Neuradno prečiščeno besedilo Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih obsega:
- Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/07 z dne 1. 6. 2007),
- Uredbo o dopolnitvi Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 86/11 z dne 28. 10. 2011).

U R E D B A
o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih

(neuradno prečiščeno besedilo št. 1)

I. SPLOŠNE DOLOČBE

1. člen
(namen uredbe)

(1) Ta uredba določa fizične, organizacijske in tehnične ukrepe ter postopke varovanja tajnih podatkov v komunikacijskih in informacijskih sistemih, ki jih morajo upoštevati in izvajati vsi organi in organizacije iz drugega in tretjega odstavka 1. člena Zakona o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo; v nadaljnjem besedilu: zakon).

(2) Pri varovanju tajnih podatkov drugih držav ali mednarodnih organizacij v komunikacijskih in informacijskih sistemih se poleg ali namesto ukrepov, predpisanih s to uredbo, izvajajo tudi drugi ukrepi, določeni z mednarodno pogodbo ali sprejetimi mednarodnimi obveznostmi.

2. člen
(namen fizičnih, organizacijskih in tehničnih ukrepov ter postopkov varovanja)

(1) Namen fizičnih, organizacijskih in tehničnih ukrepov ter postopkov varovanja tajnih podatkov je, da se vzpostavi sistem minimalnih standardov, postopkov in tehničnih ukrepov, ki ustreza stopnji tajnosti tajnih podatkov v komunikacijskih in informacijskih sistemih ter onemogoča njihovo razkritje nepooblaščenim osebam.

(2) S fizičnimi, organizacijskimi in tehničnimi ukrepi ter postopki varovanja v komunikacijskih in informacijskih sistemih, v katerih se obravnavajo tajni podatki (v nadaljnjem besedilu: sistemi), se zagotavljajo tajnost, celovitost in razpoložljivost teh podatkov ter celovitost in razpoložljivost samih sistemov.

(3) Z ukrepi in postopki iz prejšnjega odstavka se v sistemih preprečujejo dostop do tajnih podatkov nepooblaščenim uporabnikom, razkritje tajnih podatkov nepoklicanim osebam, možnost za zavrnitev dostopa do tajnih podatkov pooblaščenim uporabnikom ter zloraba, nepooblaščena sprememba ali izbris tajnih podatkov.

(4) Za izvajanje ukrepov in postopkov varovanja tajnih podatkov v posameznem sistemu je odgovoren predstojnik organa ali organizacije.

(5) Za vzpostavitev, vodenje in vzdrževanje sistema predstojnik organa ali organizacije imenuje upravljavca sistema.

3. člen
(pomen izrazov)

Posamezni izrazi, uporabljeni v tej uredbi, imajo naslednji pomen:

- informacijska varnost zajema določanje in uporabo ukrepov varovanja tajnih podatkov, ki se obravnavajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov;
- varnostno dovoljenje za delovanje sistema je pisni sklep, s katerim se dovoljuje obravnavanje tajnih podatkov v sistemu in ki potrjuje izvajanje vseh ukrepov in postopkov za zagotavljanje varnega delovanja sistema;
- ključne sestavine sistema so strežniki, usmerjevalniki in delilniki prometa, oprema za upravljanje in nadzor, aktivna oprema za prenos podatkov v nešifrirani obliki, oprema za šifrirno zaščito podatkov, varnostne pregrade, oprema za odkrivanje in zaščito pred vdori, oprema za izdelavo varnostnih kopij;
- varnostni način delovanja sistema nam pove, kako se izvaja nadzor dostopa do sistema. Razlikujemo tri varnostne načine delovanja: neselektiven, selektiven in dvojno selektiven. Razlikujejo se glede na potrebno dovoljenje uporabnikov za dostop do tajnih podatkov in pravico po vedenju;
- kritični informacijski varnostni dogodek je vsak dogodek, ki ima ali bi lahko imel za posledico nerazpoložljivost sistema ali njegovih ključnih sestavin, razkritje varovanih podatkov ali izgubo oziroma nezaželeno spremembo podatkov, uničenje ali izgubo opreme in sredstev;
- neželeno elektromagnetno sevanje je sevanje, ki se nekontrolirano razširja in omogoča odtekanje tajnih podatkov;
- širše varnostno okolje sistema (ŠVO) je celotna okolica objekta, v katerem je nameščen sistem;
- ožje varnostno okolje sistema (OVO) je objekt, v katerem je nameščen sistem;
- elektronsko varnostno okolje sistema (EVO) je programska in strojna oprema sistema.

4. člen
(varnostna odobritev sistema)

(1) Vsak predstojnik organa ali organizacije mora pred začetkom obravnavanja tajnih podatkov v sistemu s pisnim sklepom potrditi izvajanje vseh ukrepov in postopkov za zagotovitev varnega delovanja sistema (v nadaljnjem besedilu: varnostno dovoljenje za delovanje sistema).

(2) Pred izdajo varnostnega dovoljenja za delovanje sistema, v katerem se obravnavajo podatki stopnje tajnosti ZAUPNO ali višje, mora predstojnik organa ali organizacije od Urada Vlade Republike Slovenije za varovanje tajnih podatkov dobiti mnenje o varnostni ustreznosti sistema. Uradu Vlade Republike Slovenije za varovanje tajnih podatkov se pred izdajo mnenja o varnostni ustreznosti sistema omogoči varnostni pregled sistema, s katerim preveri izpolnjevanje ukrepov in postopkov za zagotovitev varnega delovanja sistema.

(3) Organ ali organizacija mora o izdaji varnostnega dovoljenja za delovanje sistema obvestiti Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

(4) Urad Vlade Republike Slovenije za varovanje tajnih podatkov vodi evidenco vseh varnostnih dovoljenj za delovanje sistemov.

(5) Ob vsaki spremembi sistema, ki ima oziroma bi lahko imela posledice za varnost v sistemu obravnavanih tajnih podatkov (širitev sistema, tehnološke spremembe, uvajanje novih tehnologij ali storitev itd.), mora upravljavec sistema ponovno izvesti postopek varnostne odobritve sistema.

5. člen
(dokumenti, potrebni za izdajo varnostnega dovoljenja za delovanje sistema)

(1) Vsak upravljavec sistema mora v postopku izdaje varnostnega dovoljenja za delovanje sistema pripraviti:
- načrt varovanja sistema, ki vsebuje opis sistema, načrt sestavin in povezav sistema, varnostne zahteve sistema, varnostna okolja, varnostne protiukrepe in varnostno upravljanje sistema;
- oceno varnostnih tveganj, ki vsebuje oceno trenutnega stanja sistema z oceno stopnje tveganja;
- varnostna navodila za delo v sistemu, ki vsebujejo varnostno upravljanje in organiziranost varnosti sistema, informacijska varnost, načrtovanje ukrepov ob nepredvidenih dogodkih, upravljanje in spreminjanje konfiguracije/nastavitev sistema, splošna varnostna navodila za uporabnike in odgovorno osebje.

(2) Struktura in vsebina varnostnih dokumentov sistema iz prejšnjega odstavka sta opredeljeni v prilogah 4, 5 in 6 te uredbe.

(3) V postopku izdaje varnostnega dovoljenja za delovanje sistema, v katerem se obravnavajo podatki stopnje tajnosti ZAUPNO ali višje, morajo biti dokumenti iz prvega odstavka tega člena priloženi k zahtevi za pridobitev mnenja Urada Vlade Republike Slovenije za varovanje tajnih podatkov.

(4) Dokumente iz prvega odstavka tega člena je treba stalno dopolnjevati, najmanj enkrat letno pa pregledati in preveriti ustreznost ukrepov in postopkov, ki so z njimi določeni.

6. člen
(določitev varnostnega načina delovanja sistema)

(1) Upravljavec sistema mora za vsak svoj sistem pisno opredeliti varnostni način delovanja.

(2) Posamezen sistem lahko deluje:
- neselektivno,
- selektivno,
- dvojno selektivno.

(3) V sistemu z neselektivnim varnostnim načinom delovanja se obravnavajo tajni podatki predvsem za neko ožje ali posebno interesno področje uporabnikov. Pri tem morajo imeti vse osebe, ki pristopajo k sistemu, 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 se obravnavajo tajni podatki različnih stopenj tajnosti. Pri tem morajo imeti vse osebe, ki pristopajo k sistemu, 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 sistemu z dvojno selektivnim varnostnim načinom delovanja se obravnavajo tajni podatki različnih stopenj tajnosti. Pri tem lahko k sistemu selektivno pristopajo 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) Selektivni pristop k sistemu in selektivni dostop do podatkov se rešujeta s pomočjo strojne in programske opreme.

II. FIZIČNI IN ORGANIZACIJSKI UKREPI VAROVANJA

7. člen
(varovanje ključnih in nekaterih drugih sestavin sistema)

(1) Vse ključne in nekatere druge sestavine sistema, s katerimi se obravnavajo tajni podatki v nešifrirani obliki (razen pri prenosu tajnih podatkov po optičnih povezavah v upravnem območju), morajo biti postavljene v prostor, ki je varovan najmanj tako, kot je določeno v Uredbi o varovanju tajnih podatkov (Uradni list RS, št. 74/05) za najvišjo stopnjo tajnosti v sistemu obravnavanih podatkov.

(2) Sestavine sistema iz prejšnjega odstavka morajo biti označene v skladu z Uredbo o varovanju tajnih podatkov.

(3) Ne glede na prvi odstavek tega člena se tajni podatki na nekaterih drugih sestavinah sistema lahko obravnavajo zunaj varnostnega območja, če je prostor ali območje, v katerem se tajni podatek obravnava, fizično ali tehnično varovan, seznanitev nepoklicanih oseb s tajnimi podatki pa onemogočena.

8. člen
(vstop v prostor s ključnimi sestavinami sistema)

(1) Pooblastilo za samostojen vstop v prostor, v katerem so nameščene ključne sestavine sistema, se lahko izda za osebe z dovoljenjem za dostop do tajnih podatkov stopnje tajnosti, ki ustreza najvišji stopnji tajnosti v sistemu obravnavanih podatkov, in katerih delovne naloge so povezane z vzdrževanjem, dograjevanjem, posodabljanjem, upravljanjem, varnostnim nadzorom ali drugim obravnavanjem ključnih sestavin sistema. Pooblastilo se lahko izda v obliki seznama.

(2) Varnostni in sistemski administratorji v sistemih ter strokovnjaki, odgovorni za šifrirno zaščito in upravljanje šifrirnih ključev, so lahko samo osebe z dovoljenjem za dostop do tajnih podatkov stopnje tajnosti, ki ustreza najmanj stopnji tajnosti v sistemu obravnavanih podatkov.

(3) Upravljavec sistema mora seznam vseh oseb, pooblaščenih za samostojen vstop v prostor, v katerem so nameščene ključne sestavine sistema, izobesiti na vidnem mestu v tem prostoru.

(4) Vzorec seznama iz prejšnjega odstavka je v prilogi 1 te uredbe.

9. člen
(vodja informacijske varnosti)

(1) Vsak predstojnik organa ali organizacije določi osebo, odgovorno za izvajanje te uredbe, upravljanje in nadzor nad ukrepi in postopki varovanja tajnih podatkov v sistemu (v nadaljnjem besedilu: vodja informacijske varnosti) in ji podeli ustrezna pisna pooblastila.

(2) Če sistem vsebuje tudi dislocirane enote, lahko predstojnik organa ali organizacije določi osebo, odgovorno za informacijsko varnost dislocirane enote sistema (v nadaljnjem besedilu: lokalni vodja informacijske varnosti).

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

(4) Predstojnik organa ali organizacije o imenovanju vodje informacijske varnosti oziroma preklicu imenovanja obvesti Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

(5) Vzorec obvestila o imenovanju vodje informacijske varnosti je v prilogi 2 te uredbe.

10. člen
(obveščanje o kritičnem informacijskem varnostnem dogodku)

Vodja informacijske varnosti oziroma predstojnik organa ali organizacije mora poskrbeti, da se o kritičnem informacijskem dogodku ter o ukrepih, sprejetih za preprečitev posledic dogodka, pisno obvesti Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

III. TEHNIČNI UKREPI IN POSTOPKI VAROVANJA

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

(1) Upravljavec sistema mora 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.

(2) Primerne načine in postopke za identifikacijo in overitev dostopa uporabnikov v sistem določi komisija iz 15. člena te uredbe.

12. člen
(selekcija dostopa uporabnikov do podatkov)

Upravljavec sistema vsakemu uporabniku sistema dostop omeji le na tiste tajne podatke, ki jih potrebuje za opravljanje svojih nalog oziroma do katerih je upravičen na podlagi pooblastila, določenega z zakonom ali predpisom, izdanim na podlagi zakona. Na podlagi tako določenih pravic upravljavec sistema vzpostavi in vzdržuje seznam uporabnikov sistema, iz katerega so za vsakega uporabnika sistema razvidni njegovi identifikacijski podatki, in njegove pravice dostopa do posameznih tajnih podatkov (v nadaljnjem besedilu: varnostna shema). Ob spremembi pravic posameznega uporabnika (na primer: prekinitev

delovnega razmerja, premestitev in podobno) mora biti varnostna shema ustrezno popravljena, sprememba pa ustrezno dokumentirana.

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

(1) Spremljanje in nadzor pristopa v sistem in dostopa do tajnih podatkov stopnje tajnosti ZAUPNO ali višje mora omogočiti ugotavljanje, kdo, kdaj in od kod je vstopil v sistem oziroma kdaj so bili posamezni tajni podatki v sistemu obravnavani, in sicer tako, da je mogoče ukrepati ob sumu nepooblaščenega vstopa v sistem ali nepooblaščenega dostopa do tajnih podatkov v sistemu ter pozneje rekonstruirati posamezne dostope do tajnih podatkov v sistemu.

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

(3) Zapise o vstopih v sistem in dostopih do podatkov mora upravljavec sistema voditi in hraniti v skladu z Uredbo o varovanju tajnih podatkov.

14. člen
(zaščita tajnih podatkov pri prenosu zunaj varnostnih območij)

(1) Prenos tajnih podatkov po komunikacijskih in informacijskih sistemih zunaj varnostnih območij oziroma upravnega območja je dovoljen le v šifrirani obliki.

(2) V sistemih se lahko uporabljajo le šifrirne rešitve, ki jih potrdi komisija iz 15. člena te uredbe, kolikor v drugih zakonskih predpisih ni drugače določeno.

(3) Izjemoma se lahko v izrednih okoliščinah tajni podatki stopnje tajnosti INTERNO, ZAUPNO in TAJNO prenašajo v nešifrirani obliki. Za vsak tak prenos mora izdati dovoljenje predstojnik organa ali oseba, ki jo je pooblastil. Take izredne okoliščine so:
- preteče ali dejanske krize, spopad ali vojne razmere ali
- kadar je hitrost dostave bistvenega pomena in pri tem niso na voljo sredstva in metode za šifrirno zaščito ter se ocenjuje, da je možnost zlorabe poslanih tajnih podatkov zelo majhna.

(4) Šifrirani tajni podatki se z uporabo pomnilnih medijev zunaj varnostnega oziroma upravnega območja prenašajo skladno s tem členom.

(5) Nešifrirani tajni podatki se z uporabo pomnilnih medijev zunaj varnostnih območij oziroma upravnega območja prenašajo skladno z Uredbo o varovanju tajnih podatkov.

15. člen
(komisija za informacijsko varnost)

(1) Vlada Republike Slovenije ustanovi medresorsko komisijo za informacijsko varnost (v nadaljnjem besedilu: komisija), ki je sestavljena iz predstavnikov Ministrstva za javno upravo, Ministrstva za notranje zadeve, Ministrstva za obrambo, Ministrstva za zunanje zadeve, Slovenske obveščevalno varnostne agencije in Urada Vlade Republike Slovenije za varovanje tajnih podatkov.

(2) Komisija uredi način svojega dela s poslovnikom, h kateremu da soglasje vlada.

(3) Komisija pripravlja tehnične in normativne rešitve za varovanje tajnih podatkov v komunikacijskih in informacijskih sistemih.

16. člen
(povezovanje sistemov)

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

(2) S povezavo sistemov iz prejšnjega odstavka se morajo strinjati upravljavci sistemov.

(3) Z internetom je dovoljeno povezati sisteme, v katerih se obravnavajo tajni podatki stopnje tajnosti INTERNO.

(4) Povezovanje sistemov mora biti izvedeno skladno z varnostnimi zahtevami za povezovanje sistemov, ki jih pripravi komisija.

17. 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.

(2) Zaščito proti neželenemu elektromagnetnemu sevanju zagotavljajo upravljavci sistemov, v katerih se obravnavajo tajni podatki in so del načrta varovanja. O ugotovitvah meritev obveščajo Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

(3) Meritve proti neželenemu elektromagnetnemu sevanju opravljajo Ministrstvo za obrambo, Policija, Slovenska obveščevalno varnostna agencija in drugi organi, ki jih pooblasti komisija.

(4) Varnostne zahteve za izvajanje zaščite proti neželenemu elektromagnetnemu sevanju pripravi komisija.

Priloga 1: Vzorec seznama vseh oseb, pooblaščenih za vstop v prostor, v katerem so nameščene ključne sestavine sistema

Priloga 2: Vzorec obvestila o imenovanju vodje informacijske varnosti

Priloga 3: Vzorec obvestila o imenovanju upravljavca sistema

Priloga 4: Vzorec dokumenta Načrt varovanja sistema

Priloga 5: Vzorec dokumenta Ocena varnostnih tveganj

Priloga 6: Vzorec dokumenta Varnostna navodila za delo v sistemu

---

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/07) vsebuje naslednje prehodne in končno določbo:

»IV. PREHODNE IN KONČNA DOLOČBA

18. člen
(pridobitev mnenja o varnostni ustreznosti sistema)

Upravljavci sistemov, v katerih se obravnavajo tajni podatki, morajo dobiti mnenje o varnostni ustreznosti sistema iz drugega odstavka 4. člena te uredbe v štirih letih po uveljavitvi te uredbe.

19. člen
(imenovanje upravljavca sistema)

(1) Predstojnik organa oziroma poslovodni organ imenuje upravljavca sistema najpozneje šest mesecev po uveljavitvi te uredbe. O njihovem imenovanju oziroma preklicu imenovanja je treba obvestiti Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

(2) Vzorec obvestila o imenovanju upravljavca sistema je v prilogi 3 te uredbe.

20. člen
(naloge komisije)

(1) Varnostne zahteve za povezovanje sistemov pripravi komisija v enem letu po uveljavitvi te uredbe.

(2) Tehnične in normativne rešitve uporabe šifrirnih sistemov in varnostne zahteve za izvajanje zaščite proti neželenemu elektromagnetnemu sevanju pripravi komisija v šestih mesecih po uveljavitvi te uredbe.

21. člen
(končna določba)

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

Uredba o dopolnitvi Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 86/11) spreminja 18. člen uredbe tako, da se glasi:

»18. člen
(pridobitev mnenja o varnostni ustreznosti sistema)

(1) Upravljavci sistemov, v katerih se obravnavajo tajni podatki, morajo dobiti mnenje o varnostni ustreznosti sistema iz drugega odstavka 4. člena te uredbe v štirih letih po uveljavitvi te uredbe.

(2) Upravljavci sistemov, ki niso pridobili mnenja v skladu s prejšnjim odstavkom, morajo o tem obvestiti Urad Vlade Republike Slovenije za varovanje tajnih podatkov in zaprositi za podaljšanje tega roka najkasneje do 31. decembra 2011. Zaradi objektivnih razlogov lahko Urad Vlade Republike Slovenije za varovanje tajnih podatkov podaljša rok za pridobitev mnenja, a najdlje do 31. decembra 2014.«;

ter vsebuje naslednjo končno določbo:

»2. člen

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