni račun proračuna Občine Prebold za leto 2021.

2. člen

Zaključni račun proračuna Občine Prebold za leto 2021 sestavljajo splošni in posebni del. V splošnem delu je podan podrobnejši prikaz predvidenih in realiziranih prihodkov in odhodkov oziroma prejemkov in izdatkov iz bilance prihodkov in odhodkov, računa finančnih terjatev in naložb ter računa financiranja, v posebnem delu pa prikaz predvidenih in realiziranih odhodkov in drugih izdatkov proračuna Občine Prebold za leto 2021.

Sestavni del zaključnega računa je tudi načrt razvojnih programov, v katerem je podan prikaz podatkov o načrtovanih vrednostih posameznih projektov, njihovih spremembah med letom 2021 ter o njihovi realizaciji v tem letu.

Proračun Občine Prebold je bil realiziran v naslednjih zneskih:

A BILANCA PRIHODKOV IN ODHODKOV konto K2/K3		Realizacija 2021 v EUR
I.	Skupaj prihodki	4.876.785,57
II.	Skupaj odhodki	5.155.018,53
III.	Proračunski presežek/primanjkljaj (I.-II.)	-278.232,96
B RAČUN FINANČNIH TERJATEV IN NALOŽB konto K2/K3		
IV.	Prejeta vračila danih posojil in prodaja kapitalskih deležev	0
V.	Dana posojila in povečanje kapitalskih deležev	0
VI.	Prejeta minus dana posojila in spremembe kapitalskih deležev (IV.-V.)	0
C RAČUN FINANCIRANJA konto K2/K3		
VI.	Zadolževanje	600.000,00
VII.	Odplačilo dolga	233.446,58
VIII.	Spremembe stanja sredstev na računih	98.320,46
IX.	Neto zadolževanje	376.553,42
XI.	Neto financiranje	278.232,96
XII.	Stanje sredstev na računih 31. 12. 2021 (del 9009-Splošni sklad za drugo)	445.916,79

3. člen

Zaključni račun proračuna Občine Prebold za leto 2021 se objavi v Uradnem listu Republike Slovenije. Splošni in posebni

del, poročilo o izvajanju načrta razvojnih programov ter dodatne obrazložitve s prilogami, se objavijo na spletnih straneh Občine Prebold.

Št. 410-0001/2022

Prebold, dne 7. aprila 2022

Župan
Občine Prebold
Vinko Debelak

1075. Odlok o rebalansu proračuna Občine Prebold za leto 2022

Na podlagi 29. člena Zakona o lokalni samoupravi (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 76/08, 79/09, 51/10, 40/12 – ZUJF, 14/15 – ZUUJFO, 11/18 – ZSPDLS-1, 30/18, 61/20 – ZIUZEOP-A in 80/20 – ZIUOOPE), 29. člena Zakona o javnih financah (Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13, 55/15 – ZFisP in 96/15 – ZIPRS1617, 13/18 in 195/20 – odl. US) in 98. člena Statuta Občine Prebold (Uradni list RS, št. 52/13 in 45/14) je Občinski svet Občine Prebold na 28. redni seji dne 7. aprila 2022 sprejel

ODLOK o rebalansu proračuna Občine Prebold za leto 2022

1. SPLOŠNA DOLOČBA

1. člen

(vsebina odloka)

S tem odlokom se za Občino Prebold za leto 2022 določajo proračun, postopki izvrševanja proračuna ter obseg zadolževanja in poroštev občine in javnega sektorja na ravni občine (v nadaljnjem besedilu: proračun).

2. VIŠINA SPLOŠNEGA DELA PRORAČUNA IN STRUKTURA POSEBNEGA DELA PRORAČUNA

2. člen

(sestava proračuna in višina splošnega dela proračuna)

V splošnem delu proračuna so prikazani prejemki in izdatki po ekonomski klasifikaciji do ravni kontov.

Splošni del proračuna se na ravni podskupin kontov določa v naslednjih zneskih:

		v EUR
A. BILANCA PRIHODKOV IN ODHODKOV		
	Skupina/Podskupina kontov/ Konto/Podkonto	Proračun leta 2022
I.	SKUPAJ PRIHODKI (70+71+72+73+74)	6.218.928
	TEKOČI PRIHODKI (70+71)	4.488.599
70	DAVČNI PRIHODKI	3.766.607
	700 Davki na dohodek in dobiček	3.317.787
	703 Davki na premoženje	404.220
	704 Domači davki na blago in storitve	44.500
	706 Drugi davki	100
71	NEDAVČNI PRIHODKI	721.992
	710 Udeležba na dobičku in dohodki od premoženja	555.492

	711 Takse in pristojbine	5.000
	712 Denarne kazni	9.000
	713 Prihodki od prodaje blaga in storitev	27.500
	714 Drugi nedavčni prihodki	125.000
72	KAPITALSKI PRIHODKI	50.000
	720 Prihodki od prodaje osnovnih sredstev	0
	721 Prihodki od prodaje zalog	0
	722 Prihodki od prodaje zemljišč in neopredmetenih dolgoročnih sredstev	50.000
73	PREJETE DONACIJE	45.000
	730 Prejete donacije iz domačih virov	45.000
	731 Prejete donacije iz tujine	0
74	TRANSFERNI PRIHODKI	1.635.328
	740 Transferni prihodki iz drugih javnofinančnih institucij	1.453.074
	741 Prejeta sredstva iz državnega proračuna iz sredstev proračuna EU	182.255
II.	SKUPAJ ODHODKI (40+41+42+43)	6.080.501
40 T	EKOČI ODHODKI	1.277.965
	400 Plače in drugi izdatki zaposlenim	292.790
	401 Prispevki delodajalcev za socialno varnost	47.880
	402 Izdatki za blago in storitve	870.295
	403 Plačila domačih obresti	6.000
	409 Rezerve	61.000
41	TEKOČI TRANSFERI	2.139.976
	410 Subvencije	218.000
	411 Transferi posameznikom in gospodinjstvom	1.231.547
	412 Transferi neprofitnim organizacijam in ustanovam	174.024
	413 Drugi tekoči domači transferi	516.405
	414 Tekoči transferi v tujino	0
42	INVESTICIJSKI ODHODKI	2.526.137
	420 Nakup in gradnja osnovnih sredstev	2.526.137
43	INVESTICIJSKI TRANSFERI	136.423
	431 Investicijski transferi pravnim in fiz. osebam, ki niso PU	91.600
	432 Investicijski transferi PU	44.823
III.	PRORAČUNSKI PRESEŽEK (I.-II.) (PRORAČUNSKI PRIMANJKLJAJ)	138.427
B.	RAČUN FINANČNIH TERJATEV IN NALOŽB	
IV.	PREJETA VRAČILA DANIH POSOJIL IN PRODAJA KAPITALSKIH DELEŽEV (750+751+752)	0
75	PREJETA VRAČILA DANIH POSOJIL	0
	750 Prejeta vračila danih posojil	
	751 Prodaja kapitalskih deležev	
	752 Kupnine iz naslova privatizacije	
V.	DANA POSOJILA IN POVEČANJE KAPITALSKIH DELEŽEV (440+441+442+443)	0
44	DANA POSOJILA IN POVEČANJE KAPITALSKIH DELEŽEV	0
	440 Dana posojila	
	441 Povečanje kapitalskih deležev in naložb	
	442 Poraba sredstev kupnin iz naslova privatizacije	

	443 Povečanje namenskega premoženja v javnih skladih in drugih osebah javnega prava, ki imajo premoženje v svoji lasti	
VI.	PREJETA MINUS DANA POSOJILA IN SPREMEMBE KAPITALSKIH DELEŽEV (IV.-V.)	0
C.	RAČUN FINANCIRANJA	
VII.	ZADOLŽEVANJE (500)	
50	ZADOLŽEVANJE	0
	500 Domače zadolževanje	, 0
VIII.	ODPLAČILA DOLGA (550)	
55	ODPLAČILA DOLGA	455.776
	550 Odplačila domačega dolga	455.776
IX.	SPREMEMBA STANJA SREDSTEV NA RAČUNU	-317.349
X.	NETO ZADOLŽEVANJE (VII.-VIII.)	455.776
XI.	NETO FINANCIRANJE (VI.+VII.-VIII.-IX.)	138.427
	STANJE SREDSTEV NA RAČUNIH DNE 31. 12. PRETEKLEGA LETA	445.917
	9009 Splošni sklad za drugo	445.917

Posebni del proračuna sestavljajo finančni načrti neposrednih uporabnikov, ki so razdeljeni na naslednje programske dele: področja proračunske porabe, glavne programe in podprograme, predpisane s programsko klasifikacijo izdatkov občinskih proračunov. Podprogram je razdeljen na proračunske postavke, te pa na podskupine kontov in konte, določene s predpisanim kontnim načrtom.

Posebni del proračuna do ravni proračunskih postavk – kontov in načrt razvojnih programov sta priložila k temu odloku in se objavita na spletni strani Občine Prebold.

Načrt razvojnih programov sestavljajo projekti.

2. POSTOPKI IZVRŠEVANJA PRORAČUNA

3. člen

(izvrševanje proračuna)

Proračun se izvršuje na ravni proračunske postavke – konta.

4. člen

(namenski prihodki in odhodki proračuna)

Namenski prihodki proračuna so določeni v prvem stavku prvega odstavka 43. člena ZJF in drugi prihodki, ki jih določi občina.

5. člen

(prerazporejanje pravic porabe)

Osnova za prerazporejanje pravic porabe je zadnji sprejeti proračun, spremembe proračuna ali rebalans proračuna.

O prerazporeditvah pravic porabe v posebnem delu proračuna (finančnem načrtu neposrednega uporabnika) med podprogrami v okviru glavnih programov odloča na predlog neposrednega uporabnika župan.

Župan s poročilom o izvrševanju proračuna v mesecu juliju in konec leta z zaključnim računom poroča občinskemu svetu o veljavnem proračunu za leto 2022 in njegovi realizaciji.

6. člen

(največji dovoljeni obseg prevzetih obveznosti v breme proračunov prihodnjih let)

Neposredni uporabnik lahko v tekočem letu razpiše javno naročilo za celotno vrednost projekta, ki je vključen v načrt razvojnih programov, če so zanj načrtovane pravice porabe na proračunskih postavkah v sprejetem proračunu.

Skupni obseg prevzetih obveznosti neposrednega uporabnika, ki bodo zapadle v plačilo v prihodnjih letih za investicijske odhodke in investicijske transfere ne sme presegati 70 % pravic porabe v sprejetem finančnem načrtu neposrednega uporabnika, od tega:

1. v letu 2023 35 % navedenih pravic porabe in
2. v ostalih prihodnjih letih 35 % navedenih pravic porabe.

Skupni obseg prevzetih obveznosti neposrednega uporabnika, ki bodo zapadle v plačilo v prihodnjih letih za blago in storitve in za tekoče transfere, ne sme presegati 40 % pravic porabe v sprejetem finančnem načrtu neposrednega uporabnika.

Omejitve iz prvega in drugega odstavka tega člena ne veljajo za prevzemanje obveznosti z najemnimi pogodbami, razen če na podlagi teh pogodb lastninska pravica preide oziroma lahko preide iz najemodajalca na najemnika, in prevzemanje obveznosti za dobavo elektrike, telefona, vode, komunalnih storitev in drugih storitev, potrebnih za operativno delovanje neposrednih uporabnikov.

Prevzete obveznosti iz drugega in tretjega odstavka tega člena se načrtujejo v finančnem načrtu neposrednega uporabnika in načrtu razvojnih programov.

7. člen

(spreminjanje načrta razvojnih programov)

Predstojnik neposrednega uporabnika župan lahko spreminja vrednost projektov v načrtu razvojnih programov. Projekte, katerih vrednost se spremeni za več kot 20 % mora predhodno potrditi občinski svet.

Projekti, za katere se zaradi prenosa plačil v tekoče leto, zaključek financiranja prestavi iz predhodnega v tekoče leto, se uvrstijo v načrt razvojnih programov po uveljavitvi proračuna.

Novi projekti se uvrstijo v načrt razvojnih programov na podlagi odločitve občinskega sveta.

8. člen

(proračunski skladi)

Proračunski skladi so:

1. proračun proračunske rezerve, oblikovane po ZJF.

Proračunska rezerva se v letu 2022 oblikuje v višini 20.000,00 eurov.

Na predlog za finance pristojnega organa občinske uprave odloča o uporabi sredstev proračunske rezerve za namene iz drugega odstavka 49. člena ZJF župan in o tem s pisnimi poročili obvešča občinski svet.

4. POSEBNOSTI UPRAVLJANJA IN PRODAJE STVARNEGA IN FINANČNEGA PREMOŽENJA DRŽAVE

9. člen

Če so izpolnjeni pogoji iz tretjega odstavka 77. člena ZJF, lahko župan dolžniku do višine 500 eurov odpiše oziroma delno odpiše plačilo dolga.

5. OBSEG ZADOLŽEVANJA IN POROŠTEV OBČINE IN JAVNEGA SEKTORJA

10. člen

(obseg zadolževanja občine in izdanih poroštev občine)

Zaradi kritja presežkov odhodkov nad prihodki v bilanci prihodkov in odhodkov, presežkov izdatkov nad prejemki v računu finančnih terjatev in naložb ter odplačila dolgov v računu financiranja se občina za proračun leta 2022 ne bo zadolžila.

Obseg poroštev občine za izpolnitev obveznosti javnih zavodov in javnih podjetij, katerih ustanoviteljica je Občina Prebold, v letu 2022 je 0 EUR.

11. člen

(obseg zadolževanja javnih zavodov in javnih podjetij ter obseg zadolževanja in izdanih poroštev pravnih oseb, v katerih ima občina odločujoč vpliv na upravljanje)

Pravne osebe javnega sektorja na ravni občine (javni zavodi in javna podjetja, katerih ustanoviteljica je občina) se v letu 2022 ne smejo zadolževati.

Pravne osebe, v katerih ima občina odločujoč vpliv na upravljanje, se v letu 2022 ne smejo zadolžiti.

6. PREHODNE IN KONČNE DOLOČBE

12. člen

(začasno financiranje v letu 2023)

V obdobju začasnega financiranja Občine Prebold v letu 2023, če bo začasno financiranje potrebno, se uporablja ta odlok in sklep o določitvi začasnega financiranja.

13. člen

(uveljavitev odloka)

Ta odlok začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.

Št. 410-0003/2022

Prebold, dne 7. aprila 2022

Župan
Občine Prebold
Vinko Debelak

SLOVENSKE KONJICE

1076. Zaključni račun proračuna Občine Slovenske Konjice za leto 2021

Na podlagi 98. člena Zakona o javnih financah (Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13, 55/15 – ZFisP, 96/15 – ZIPRS1617, 13/18 in 195/20 – odl. US) in 81. člena Statuta Občine Slovenske Konjice (Uradni list RS, št. 87/15 in 12/16 – popr. in 69/17) je Občinski svet Občine Slovenske Konjice na 23. redni seji dne 31. 3. 2022 sprejel

ZAKLJUČNI RAČUN proračuna Občine Slovenske Konjice za leto 2021

1. člen

Sprejme se zaključni račun proračuna Občine Slovenske Konjice za leto 2021.

2. člen

Zaključni račun izkazuje:

A. BILANCA PRIHODKOV IN ODHODKOV		v EUR
I.	SKUPAJ PRIHODKI (70+71+72+73+74+78)	17.262.826,13
	TEKOČI PRIHODKI (70+71)	12.727.865,70
70	DAVČNI PRIHODKI	11.095.672,04
700	Davki na dohodek in dobiček	9.455.028,00
703	Davki na premoženje	1.358.248,34
704	Domači davki na blago in storitve	282.395,70
71	NEDAVČNI PRIHODKI	1.632.193,66

710	Udeležba na dobičku in dohodki od premoženja	1.240.982,10
711	Takse in pristojbine	15.702,68
712	Globe in druge denarne kazni	45.000,18
713	Prihodki od prodaje blaga in storitev	31.817,74
714	Drugi nedavčni prihodki	298.690,96
72	KAPITALSKI PRIHODKI	1.009.446,51
720	Prihodki od prodaje osnovnih sredstev	72.492,73
722	Prihodki od prodaje zemljišč in nematerialnega premoženja	936.953,78
73	PREJETE DONACIJE	1.945,52
730	Prejete donacije iz domačih virov	1.945,52
731	Prejete donacije iz tujine	0,00
74	TRANSFERNI PRIHODKI	3.503.296,52
740	Transforni prihodki iz drugih javnofinančnih institucij	3.348.542,87
741	Prejeta sredstva iz državnega proračuna iz sredstev proračuna Evropske unije	154.753,65
78	PREJETA SREDSTVA IZ EVROPSKE UNIJE	20.271,88
786	Ostala prejeta sredstva iz proračuna Evropske unije	0,00
787	Prejeta sredstva od drugih evropskih institucij in iz drugih držav	20.271,88
II.	SKUPAJ ODHODKI (40+41+42+43)	15.925.131,92
40	TEKOČI ODHODKI	2.802.387,40
400	Plače in drugi izdatki zaposlenim	614.633,12
401	Prispevki delodajalcev za socialno varnost	98.659,07
402	Izdatki za blago in storitve	1.922.189,10
403	Plačila domačih obresti	15.076,11
409	Rezerve	151.830,00
41	TEKOČI TRANSFERI	5.457.179,66
410	Subvencije	68.721,22
411	Transferi posameznikom in gospodinjstvom	3.464.722,92
412	Transferi neprofitnim organizacijam in ustanovam	324.869,31
413	Drugi tekoči domači transferi	1.598.866,21
42	INVESTICIJSKI ODHODKI	7.294.214,57
420	Nakup in gradnja osnovnih sredstev	7.294.214,57
43	INVESTICIJSKI TRANSFERI	371.350,29
431	Investicijski transferi pravnim in fizičnim osebam, ki niso proračunski uporabniki	89.370,00
432	Investicijski transferi proračunskim uporabnikom	281.980,29
	PRORAČUNSKI PRIMANJKLJAJ (I.-II.)	1.337.694,21
B. RAČUN FINANČNIH TERJATEV IN NALOŽB		
IV.	PREJETA VRAČILA DANIH POSOJIL IN PRODAJA KAPITALSKIH DELEŽEV (75)	0,00
75	PREJETA VRAČILA DANIH POSOJIL IN PRODAJA KAPITALSKIH DELEŽEV	0,00
750	Prejeta vračila danih posojil	0,00
751	Prodaja kapitalskih deležev	0,00
752	Kupnine iz naslova privatizacije	0,00
V.	DANA POSOJILA IN POVEČANJE KAPITALSKIH DELEŽEV (44)	0,00
44	DANA POSOJILA IN POVEČANJE KAPITALSKIH DELEŽEV	0,00

440	Dana posojila	0,00
441	Povečanje kapitalskih deležev in naložb	0,00
442	Poraba sredstev kupnin iz naslova privatizacije	0,00
VI.	PREJETA MINUS DANA POSOJILA IN SPREMEMBE KAPITALSKIH DELEŽEV (IV.-V.)	0,00
C. RAČUN FINANCIRANJA		
VII.	ZADOLŽEVANJE (50)	200.000,00
50	ZADOLŽEVANJE	200.000,00
500	Domače zadolževanje	200.000,00
VIII.	ODPLAČILA DOLGA (55)	585.709,22
55	ODPLAČILA DOLGA	585.709,22
550	Odplačila domačega dolga	585.709,22
IX.	POVEČANJE (ZMANJŠANJE) SREDSTEV NA RAČUNIH (I.+IV.+VII.-II.-V.-VIII.)	951.984,99
X.	NETO ZADOLŽEVANJE (VII.-VIII.)	-385.709,22
XI.	NETO FINANCIRANJE (VI.+VII.-VIII.-IX.-III.)	-1.337.694,21
XII.	STANJE SREDSTEV NA RAČUNIH 31. 12. PRETEKLEGA LETA	2.466.345,34
9009	Splošni sklad za drugo	2.466.345,34

3. člen

Zaključni račun proračuna Občine Slovenske Konjice za leto 2021 sestavljajo splošni in posebni del ter načrt razvojnih programov. Splošni del na nivoju trimestrnih kontov se objavi v Uradnem listu Republike Slovenije, ostali deli pa na spletni strani občine.

4. člen

Zaključni račun začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.

Št. 4500-0001/2022(110)

Slovenske Konjice, dne 31. marca 2022

Župan
Občine Slovenske Konjice
Darko Ratajc

1077. Odlok o rebalansu 1 proračuna Občine Slovenske Konjice za leto 2022

Na podlagi 29. člena Zakona o lokalni samoupravi (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 76/08, 79/09, 51/10, 40/12 – ZUJF, 14/15 – ZUUJFO, 11/18 – ZSPDLS-1, 30/18, 61/20 – ZIUZEOP-A in 80/20 – ZIUOOPE), 29. člena Zakona o javnih financah (Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13, 55/15 – ZFisP in 96/15 – ZIPRS1617, 13/18 in 195/20 – odl. US) ter 77. člena Statuta Občine Slovenske Konjice (Uradni list RS, št. 87/15 in 12/16 – popr. in 69/17) je Občinski svet Občine Slovenske Konjice na 23. redni seji dne 31. 3. 2022 sprejel

ODLOK o rebalansu 1 proračuna Občine Slovenske Konjice za leto 2022

1. člen

V Odloku o proračunu Občine Slovenske Konjice za leto 2022 (Uradni list RS, št. 205/21) se drugi odstavek 2. člena spremeni tako, da se glasi:

»Splošni del proračuna se na ravni podskupin kontov določa v naslednjih zneskih:

A. BILANCA PRIHODKOV IN ODHODKOV		v EUR
I.	SKUPAJ PRIHODKI (70+71+72+73+74+78)	15.480.742,00
	TEKOČI PRIHODKI (70+71)	12.941.515,00
70	DAVČNI PRIHODKI	11.249.705,00
700	Davki na dohodek in dobiček	9.776.205,00
703	Davki na premoženje	1.215.000,00
704	Domači davki na blago in storitve	258.500,00
71	NEDAVČNI PRIHODKI	1.691.810,00
710	Udeležba na dobičku in dohodki od premoženja	1.156.410,00
711	Takse in pristojbine	10.000,00
712	Globe in druge denarne kazni	25.000,00
713	Prihodki od prodaje blaga in storitev	41.500,00
714	Drugi nedavčni prihodki	458.900,00
72	KAPITALSKI PRIHODKI	160.000,00
720	Prihodki od prodaje osnovnih sredstev	60.000,00
722	Prihodki od prodaje zemljišč in nematerialnega premoženja	100.000,00
73	PREJETE DONACIJE	5.000,00
730	Prejete donacije iz domačih virov	5.000,00
731	Prejete donacije iz tujine	0,00
74	TRANSFERNI PRIHODKI	2.196.337,00
740	Transferni prihodki iz drugih javnofinančnih institucij	1.557.727,00
741	Prejeta sredstva iz državnega proračuna iz sredstev proračuna Evropske unije	638.610,00
78	PREJETA SREDSTVA IZ EVROPSKE UNIJE	177.890,00
786	Ostala prejeta sredstva iz proračuna Evropske unije	0,00
787	Prejeta sredstva od drugih evropskih institucij in iz drugih držav	177.890,00
II.	SKUPAJ ODHODKI (40+41+42+43)	17.354.514,00
40	TEKOČI ODHODKI	3.446.190,00
400	Plače in drugi izdatki zaposlenim	693.600,00
401	Prispevki delodajalcev za socialno varnost	108.900,00
402	Izdatki za blago in storitve	2.341.900,00
403	Plačila domačih obresti	25.000,00
409	Rezerve	276.790,00
41	TEKOČI TRANSFERI	5.943.286,00
410	Subvencije	74.000,00
411	Transferi posameznikom in gospodinjstvom	3.857.766,00
412	Transferi neprofitnim organizacijam in ustanovam	374.240,00
413	Drugi tekoči domači transferi	1.637.280,00
42	INVESTICIJSKI ODHODKI	7.715.010,00
420	Nakup in gradnja osnovnih sredstev	7.715.010,00
43	INVESTICIJSKI TRANSFERI	250.028,00
431	Investicijski transferi pravnim in fizičnim osebam, ki niso proračunski uporabniki	70.000,00
432	Investicijski transferi proračunskim uporabnikom	180.028,00
	PRORAČUNSKI PRIMANJLJAJ (I.-II.)	-1.873.772,00

B. RAČUN FINANČNIH TERJATEV IN NALOŽB		
IV.	PREJETA VRAČILA DANIH POSOJIL IN PRODAJA KAPITALSKIH DELEŽEV (75)	0,00
75	PREJETA VRAČILA DANIH POSOJIL IN PRODAJA KAPITALSKIH DELEŽEV	0,00
750	Prejeta vračila danih posojil	0,00
751	Prodaja kapitalskih deležev	0,00
752	Kupnine iz naslova privatizacije	0,00
V.	DANA POSOJILA IN POVEČANJE KAPITALSKIH DELEŽEV (44)	0,00
44	DANA POSOJILA IN POVEČANJE KAPITALSKIH DELEŽEV	0,00
440	Dana posojila	0,00
441	Povečanje kapitalskih deležev in naložb	0,00
442	Poraba sredstev kupnin iz naslova privatizacije	0,00
VI.	PREJETA MINUS DANA POSOJILA IN SPREMEMBE KAPITALSKIH DELEŽEV (IV.-V.)	0,00
C. RAČUN FINANCIRANJA		
VII.	ZADOLŽEVANJE (50)	350.000,00
50	ZADOLŽEVANJE	350.000,00
500	Domače zadolževanje	350.000,00
VIII.	ODPLAČILA DOLGA (55)	623.100,00
55	ODPLAČILA DOLGA	623.100,00
550	Odplačila domačega dolga	623.100,00
IX.	POVEČANJE (ZMANJŠANJE) SREDSTEV NA RAČUNIH (I.+IV.+VII.-II.-V.-VIII.)	-2.146.872,00
X.	NETO ZADOLŽEVANJE (VII.-VIII.)	-273.100,00
XI.	NETO FINANCIRANJE (VI.+VII.-VIII.-IX.-III.)	1.873.772,00
XII.	STANJE SREDSTEV NA RAČUNIH 31. 12. PRETEKLEGA LETA	3.418.330,33
9009	Splošni sklad za drugo	3.418.330,33

«

2. člen

Ta odlok začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.

Št. 410-0103/2022(110)

Slovenske Konjice, dne 31. marca 2022

Župan
Občine Slovenske Konjice
Darko Ratajc

1078. Sklep o potrditvi Elaborata o oblikovanju cene oskrbe s pitno vodo v Občini Slovenske Konjice

Na podlagi 16. člena Statuta Občine Slovenske Konjice (Uradni list RS, št. 87/15, 12/16 – popravek in 69/17), Uredbe o metodologiji za oblikovanje cen storitev obveznih občinskih gospodarskih javnih služb varstva okolja (Uradni list RS, št. 87/12, 109/12, 76/17 in 78/19) in 12. člena Odloka o organizaciji javnega komunalnega podjetja (Uradni list RS, št. 27/11) je Občinski svet Občine Slovenske Konjice na 23. redni seji dne 31. 3. 2022 sprejel

S K L E P**o potrditvi Elaborata o oblikovanju cene oskrbe s pitno vodo v Občini Slovenske Konjice****I.**

Občinski svet Občine Slovenske Konjice potrjuje Elaborat o oblikovanju cene oskrbe s pitno vodo v Občini Slovenske Konjice, ki ga je izdelal izvajalec gospodarske javne službe JKP, Javno komunalno podjetje d.o.o. Slovenske Konjice, z datumom izdelave februar 2022.

II.

(1) Občinski svet Občine Slovenske Konjice potrjuje predlog izračuna, da predračunska lastna cena omrežnina vodarina presega 10 % od potrjene cene in se cena zviša iz 4,3878 EUR/mesec za DN 20 na predračunsko lastno ceno 4,8280 EUR/mesec za DN 20.

(2) Obračunska lastna cena vodarine ne presega 10 % od potrjene cene in cena ostane nespremenjena.

III.

Vse zgoraj navedene cene ostajajo nespremenjene do uveljavitve, ki jo bo sprejel Občinski svet Občine Slovenske Konjice po analizi poslovanja JKP.

IV.

Ta sklep se objavi v Uradnem listu Republike Slovenije in začne veljati naslednji dan po objavi. Uporabljati se začne naslednji dan po uveljavitvi, ki jo bo sprejel Občinski svet Občine Slovenske Konjice.

Št. 032-0001/2022-5/3-1(150)

Slovenske Konjice, dne 31. marca 2022

Župan
Občine Slovenske Konjice
Darko Ratajc

1079. Sklep o potrditvi Elaborata o oblikovanju cene izvajanja storitev obvezne občinske gospodarske javne službe ravnanja s komunalnimi odpadki v Občini Slovenske Konjice

Na podlagi 16. člena Statuta Občine Slovenske Konjice (Uradni list RS, št. 87/15, 12/16 – popravek in 69/17), Uredbe o metodologiji za oblikovanje cen storitev obveznih občinskih gospodarskih javnih služb varstva okolja (Uradni list RS, št. 87/12, 109/12, 76/17 in 78/19) in 12. člena Odloka o organizaciji javnega komunalnega podjetja (Uradni list RS, št. 27/11) je Občinski svet Občine Slovenske Konjice na 23. redni seji dne 31. 3. 2022 sprejel

S K L E P

o potrditvi Elaborata o oblikovanju cene izvajanja storitev obvezne občinske gospodarske javne službe ravnanja s komunalnimi odpadki v Občini Slovenske Konjice

I.

Občinski svet Občine Slovenske Konjice potrjuje Elaborat o oblikovanju cene izvajanja storitev obvezne občinske javne službe varstva okolja ravnanje s komunalnimi odpadki v občini Slovenske Konjice, ki ga je izdelal izvajalec gospodarske javne službe JKP, Javno komunalno podjetje d.o.o. Slovenske Konjice, z datumom izdelave februar 2022.

II.

(1) Občinski svet Občine Slovenske Konjice potrjuje predlog izračuna, da obračunske oziroma predračunske lastne cene:

- zbiranje določenih vrst komunalnih odpadkov – izvajanje storitev,
- zbiranje biološko razgradljivih odpadkov – izvajanje storitev,
- zbiranje biološko razgradljivih odpadkov – javna infrastruktura,
- obdelava določenih vrst komunalnih odpadkov – izvajanje storitev,
- obdelava določenih vrst komunalnih odpadkov – javna infrastruktura,

– odlaganje ostankov predelave ali odstranjevanja komunalnih odpadkov – izvajanje storitev,

– odlaganje ostankov predelave ali odstranjevanja komunalnih odpadkov – javna infrastruktura, ne presega 10 % od potrjenih cen in cene ostanejo nespremenjene.

(2) Predračunska lastna cena zbiranje določenih vrst komunalnih odpadkov – javna infrastruktura presega 10 % od potrjene cene in se cena zniža iz 0,0164 €/kg na predračunsko lastno ceno 0,0129 €/kg.

(3) Potrjuje se preračun porazdelitev količin posameznih vrst storitev ravnanja s komunalnimi odpadki med uporabnike.

III.

Vse zgoraj navedene cene in preračun porazdelitve količin posameznih vrst storitev ravnanja s komunalnimi odpadki med uporabniki, ostajajo nespremenjeni do uveljavitve, ki jo bo sprejel Občinski svet Občine Slovenske Konjice po analizi poslovanja JKP.

IV.

Ta sklep se objavi v Uradnem listu Republike Slovenije in začne veljati naslednji dan po objavi. Uporabljati se začne naslednji dan po uveljavitvi, ki jo bo sprejel Občinski svet Občine Slovenske Konjice.

Št. 032-0001/2022-5/3-2(150)

Slovenske Konjice, dne 31. marca 2022

Župan
Občine Slovenske Konjice
Darko Ratajc

1080. Sklepa o potrditvi Elaborata o oblikovanju cene odvajanja komunalne in padavinske odpadne vode v Občini Slovenske Konjice

Na podlagi 16. člena Statuta Občine Slovenske Konjice (Uradni list RS, št. 87/15, 12/16 – popravek in 69/17), Uredbe o metodologiji za oblikovanje cen storitev obveznih občinskih gospodarskih javnih služb varstva okolja (Uradni list RS, št. 87/12, 109/12, 76/17 in 78/19) in 12. člena Odloka o organizaciji javnega komunalnega podjetja (Uradni list RS, št. 27/11) je Občinski svet Občine Slovenske Konjice na 23. redni seji dne 31. 3. 2022 sprejel

S K L E P A

o potrditvi Elaborata o oblikovanju cene odvajanja komunalne in padavinske odpadne vode v Občini Slovenske Konjice

I.

Občinski svet Občine Slovenske Konjice potrjuje Elaborat o oblikovanju cene odvajanja komunalne in padavinske

odpadne vode v Občini Slovenske Konjice, ki ga je izdelal izvajalec gospodarske javne službe JKP, Javno komunalno podjetje d.o.o. Slovenske Konjice, z datumom izdelave februar 2022.

II.

Občinski svet Občine Slovenske Konjice potrjuje predlog izračuna, da obračunska lastna cena omrežnina odvajanje komunalne odpadne vode, obračunska lastna cena omrežnina odvajanja padavinske odpadne vode, obračunska lastna cena odvajanje komunalne odpadne vode in obračunska lastna cena odvajanje padavinske odpadne vode ne presegajo 10 % od potrjene cene in cene ostajajo nespremenjene.

III.

Ta sklep se objavi v Uradnem listu Republike Slovenije in se uporablja od 1. 5. 2022.

Št. 032-0001/2022-5/3-3(150)
Slovenske Konjice, dne 31. marca 2022

Župan
Občine Slovenske Konjice
Darko Ratajc

1081. Sklep o potrditvi Elaborata o oblikovanju cene čiščenja komunalne in padavinske odpadne vode v Občini Slovenske Konjice

Na podlagi 16. člena Statuta Občine Slovenske Konjice (Uradni list RS, št. 87/15, 12/16 – popravek in 69/17), Uredbe o metodologiji za oblikovanje cen storitev obveznih občinskih gospodarskih javnih služb varstva okolja (Uradni list RS, št. 87/12, 109/12, 76/17 in 78/19) in 12. člena Odloka o organizaciji javnega komunalnega podjetja (Uradni list RS, št. 27/11) je

Občinski svet Občine Slovenske Konjice na 23. redni seji dne 31. 3. 2022 sprejel

S K L E P

o potrditvi Elaborata o oblikovanju cene čiščenja komunalne in padavinske odpadne vode v Občini Slovenske Konjice

I.

Občinski svet Občine Slovenske Konjice potrjuje Elaborat o oblikovanju cene čiščenja komunalne in padavinske odpadne vode v Občini Slovenske Konjice, ki ga je izdelal izvajalec gospodarske javne službe JKP, Javno komunalno podjetje d.o.o. Slovenske Konjice, z datumom izdelave februar 2022.

II.

(1) Obračunska lastna cena omrežnina čiščenje komunalne odpadne vode, obračunska lastna cena omrežnina čiščenje padavinske odpadne vode in obračunska lastna cena čiščenje komunalne odpadne vode in obračunska lastna cena čiščenja padavinske odpadne vode ne presegajo 10 % od potrjene cene in cene ostanejo nespremenjene.

(2) Obračunska lastna cena omrežnina črpanja, prevoz in čiščenje greznične gošče in blata MKČN ter obračunska lastna cena storitev črpanja, prevoz in čiščenje greznične gošče in blata MKČN ne presegata 10 % od potrjene cene in ceni ostane nespremenjeni.

III.

Ta sklep se objavi v Uradnem listu Republike Slovenije in se uporablja od 1. 5. 2022.

Št. 032-0001/2022-5/3-4(150)
Slovenske Konjice, dne 31. marca 2022

Župan
Občine Slovenske Konjice
Darko Ratajc

VSEBINA**VLADA**

- | | | |
|-------|---|------|
| 1070. | Uredba o varovanju tajnih podatkov | 3185 |
| 1071. | Uredba o določitvi nalog kontaktne točke za spodbujanje rabe obnovljivih virov energije | 3243 |
| 1072. | Uredba o nadomestilu za izrabo prostora za proizvodno napravo na veter | 3245 |

MINISTRSTVA

- | | | |
|-------|---|------|
| 1073. | Pravilnik o spremembah in dopolnitvah Pravilnika o temeljnih kvalifikacijah za voznike motornih vozil v cestnem prometu | 3247 |
|-------|---|------|

OBČINE**PREBOLD**

- | | | |
|-------|---|------|
| 1074. | Zaključni račun proračuna Občine Prebold za leto 2021 | 3253 |
| 1075. | Odlok o rebalansu proračuna Občine Prebold za leto 2022 | 3253 |

SLOVENSKE KONJICE

- | | | |
|-------|---|------|
| 1076. | Zaključni račun proračuna Občine Slovenske Konjice za leto 2021 | 3255 |
| 1077. | Odlok o rebalansu 1 proračuna Občine Slovenske Konjice za leto 2022 | 3256 |
| 1078. | Sklep o potrditvi Elaborata o oblikovanju cene oskrbe s pitno vodo v Občini Slovenske Konjice | 3257 |
| 1079. | Sklep o potrditvi Elaborata o oblikovanju cene izvajanja storitev obvezne občinske gospodarske javne službe ravnanja s komunalnimi odpadki v Občini Slovenske Konjice | 3258 |
| 1080. | Sklepa o potrditvi Elaborata o oblikovanju cene odvajanja komunalne in padavinske odpadne vode v Občini Slovenske Konjice | 3258 |
| 1081. | Sklep o potrditvi Elaborata o oblikovanju cene čiščenja komunalne in padavinske odpadne vode v Občini Slovenske Konjice | 3259 |

Uradni list RS – Mednarodne pogodbe, št. 6/22**VSEBINA**

- | | | |
|-----|--|----|
| 17. | Uredba o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Madžarske o sodelovanju pri gospodarskem in družbenem razvoju narodnostno mešanega območja na obeh straneh slovensko-madžarske meje | 93 |
|-----|--|----|

Uradni list RS – Razglasni del

Razglasni del je objavljen v elektronski izdaji št. 50/22 na spletnem naslovu: www.uradni-list.si

VSEBINA

- | | |
|-----------------------|------|
| Razpisi delovnih mest | 1195 |
| Druge objave | 1196 |

ISSN 1318-0576



Izdajatelj Služba Vlade RS za zakonodajo – v. d. direktorica mag. Mateja Lekan Štrukelj • Založnik Uradni list Republike Slovenije d.o.o. – direktor Denis Stroligo • Priprava Uradni list Republike Slovenije d.o.o. • Naročnina za obdobje 1. 1. do 31. 12. 2022 je 599 EUR (brez DDV), v ceno posameznega Uradnega lista Republike Slovenije je vračunan 5% DDV • Reklamacije se upoštevajo le mesec dni po izidu vsake številke • Uredništvo in uprava Ljubljana, Dunajska cesta 167 • Poštni predal 379 • Telefon tajništvo (01) 2001 821, računovodstvo in naročnine (01) 2001 863, telefaks (01) 2001 825, prodaja (01) 2001 838, preklici (01) 2001 842, telefaks (01) 4250 199, uredništvo (01) 2001 841/868, uredništvo (javni razpisi ...) (01) 2001 842, uredništvo – telefaks (01) 4250 199 • Internet: www.uradni-list.si – uredništvo e-pošta: objave@uradni-list.si • Transakcijski račun 02922-0011569767