REPUBLIKA SLOVENIJA
URAD VLADE RS ZA VAROVANJE TAJNIH PODATKOV

Gregorčičeva 27, 1000 Ljubljana

T: 01 478 1390
F: 01 478 1399
E: gp.uvtp@gov.si
http://www.uvtp.gov.si/

Številka: 007-36/2017
Datum: 8. 1. 2018
EVA: 2017-1535-0002

GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE
Gp.gs@gov.si

ZADEVA: Predlog zakona o spremembah in dopolnitvah Zakona o tajnih podatkih – predlog za obravnavo

1. Predlog sklepov vlade:

Na podlagi 2. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G in 65/14) je Vlada Republike Slovenije na svoji ……. seji dne ……. sprejela naslednji

SKLEP

Vlada Republike Slovenije je določila besedilo predloga Zakona o spremembah in dopolnitvah Zakona o tajnih podatkih (EVA 2017-1535-0002) ter ga posreduje v obravnavo Državnemu zboru Republike Slovenije.

mag. Lilijana Kozlovič
GENERALNA SEKRETARKA

Priloga:
- Predlog Zakona o spremembah in dopolnitvah Zakona o tajnih podatkih (EVA 2017-1535-0002)

Sklep prejmejo:
- Državni zbor Republike Slovenije
- Služba Vlade Republike Slovenije za zakonodajo

2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:
- Dobran Božič, direktor, Urad Vlade RS za varovanje tajnih podatkov
- Mateja Kapš, sekretarka, Urad Vlade RS za varovanje tajnih podatkov
- Marko Rosandič, podsekretar, Urad Vlade RS za varovanje tajnih podatkov

3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva: /

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:

- Dobran Božič, direktor, Urad Vlade RS za varovanje tajnih podatkov
- Mateja Kapš, sekretarka, Urad Vlade RS za varovanje tajnih podatkov

5. Kratek povzetek gradiva:

Predlagane spremembe in dopolnitve ZTP ne odstopajo od ciljev in načel, na katerih sloni sedanja ureditev tega področja. Poglaviten cilj predlagane novele ZTP je zgolj izboljšati učinkovitost sistema in posledično varnost tajnih podatkov.

Glede na pojmovno razlago in razumevanje na kompleksnem področju tajnih podatkov smo ločili obravnavo in hrambo tajnih podatkov, ki skupaj z nadzorom pomenita varovanje tajnih podatkov.

Sedanji ZTP praktično nima določb, ki bi urejale varovanje tajnih podatkov v KIS in eksplicitno opredeljevale naloge UVTP na tem področju. Predlagana dopolnitev ZTP zato zelo natančno določa sestavne dele sistema in potrebo po izvedbi postopka varnostne odobritve sistemov, v katerih se obravnavajo oziroma hranijo tajni podatki.

Na področju industrijske varnosti je največja novost podrobnejša ureditev preverjanja lastniške strukture organizacije in tako imenovanih povezanih oseb, to je oseb, ki imajo v lasti določen lastniški ali upravljavski delež organizacije, oziroma drugih oseb, ki nadzirajo ali bi lahko izvajale neposreden ali posreden nadzor nad organizacijo oziroma bi lahko vplivale na njeno dejavnost. Z določili, ki se nanašajo na obveznost pristojnih organov, da preverijo, ali povezane osebe niso sodelovale oziroma ne sodelujejo z organizacijami ali skupinami, ki ogrožajo vitalne interese RS ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je RS, se v zakonodajo vnaša jasnejša podlaga za varnostno preverjanje lastniške strukture organizacije.
V predlagani spremembi ZTP so izenačeni tudi pogoji za dostopanje do tajnih podatkov stopnje tajnosti INTERNO za zaposlene v organih in za zaposlene v organizacijah.
Naslednja pomembna novost je, da je predlagatelj v predlogu opredelil način obravnavanja tajnih podatkov v okviru izvajanja naročila, ki lahko poteka v prostorih naročnika ali v prostorih organizacije. S tem določilom se ureja dosedanja zakonska pomanjkljivost na področju industrijske varnosti, ki je predvidevala izdajanje varnostnega dovoljenja organizaciji zgolj v primerih, ko se tajni podatki organizaciji posredujejo v fizični obliki oziroma v njene prostore. S predlagano ureditvijo se zvišuje raven varnostnih standardov na področju industrijske varnosti, ki bodo tako skladni z mednarodnimi varnostnimi standardi in s tujo prakso na tem področju.

Tretji segment, pri katerem se je pokazala potreba po spremembah in dopolnitvah ZTP, je segment osebne varnosti. Veljavni 3. člen ZTP določa osebe, ki lahko v zvezi z opravljanjem svoje funkcije dostopajo do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov.
Glede na dejstvo, da zveza Nato in EU v svojih predpisih dostop do tajnih podatkov Nata in EU (v nadaljnjem besedilu: tuji tajni podatki) dovoljujeta osebam, ki imajo dostop brez dovoljenja za dostop do tujih tajnih podatkov v skladu z nacionalno zakonodajo, je bila RS ob izvedbah inšpekcije Nata in EU v RS vsakokrat opozorjena na preširok krog teh oseb. S predlagano spremembo bi bil dostop do tujih tajnih podatkov brez opravljenega varnostnega preverjanja omogočen le državnim funkcionarjem na najvišjih položajih, to je predsedniku republike, predsedniku vlade, državnega sveta in vrhovnega sodišča ter ministrom in poslancem. Predlog novega 3. člena je tako primerljiv z ureditvami, ki jih imajo v drugih državah članicah zveze Nato in EU, in bi v popolnosti odpravil vse zadržke inšpekcijskih pregledov, ki jih izvajata zveza Nato in EU.

Besedilo sprememb in dopolnitev ZTP je pripravila Medresorska delovna skupine za pripravo sprememb predpisov s področja obravnavanja in varovanja tajnih podatkov, ki je bila ustanovljena s

Sklepom direktorja Urada Vlade RS za varovanje tajnih podatkov, št. 007-7/2013/2 dne 29. 1. 2013, in katere člani so predstavniki tistih ključnih organov, ki se v Republiki Sloveniji v največji meri srečujejo s področjem tajnih podatkov (UVTP, MNZ, Policija, MO, SOVA, MJU, MZZ, MGRT).

6. Presoja posledic za:

a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	**DA/**NE
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	DA/**NE**
c)	administrativno področje	DA/**NE**
č)	gospodarstvo, zlasti za mala in srednja podjetja ter konkurenčnost podjetij	**DA**/NE
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	DA/**NE**
e)	socialno področje	DA/**NE**
f)	dokumente razvojnega načrtovanja: – nacionalne dokumente razvojnega načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna – razvojne dokumente Evropske unije in mednarodnih organizacij	DA/**NE**

7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:

Za učinkovito izvajanje predlaganih sprememb zakona bo Ministrstvo za javno upravo v letu 2018 vzpostavilo kriptografski laboratorij. Ocenjujemo, da bo njegova vzpostavitev stala 150.000 EUR. V letu 2019 pa se bo vzpostavil še TEMPEST laboratorij (gre za zaščito pred neželenim elektromagnetnim sevanjem). Za njegovo vzpostavitev bo ministrstvo namenilo 1.500.000 EUR. Za vzdrževanje obeh laboratorijev ocenjujemo letni strošek 20.000 EUR, s tem da bo v letu 2018 vzdrževanje v višini 10.000 EUR le za kriptografski laboratorij.

(Samo če izberete DA pod točko 6.a.)

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

	Tekoče leto (t)	t + 1	t + 2	t + 3
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) obveznosti za druga javnofinančna sredstva				

II. Finančne posledice za državni proračun

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1

MJU	3130-17-0009 Informacijska varnost	PP170089 Razvoj, vzdrževanje in upravljanje informacijske varnosti	0 EUR	160.000 EUR
SKUPAJ			**0 EUR**	**160.000 EUR**

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:

Novi prihodki	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ		

OBRAZLOŽITEV:

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

V zvezi s predlaganim vladnim gradivom se navedejo predvidene spremembe (povečanje, zmanjšanje):

- prihodkov državnega proračuna in občinskih proračunov,
- odhodkov državnega proračuna, ki niso načrtovani v ukrepih oziroma projektih sprejetih proračunov,
- obveznosti za druga javnofinančna sredstva (drugi viri), ki niso načrtovana v ukrepih oziroma projektih sprejetih proračunov.

II. Finančne posledice za državni proračun

Prikazane morajo biti finančne posledice za državni proračun, ki so na proračunskih postavkah načrtovane v dinamiki projektov oziroma ukrepov:

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

Navedejo se proračunski uporabnik, ki financira projekt oziroma ukrep; projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in proračunske postavke (kot proračunski vir financiranja), na katerih so v celoti ali delno zagotovljene pravice porabe (v tem primeru je nujna povezava s točko II.b). Pri uvrstitvi novega projekta oziroma ukrepa v načrt razvojnih programov se navedejo:

- proračunski uporabnik, ki bo financiral novi projekt oziroma ukrep,
- projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in
- proračunske postavke.

Za zagotovitev pravic porabe na proračunskih postavkah, s katerih se bo financiral novi projekt oziroma ukrep, je treba izpolniti tudi točko II.b, saj je za novi projekt oziroma ukrep mogoče zagotoviti pravice porabe le s prerazporeditvijo s proračunskih postavk, s katerih se financirajo že sprejeti oziroma veljavni projekti in ukrepi.

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

Navedejo se proračunski uporabniki, sprejeti (veljavni) ukrepi oziroma projekti, ki jih proračunski uporabnik izvaja, in proračunske postavke tega proračunskega uporabnika, ki so v dinamiki teh

projektov oziroma ukrepov ter s katerih se bodo s prerazporeditvijo zagotovile pravice porabe za dodatne aktivnosti pri obstoječih projektih oziroma ukrepih ali novih projektih oziroma ukrepih, navedenih v točki II.a.

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:

Če se povečani odhodki (pravice porabe) ne bodo zagotovili tako, kot je določeno v točkah II.a in II.b, je povečanje odhodkov in izdatkov proračuna mogoče na podlagi zakona, ki ureja izvrševanje državnega proračuna (na primer priliv namenskih sredstev EU). Ukrepanje ob zmanjšanju prihodkov in prejemkov proračuna je določeno z zakonom, ki ureja javne finance, in zakonom, ki ureja izvrševanje državnega proračuna.

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:
(Samo če izberete NE pod točko 6.a.)
Kratka obrazložitev

8. Predstavitev sodelovanja z združenji občin:

Vsebina predloženega gradiva (predpisa) vpliva na: – pristojnosti občin, – delovanje občin, – financiranje občin.	DA/**NE**

Gradivo (predpis) je bilo poslano v mnenje:
- Skupnosti občin Slovenije (SOS): **DA**/NE
- Združenju občin Slovenije (ZOS): **DA**/NE
- Združenju mestnih občin Slovenije (ZMOS): **DA**/NE

Predlogi in pripombe združenj so bili upoštevani:

Ni bilo pripomb.

9. Predstavitev sodelovanja javnosti:	
Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	DA/**NE**

(Če je odgovor NE, navedite, zakaj ni bilo objavljeno.)

Gradivo je objavljeno na spletnem portalu E-demokracija. Pripomb nismo prejeli.

10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	DA/**NE**
11. Gradivo je uvrščeno v delovni program vlade:	**DA**/NE

Po pooblastilu: Milan Tarman, sekretar

PRILOGA

EVA: 2017-1535-0002

PREDLOG ZAKONA O SPREMEMBAH IN DOPOLNITVAH ZAKONA O TAJNIH PODATKIH (ZTP-E)

1. OCENA STANJA IN RAZLOGI ZA SPREJEM ZAKONA

Javnost dela in pravica dostopa do podatkov in informacij državnih organov je splošno sprejeto načelo v sleherni moderni družbi, obenem pa pogoj in zagotovilo normalnega delovanja teh organov, ki brez zaupanja, sodelovanja in podpore javnosti praktično ne morejo biti učinkoviti. Pravica, da vsakdo lahko pridobi informacijo javnega značaja, je v Republiki Sloveniji (v nadaljnjem besedilu: RS) ustavna kategorija, saj Ustava RS v 39. členu določa, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. Razumljivo je, da načelo javnosti dela in dostopnosti do podatkov in informacij državnih organov in nosilcev javnih pooblastil ne more veljati absolutno in neomejeno. V zvezi s tem je najpomembnejše vprašanje, v katerih primerih, na kakšen način in pod katerimi pogoji je dopustno posamezne podatke in informacije odtegniti javnosti. Nekateri podatki in informacije, ki nastanejo oziroma obstajajo v državnih organih, se morajo zaradi zavarovanja določenih državnih interesov in koristi določiti kot tajni, s čimer se njihova dostopnost bistveno omeji. Določitev podatkov in informacij za tajne je v današnjem času lahko najenostavnejši način omejevanja javnosti dela državnih organov, ki se lahko zlorablja za prikrivanje različnih nepravilnosti ali celo nezakonitosti v teh organih. Po drugi strani ohlapen odnos do instituta tajnosti podatkov lahko povzroči, da pridejo v javnost tudi podatki in informacije, s katerimi se lahko ogrozijo interesi in koristi države. Zato je ustrezna pravna ureditev teh vprašanj zelo pomembna.

RS je vprašanja, povezana z določanjem in dostopom do podatkov in informacij, ki jih je zaradi interesov in koristi države treba opredeliti kot tajne, rešila že leta 2001 v Zakonu o tajnih podatkih (Uradni list RS, št. 87/01, v nadaljnjem besedilu: ZTP). Tako so bile določene skupne

osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov za vse državne organe, zlasti za organe državne uprave in druge uporabnike njihovih podatkov in informacij.

Eden izmed temeljnih pogojev, ki jih je RS morala izpolniti pred vstopom v Evropsko unijo in Nato, je bil vzpostavitev ustreznega sistema obravnavanja tajnih podatkov. Standardi obeh mednarodnih organizacij predpostavljajo, da je način varovanja tajnih podatkov pri vsaki članici na taki ravni, da omogoča popolno medsebojno zaupanje pri izmenjavi podatkov, brez dodatnega varnostnega dogovarjanja ali ukrepanja. S sprejemom ZTP in njegove novele v letu 2003 je RS področje tajnih podatkov uskladila s standardi omenjenih organizacij, ki sta tudi obe potrdili in ocenili, da je Slovenija na tem področju vredna zaupanja.

Praksa izvajanja takratnega ZTP in njegove novele na nacionalni ravni je pokazala, da so potrebne nekatere rešitve, ki bodo dopolnile oziroma nadgradile nacionalni sistem obravnavanja in varovanja tajnih podatkov. Predlagane spremembe in dopolnitve so bile usmerjene predvsem v večjo učinkovitost sistema in posledično večjo varnost nacionalnih in tujih tajnih podatkov. Pokazala se je potreba po naslednjih spremembah in dopolnitvah:

- podrobnejši opredelitvi postopkovnih določb, ki urejajo varnostno preverjanje oseb, in njihovi prilagoditvi posebnostim obravnavanja tajnih podatkov;
- natančnejši razmejitvi pristojnosti organov, pristojnih za izdajo dovoljenja za dostop do tajnih podatkov;
- opredelitvi pristojnega organa in postopka izdajanja dovoljenja za dostop do tujih tajnih podatkov fizični osebi ter varnostnega dovoljenja za dostop do tujih tajnih podatkov organizaciji;
- vzpostavitvi inšpekcijskega nadzora nad izvajanjem predpisov s področja tajnih podatkov;
- uskladitvi ZTP z določbami Zakona o prekrških;
- dopolnitvi ureditve posredovanja tajnih podatkov izvajalcem naročil (organizacijam); to je področje industrijske varnosti;
- dopolnitvi določb o določanju tajnih podatkov, spremembi in preklicu tajnosti ter njihovem posredovanju tretjim osebam …

Vse našteto je RS uredila s sprejetjem novele ZTP v letu 2006.

V desetih letih, odkar je v uporabi zadnja novela ZTP, je bilo mogoče zaznati zlasti silovit razvoj segmenta informatike, kar posledično zahteva nove aktivnosti na področju informacijske varnosti, predvsem v okviru delovanja Urada Vlade RS za varovanje tajnih podatkov (v nadaljnjem besedilu: UVTP), ki je vsebinski nosilec ZTP in predpisov, sprejetih na njegovi podlagi. Tako na primer UVTP na področju informacijske varnosti aktivno deluje že od konca leta 2007. V okviru varnostnih odborov zveze Nato in EU tvorno sodeluje pri sooblikovanju skupne kibernetske varnosti, kjer zastopamo interese RS. UVTP je aktivno sodeloval pri usklajevanju in pripravi Strategije kibernetske varnost RS.

UVTP opravlja tudi naloge s področja kriptografije za potrebe varovanja nacionalnih tajnih podatkov ter tajnih podatkov EU in Nata. Na nacionalni ravni UVTP v sodelovanju s Komisijo za informacijsko varnost opravlja vrednotenje šifrirnih rešitev, ki se uporabljajo za varovanje prenosa tajnih podatkov v komunikacijsko-informacijskih sistemih (v nadaljnjem besedilu: KIS). Za namene izvajanja šifrirnega vrednotenja je UVTP v aprilu 2011 ustanovil medresorsko strokovno delovno skupino za komunikacijsko varnost. Na področju EU smo vključeni v Varnostni odbor Sveta EU za informacijsko varnost in med drugim sodelujemo pri oblikovanju kriptografskih predpisov za varovanje tajnih podatkov EU. Prav tako smo vključeni v delovno skupino Crypto CaT zveze Nato, ki je zadolžena za pripravo kriptografskih predpisov za varovanje tajnih podatkov Nata. UVTP je vključen tudi v procese kriptografske transformacije in modernizacije v zvezi Nato. V skladu z določili varnostnih politik EU UVTP opravlja naloge organa za razdeljevanje šifrirnega materiala EU.

Na podlagi dosedanjih izkušenj in zaradi potreb po celoviti ureditvi organizacije področja informacijske varnosti je bil izoblikovan načrt za postavitev krovnih organov s področja varovanja tajnih podatkov v KIS, ki bodo centralizirano izvajali svoje naloge.

Ne nazadnje tudi vsi prej navedeni primeri nazorno kažejo na potrebo po spremembi in dopolnitvi področja informacijske varnosti v ZTP.

Drugi segment, pri katerem izkušnje in spoznanja iz dosedanje prakse kažejo potrebo po natančnejši ureditvi, je segment industrijske varnosti. Izkazalo se je, da veliko organizacij, ki dostopajo do tajnih podatkov zaradi izvršitve naročil organa (naročnika), deluje v prostorih naročnika. Zato se vedno znova postavlja vprašanje, zakaj naj bi organizacija, ki zaradi narave tajnega naročila tajnih podatkov ne bo obravnavala v lastnih prostorih, izpolnjevala fizične in tehnične pogoje za varovanje tajnih podatkov. Zaradi zdaj veljavnih zakonskih določil namreč mnoge organizacije vlagajo velika finančna sredstva v izgradnjo oziroma vzpostavitev upravnih in varnostnih območij, čeprav jih za izvajanje konkretnih tajnih naročil dejansko ne potrebujejo.

Na področju industrijske varnosti se je zaradi sprememb globalne varnostne situacije v svetu pokazala potreba po preverjanju lastniške strukture organizacije in tako imenovanih povezanih oseb, to je oseb, ki imajo v lasti določen lastniški ali upravljavski delež organizacije, oziroma drugih oseb, ki nadzirajo ali bi lahko izvajale neposreden ali posreden nadzor nad organizacijo oziroma bi lahko vplivale na njeno dejavnost. Z zdaj veljavno ureditvijo namreč ni podrobno opredeljen obseg potrebnega preverjanja tako imenovanega ozadja poslovanja organizacije, ki bi lahko bilo v nasprotju z varnostnimi, političnimi ali gospodarskimi interesi RS.

UVTP je zaznal tudi nedoslednosti pri izvajanju pogodb, ki v svoji izvedbi omogočajo dostop do tajnih podatkov. Pomanjkljiva določila o načinih varovanja tajnih podatkov v pogodbah so pogosto vzrok za nepravilno ravnanje s tajnimi podatki in njihovo nepravilno varovanje.

Tretji segment, pri katerem se je pokazala potreba po spremembah in dopolnitvah, je segment osebne varnosti. Prvo vprašanje se nanaša na krog oseb (izjeme), ki ne potrebujejo dovoljenja za dostop do tajnih podatkov, ampak lahko dostopajo do tajnih podatkov že zaradi same funkcije in seveda v skladu s potrebo po seznanitvi z določenim tajnim podatkom. Krog oseb, ki lahko do tajnih podatkov dostopajo brez dovoljenja za dostop do tajnih podatkov, je po slovenskih predpisih enormno širok in precej odstopa od primerljivih ureditev v državah članicah EU in zveze Nato, kjer je omejen le na ključne nosilce oblasti, in ne nazadnje tudi od ureditev podpisnic bilateralnih sporazumov z RS o medsebojni izmenjavi in varovanju tajnih podatkov. S spremembo predpisov zveze Nato in EU so te iste osebe dobile tudi dostop brez dovoljenja za dostop do tajnih podatkov zveze Nato in EU (tuji tajni podatki). Posledično je inšpekcija zveze Nato in EU našo državo opozorila na preširok obseg izjem. Če se krog izjem ne bo krčil, je treba z zakonom predpisati ozek krog oseb (ključne nosilce oblasti), ki bodo imele omogočen dostop do tujih tajnih podatkov brez dovoljenja za dostop do tujih tajnih podatkov, ter posebej opredeliti izjeme pri dostopu do nacionalnih tajnih podatkov.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

Predlagane spremembe in dopolnitve ZTP ne odstopajo od ciljev in načel, na katerih sloni že sedanja ureditev tega področja. Poglaviten cilj predlaganega zakona je zgolj izboljšati učinkovitost sistema in posledično varnost tajnih podatkov.

Glede na pojmovno razlago in razumevanje na kompleksnem področju tajnih podatkov je UVTP ločil obravnavo in hrambo tajnih podatkov, ki skupaj z arhiviranjem in nadzorom pomenita varovanje tajnih podatkov.

Sedanji ZTP praktično nima določb, ki bi urejale varovanje tajnih podatkov v KIS in eksplicitno opredeljevale naloge UVTP na tem področju. Predlagana dopolnitev ZTP zato zelo natančno določa sestavne dele sistema in potrebo po izvedbi postopka varnostne odobritve sistemov, v katerih se obravnavajo oziroma hranijo tajni podatki.

UVTP kot krovni nacionalni varnostni organ že zdaj v skladu s sklepom Vlade RS št. 38600-3/2009/21 z dne 8. 4. 2010 opravlja koordinacijo varnostnih organov, ki na podlagi obstoječih normativnih aktov opravljajo naloge s področja informacijske varnosti; to so MO, MNZ – Policija in SOVA. S predlagano ureditvijo bo UVTP postal krovno koordinacijsko telo, konkretne naloge pa se bodo še naprej opravljale v okviru posameznih organov. Navedeni sklep je UVTP pripravil

v sodelovanju s Komisijo za informacijsko varnost, ministrstvom, pristojnim za obrambo, ministrstvom, pristojnim za notranje zadeve, ministrstvom, pristojnim za zunanje zadeve, ministrstvom, pristojnim za javno upravo, in Slovensko obveščevalno-varnostno agencijo, ob upoštevanju mnenja Sekretariata Sveta za nacionalno varnost.

Na področju industrijske varnosti je največja novost podrobnejša ureditev preverjanja lastniške strukture organizacije in tako imenovanih povezanih oseb, to je oseb, ki imajo v lasti določen lastniški ali upravljavski delež organizacije, oziroma drugih oseb, ki nadzirajo ali bi lahko izvajale neposreden ali posreden nadzor nad organizacijo oziroma bi lahko vplivale na njeno dejavnost. Z določili, ki se nanašajo na obveznost pristojnih organov, da preverijo, ali povezane osebe niso sodelovale oziroma ne sodelujejo z organizacijami ali skupinami, ki ogrožajo vitalne interese RS ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je RS, se v zakonodajo vnaša jasnejša podlaga za varnostno preverjanje lastniške strukture organizacije. Z zdaj veljavno ureditvijo namreč ni podrobno opredeljen obseg potrebnega preverjanja tako imenovanega ozadja poslovanja organizacije, ki bi lahko bilo v nasprotju z varnostnimi, političnimi ali gospodarskimi interesi RS. Nadalje se s konkretno navedbo odstotkovne vrednosti lastništva organizacije (če je lastnik organizacije v višini vsaj 25 odstotkov druga družba), ki pomeni nekakšno začetno osnovo za potrebo po varnostnem preverjanju tudi povezanih oseb te lastniške družbe, vzpostavlja enoten kriterij za vse organe, pristojne za vodenje postopka varnostnega preverjanja organizacij. V predlagani spremembi ZTP so izenačeni tudi pogoji za dostopanje do tajnih podatkov stopnje tajnosti INTERNO za zaposlene v organih in za zaposlene v organizacijah.

Nadalje je s predlagano novelo ZTP predstojnik ministrstva, pristojnega za gospodarstvo, pristojen predlagatelj za izdajo varnostnega dovoljenja tistim organizacijam, ki to dovoljenje potrebujejo zaradi sodelovanja na javnih razpisih tuje države ali mednarodne organizacije ali zaradi izvedbe naročila tuje države ali mednarodne organizacije. S to spremembo se odpravlja nejasnost oziroma razlaga, da je predstojnik ministrstva, pristojnega za gospodarstvo, pristojen predlagatelj tudi za organizacije, ki potrebujejo varnostno dovoljenje zaradi sodelovanja na javnih razpisih, ki jih objavljajo slovenski naročniki.

Naslednja pomembna novost je, da predlagatelj v predlogu opredeli način obravnavanja tajnih podatkov v okviru izvajanja naročila, ki lahko poteka v prostorih naročnika ali v prostorih organizacije. S tem določilom se ureja dosedanja zakonska pomanjkljivost na področju industrijske varnosti, ki je predvidevala izdajanje varnostnega dovoljenja organizaciji zgolj v primerih, ko se tajni podatki organizaciji posredujejo v fizični obliki oziroma v njene prostore. S predlagano ureditvijo se zvišuje raven varnostnih standardov na področju industrijske varnosti, ki bodo tako skladni z mednarodnimi varnostnimi standardi in s tujo prakso na tem področju. Navsezadnje je samo naročnik tisti, ki lahko na podlagi vsebine naročila opredeli potreben način obravnavanja tajnih podatkov. Z dopolnitvijo zakona se tudi organu, pristojnemu za varnostno preverjanje organizacije, omogoča ustrezno zbiranje podatkov, potrebnih za odločitev o izdaji varnostnega dovoljenja.

Tretji segment, pri katerem se je pokazala potreba po spremembah in dopolnitvah, je segment osebne varnosti. Zdaj veljavni 3. člen ZTP določa osebe, ki lahko v zvezi z opravljanjem svoje funkcije dostopajo do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov. Osebe dobijo dovoljenje z začetkom opravljanja funkcije oziroma opravljanja dela in podpisom izjave, da so seznanjene z ZTP in drugimi predpisi, ki urejajo varovanje tajnih podatkov, ter da se zavezujejo, da bodo s tajnimi podatki ravnale v skladu s temi predpisi. Krog oseb, ki lahko do tajnih podatkov dostopajo brez dovoljenja za dostop do tajnih podatkov zaradi opravljanja svoje funkcije ali delovnih dolžnosti, je po slovenskih predpisih enormno širok in precej odstopa od primerljivih ureditev v državah članicah EU in zveze Nato, kjer je omejen na ključne nosilce oblasti. Glede na to, da zveza Nato in EU v svojih predpisih dostop do tajnih podatkov Nata in EU dovoljujeta osebam z dostopom brez dovoljenja za dostop do tajnih podatkov v skladu z nacionalno zakonodajo, je bila RS ob inšpekciji Nata in EU v RS vsakokrat opozorjena na preširok krog teh oseb. S predlagano spremembo bi bil dostop do tujih tajnih podatkov brez opravljenega varnostnega preverjanja omogočen le državnim funkcionarjem na najvišjih položajih, to je predsedniku republike, predsedniku vlade, predsedniku državnega sveta in

predsedniku vrhovnega sodišča ter ministrom in poslancem. Osebe, ki bodo imele dostop do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov, in sicer tako nacionalnih kot tujih tajnih podatkov, bodo morale pred dostopom do tajnih podatkov opraviti osnovno usposabljanje, ki ga bo izvedel nacionalni varnostni organ, in podpisati izjavo, da so seznanjene z ZTP in drugimi predpisi, ki urejajo varovanje tajnih podatkov, ter da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi. Predlog novega 3. člena je tako primerljiv z ureditvami, ki jih imajo v drugih državah članicah zveze Nato in EU, in bi v popolnosti odpravil vse zadržke, ki sta jih ob inšpekcijskih pregledih navajala zveza Nato in EU.

3. OCENA FINANČNIH POSLEDIC PREDLOGA ZAKONA ZA DRŽAVNI PRORAČUN IN DRUGA JAVNOFINANČNA SREDSTVA

Predlog zakona bo imel finančne posledice za državni proračun. Za učinkovito izvajanje predlaganih sprememb zakona bo Ministrstvo za javno upravo v letu 2018 vzpostavilo kriptografski laboratorij. Ocenjujemo, da bo njegova vzpostavitev stala 150.000 EUR. V letu 2019 pa se bo vzpostavil še TEMPEST laboratorij (gre za zaščito pred neželenim elektromagnetnim sevanjem). Za njegovo vzpostavitev bo ministrstvo namenilo 1.500.000 EUR. Za vzdrževanje obeh laboratorijev ocenjujemo letni strošek 20.000 EUR, s tem da bo v letu 2018 vzdrževanje v višini 10.000 EUR le za kriptografski laboratorij. Predlog zakona ne bo imel finančnih posledic za druga javnofinančna sredstva.

4. NAVEDBA, DA SO SREDSTVA ZA IZVAJANJE ZAKONA V DRŽAVNEM PRORAČUNU ZAGOTOVLJENA, ČE PREDLOG ZAKONA PREDVIDEVA PORABO PRORAČUNSKIH SREDSTEV V OBDOBJU, ZA KATEREGA JE BIL DRŽAVNI PRORAČUN SPREJET

Za izvajanje zakona so za leto 2018 zagotovljena sredstva v državnem proračunu, in sicer v okviru Ministrstva za javno upravo, projekt informacijska varnost (šifra 3130-17-0009), na proračunski postavki PP170089 – Razvoj, vzdrževanje in upravljanje informacijske varnosti. Sredstva so zagotovljena v višini 160.000 eurov.

5. PRIKAZ UREDITVE V DRUGIH PRAVNIH SISTEMIH IN PRILAGOJENOST PREDLAGANE UREDITVE PRAVU EVROPSKE UNIJE

Predlog zakona je usklajen s pravnim redom EU. Z Zakonom o spremembah in dopolnitvah Zakona o tajnih podatkih se v pravni red Republike Slovenije ne prenašajo določbe direktiv Evropske unije, temveč se z njim na posameznih področjih varovanja tajnih podatkov zgolj natančneje usklajuje pravni red, opredeljen s sklepom Sveta Evropske unije 2013/488/EU in sklepom Evropske komisije (EU, Euratom) 2015/443.

ČEŠKA REPUBLIKA

Zakonodaja Češke republike, kjer je osnovni predpis na področju tajnih podatkov »Act N 412/2005 Coll on the Protection of Classified Information«, dovoljuje bistveno manj izjem, to je oseb, ki imajo dostop do nacionalnih tajnih podatkov brez dovoljenja za dostop do tajnih podatkov, kot zakonodaja RS. Kljub temu imajo še posebno dikcijo, kjer so taksativno opredeljene tiste osebe, ki imajo omogočen dostop tudi do tujih tajnih podatkov brez dovoljenja za dostop do tujih tajnih podatkov. Dostop do tujih tajnih podatkov brez dovoljenja za dostop do tujih tajnih podatkov ima v Češki republiki zgolj pet oseb, in sicer predsednik države, predsednik vlade, predsednika obeh domov parlamenta in minister za zunanje zadeve.

Zakonodaja Češke republike tudi podrobno opredeljuje področje varovanja tajnih podatkov v komunikacijsko-informacijskih sistemih. Zakon predpisuje obvezno varnostno vrednotenje (akreditacijo) vseh komunikacijsko-informacijskih sistemov, v katerih se obravnavajo tajni podatki – opravi se na podlagi ocene tveganja − nadalje kriptografsko zaščito tajnih podatkov

pri elektronskem prenosu zunaj upravnih oziroma varnostnih območij ter postopek varnostnega vrednotenja kriptografskih rešitev. Proti neželenemu elektromagnetnemu sevanju morajo biti zaščiteni sistemi, v katerih se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje. Nacionalni varnostni organ izvaja naloge organa, pristojnega za varnostno vrednotenje sistemov, zaščito pred neželenim elektromagnetnim sevanjem, varnostno vrednotenje kriptografskih rešitev in razdeljevanje kriptografskega materiala.

Tudi zakonodaja Češke republike pozna institut tako imenovanega »varnostnega dovoljenja za obravnavanje tajnih podatkov pri naročniku«. Na varnostnem dovoljenju, izdanem organizaciji, je specificirano, ali organizacija izpolnjuje pogoje tudi za obravnavanje in hrambo tajnih podatkov v lastnih prostorih, ali pa se bodo ti obravnavali in hranili izključno pri naročniku. Prav tako uporabljajo postopek preverjanja lastništva organizacije ter postopek ugotavljanja vpliva tujega lastništva, tujega kapitala in morebitnih drugih vplivov na poslovanje organizacije iz tujine. Organizacija mora sama, pred začetkom postopka varnostnega preverjanja, pristojnemu organu predložiti vsa dokazila, kot so našteta v predpisu.

ZVEZNA REPUBLIKA NEMČIJA

Tudi nemška zakonodaja, ki ureja področje tajnih podatkov s »Security Clearance Check Act« (20. april 1994), opredeljuje krog oseb, ki jim je omogočen dostop do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov, vendar je ta krog oseb restriktivnejši kot v RS. Omejen je namreč na naslednje osebe: zvezni kancler, poslanec, ustavni sodnik, predsednik zveznega sveta in član vlade.
Nemška zakonodaja s področja tajnih podatkov je ena izmed tistih, ki ne opredeljuje varovanja tajnih podatkov v komunikacijsko-informacijskih sistemih, saj je za celotno tovrstno področje (kriptografska zaščita, zaščita pred neželenim elektromagnetnim sevanjem, kibernetska varnost, varnostno vrednotenje sistemov (akreditacija) …) v Nemčiji pristojen Zvezni urad za informacijsko varnost (Bundesamt für Sicherheit in der Informationstechnik − BSI), v katerem je zaposleno več kot 3000 ljudi. Standardi varovanja tajnih podatkov v komunikacijsko-informacijskih sistemih so vsaj taki, kot jih predvidevata zveza Nato in EU, oziroma v nekaterih pogledih celo strožji ter kot taki primerljivi z našimi predlogi v noveli Zakona o tajnih podatkih.
Zakonodaja Zvezne republike Nemčije pozna institut tako imenovanega »varnostnega dovoljenja za obravnavanje tajnih podatkov pri naročniku«. Na varnostnem dovoljenju, izdanem organizaciji, je specificirano, ali organizacija izpolnjuje pogoje tudi za obravnavanje in hrambo tajnih podatkov v lastnih prostorih, ali pa se bodo ti obravnavali in hranili izključno pri naročniku. Opredeljen je način hrambe dokumentacije.

Prav tako uporabljajo postopek preverjanja lastništva organizacije ter postopke ugotavljanja vpliva tujega lastništva, tujega kapitala in morebitnih drugih vplivov na poslovanje organizacije iz tujine. Tak postopek se izvede vsakič, ko se spremeni lastniška struktura organizacije, še posebej pozorni so pri preverjanju tujega lastništva. Vpliv tujega lastništva je tudi eden glavnih vzrokov za to, da se organizaciji zavrne izdaja varnostnega dovoljenja (zakonsko določilo: »foreign ownership or capital influence, in particular from countries of security concern (whether or not majority or minority stake) can also justify FSC being denied, where security risk cannot be accepted«).

Organizacija mora sama, pred začetkom postopka varnostnega preverjanja, pristojnemu organu predložiti vsa dokazila, našteta v predlogu spremembe 35.a člena ZTP. Poleg tega mora predložiti dokazila o lastništvu organizacije, in sicer tako neposrednem (v odstotkih) kot tudi posrednem lastništvu.

REPUBLIKA HRVAŠKA

Naj omenimo še Republiko Hrvaško, katere zakon s področja tajnih podatkov, to je »Zakon o tajnosti podataka«, sega v leto 2007. Res je, da je tudi Republika Hrvaška v svojem zakonu opredelila osebe, ki imajo dostop do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov, vendar je ta krog oseb omejen le na ključne nosilce oblasti. Tako imajo v skladu s hrvaško zakonodajo dostop do tajnih podatkov brez dovoljenja predsednik Republike Hrvaške, predsednik Vlade Republike Hrvaške in predsednik Državnega zbora Republike Hrvaške (hrvaški sabor).

Varovanje tajnih podatkov v komunikacijsko-informacijskih sistemih opredeljuje tudi zakonodaja Republike Hrvaške. Priprava normativnih aktov in organizacijski vidik varovanja tajnih podatkov v komunikacijsko-informacijskih sistemih sta v pristojnosti nacionalnega varnostnega organa (Ured Viječa za nacionalnu sigurnost − UVNS). Zakon v 12. členu opredeljuje komunikacijsko-informacijske sisteme, v katerih se obravnavajo tajni podatki, postopek varnostnega vrednotenja (akreditacijo) komunikacijsko-informacijskih sistemov in ukrepe fizične zaščite prostorov, v katerih so postavljeni ti sistemi. Proti neželenemu elektromagnetnemu sevanju morajo biti zaščiteni sistemi, v katerih se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje. Nadalje so s 17. členom ustanovili Zavod za varnost informacijskih sistemov (Zavod za sigurnost informacijskih sustava), ki je osrednji državni organ za tehnično področje varovanja komunikacijsko-informacijskih sistemov in državni odzivni center za obravnavo incidentov v komunikacijsko-informacijskih sistemih javne uprave (GOV CERT). Zavod tako na področju varovanja podatkov (tajnih in netajnih) v komunikacijsko-informacijskih sistemih kot tudi na področju kibernetske varnosti svojo dejavnost opravlja v sodelovanju s hrvaškim nacionalnim varnostnim organom. Fizične, organizacijske in tehnične ukrepe ter postopke varovanja tajnih podatkov v komunikacijsko-informacijskih sistemih imajo podrobno predpisane v Uredbi o ukrepih varovanja podatkov (Uredba o mjerama informacijske sigurnosti – Narodne novine, broj 79/07). Zavod za varnost informacijskih sistemov izvaja naloge organa, pristojnega za varnostno vrednotenje sistemov, zaščito pred neželenim elektromagnetnim sevanjem, varnostno vrednotenje kriptografskih rešitev in razdeljevanje kriptografskega materiala.

Zakonodaja Republike Hrvaške prav tako pozna institut tako imenovanega »varnostnega dovoljenja za obravnavanje tajnih podatkov pri naročniku«. Na varnostnem dovoljenju, izdanem organizaciji, je specificirano, ali organizacija izpolnjuje pogoje za obravnavanje in hrambo tajnih podatkov v lastnih prostorih, ali pa se bodo ti obravnavali in hranili izključno pri naročniku. Uporabljajo tudi postopek preverjanja lastništva organizacije ter postopek ugotavljanja vpliva tujega lastništva, tujega kapitala in morebitnih drugih vplivov na poslovanje organizacije iz tujine. Na podlagi »Ugovora o provođenju postupka izdavanja certifikata poslovne sigurnosti« mora organizacija UVNS obvezno poročati o vsakršni spremembi lastniške strukture organizacije (sprememba delničarjev družbe ali samih družbenikov, ki imajo več kot 5 odstotkov lastništva). Organizacija mora sama, pred začetkom postopka varnostnega preverjanja, pristojnemu organu predložiti vsa dokazila, našteta v predlogu spremembe 35.a člena ZTP.

6. DRUGE POSLEDICE, KI JIH BO IMELO SPREJETJE ZAKONA

6.1 Presoja administrativnih posledic:

Nima administrativnih posledic.

6.2 Presoja posledic za okolje, vključno s prostorskimi in varstvenimi vidiki:

Nima posledic za okolje.

6.3 Presoja posledic za gospodarstvo:

Nima posledic za gospodarstvo, saj imajo podjetja (organizacije) že zdaj možnost pridobiti varnostno dovoljenje za obravnavanje nacionalnih tajnih podatkov in tajnih podatkov zveze Nato ter EU, kar jim omogoča sodelovanje pri izvajanju naročila organa ali sodelovanje na javnih razpisih tuje države ali mednarodne organizacije ali izvedbo naročila tuje države ali mednarodne organizacije.

6.4 Presoja posledic za socialno področje:

Nima posledic za socialno področje.

6.5 Presoja posledic za dokumente razvojnega načrtovanja:

Nima posledic za dokumente razvojnega načrtovanja.

6.6 Presoja posledic za druga področja:

Nima posledic za druga področja.

6.7 Izvajanje sprejetega predpisa:

a) Predstavitev sprejetega zakona: /

b) Spremljanje izvajanja sprejetega predpisa

Za izvajanje zakona bo potrebna prilagoditev nekaterih podzakonskih aktov, ki so izdani na podlagi ZTP. Spremljanje izvajanja zakona v praksi in presoja posledic bosta tako kot doslej potekala prek medresorskih delovnih skupin, ki jih za posamezna področja imenuje direktor UVTP, in odzivov strokovne javnosti.

6.8 Druge pomembne okoliščine v zvezi z vprašanji, ki jih ureja predlog zakona: /

7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA

Predlog zakona je bil poslan v medresorsko usklajevanje vsem ministrstvom, organom v sestavi ministrstev in vladnim službam (v nadaljnjem besedilu: organi) ter združenju občin. Objavljen je bil tudi na portalu E-demokracija, kjer smo pripombe sprejemali do 1. 9. 2017, vendar le-teh ni bilo.
Prispele pripombe organov so bile v večini upoštevane.

K 1.členu (opredelitev pojmov) predloga novele ZTP-ja so podali pripombe Ministrstvo za infrastrukturo (MZI), Ministrstvo za notranje zadeve (MNZ), Ministrstvo za finance (MF) in Ministrstvo za pravosodje (MP). Pripombe MZI, MF in MNZ glede črtanja definicije pojma predstojnika organa so bile upoštevane. Upoštevane so bile tudi ostale redakcijske pripombe, ki so prispele s strani MNZ.
Pripombe MP: Glede na dejstvo, da se uvaja precej novih pojmov in popravkov definicij že obstoječih pojmov, pripomba MP, da se dodajo samo spremembe relevantnih določb, ne pa celoten seznam definicij, predlagatelj ni upošteval. Predlagatelj tudi ni upošteval predloga MP, da se med definicijo pojmov doda pojem »kriptografski material«, saj so pojmi v povezavi s kriptografijo eksplicitno opredeljeni v Navodilu o obravnavanju kriptografskega materiala, ki pa je označeno s stopnjo tajnosti INTERNO. Trenutna definicija pojma »varnostno preverjanje« obsega tako postopek pridobivanja dovoljenja za dostop do tajnih podatkov kot tudi varnostnega dovoljenja organizacije in postopek vmesnega varnostnega preverjanja, zato predlagatelj pripombe MP ni upošteval. Za dostopanje do tajnih podatkov stopnje tajnosti INTERNO, pa ni varnostnega preverjanja osebe in posledično izdanega dovoljenja. Pripombo glede definicije »varnostnega zadržka« je predlagatelj upošteval, ravno tako predlog glede »javne varnosti«.

K 2. členu (izjeme glede dostopanja do tajnih podatkov) so podali pripombe MP, MZI, Ministrstvo za obrambo (MO), Generalni sekretariat Vlade RS (GSV) in Statistični urad (SURS). Predlagatelj je upošteval vse prispele pripombe z izjemo pripombe MP, ki se nanaša na spremembo tretjega odstavka, in pripombo SURS ter GSV. MP namreč meni, da bi bilo potrebno spremembe tretjega odstavka črtati in pustiti nespremenjeno besedilo dosedanjega tretjega odstavka. Delovanja nosilcev najvišjih ali pomembnih političnih in strokovnih funkcij se po mnenju MP ne more pogojevati z izvedbo osnovnega usposabljanja. V povezavi s tem predlagatelj meni, da je osnovno usposabljanje najboljši način seznanitve s področjem tajnih podatkov, kar je podrobno pojasnil tudi v obrazložitvi k dotičnemu členu.

SURS predlaga, da se drugi odstavek 3. člena razširi še s »predstojnikom vladne službe, ki je neposredno odgovoren predsedniku vlade«, GSV pa razširitev z generalnim sekretarjem vlade. Pri navajanju oseb iz dotičnega odstavka (dostop do tajnih podatkov tuje države ali mednarodne organizacije brez pooblastila za dostop do tujih tajnih podatkov) je predlagatelj sledil izključno opozorilu / predlogu podanem s strani inšpekcije zveze Nato in EU. Posledično predloga SURS in GSV zato predlagatelj ni upošteval. Predsednik Državnega zbora ni naveden z namenom, ker je poslanec in
GSV predlaga, da se med osebe, ki v zvezi z opravljanjem svoje funkcije lahko dostopajo do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov, doda tudi generalni sekretar vlade. Predlagatelj pripombe ni upošteval, saj je generalni sekretar vlade predstojnik vladne službe, ki je neposredno odgovoren predsedniku vlade in potemtakem že spada v kategorijo oseb, ki lahko dostopajo do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov. Predlagatelj je za navajanje oseb uporabil v vseh primerih ednino.

Upoštevane pripombe:
MZI: besedilo »- guverner, namestnik in vice guverner..." nadomesti z besedilom "- guverner, namestnik guvernerja in vice guverner;«
MP: »državni pravobranilec« se nadomesti z »državni odvetnik« ter dodajo se ustavni sodniki
V drugem odstavku so poleg podatkov tuje države navedeni tudi podatki mednarodnih organizacij.
MO: Predsednik Državnega zbora se je črtal, ker je zajet že med poslanci, in pa poenoteno je navajanje funkcij.

MF predlaga, da se pojem »organizacija« opredeli v členu, ki določa pomen posameznih izrazov v ZTP. Pojem organizacije je opredeljen v tretjem odstavku 1. člena ZTP (»Po tem zakonu morajo ravnati tudi dobavitelji, izvajalci gradenj ali izvajalci storitev (v nadaljnjem besedilu: organizacije), ki se jim podatki iz prvega odstavka tega člena posredujejo zaradi izvršitve naročil organa.«)

Ministrstvo za kulturo (MK) je pripravilo predlog člena glede pravnega nasledstva organa ali organizacija, v katerem je bila stopnja tajnosti podatka določena. Pripombe glede obrazložitve dotičnega člena, podane s strani MK, je predlagatelj upošteval.
MK je podalo tudi pripombe na 18. člen trenutno veljavnega ZTP, kateri pa se ne odpira in zato predlagatelj pripombe ni upošteval.

GSV predlaga, da se varovani tajni podatki ravno tako uredijo v ZTP. Predlagatelj pripombe ni upošteval, saj se varovani tajni podatki urejajo v Uredbi o upravnem poslovanju, ki je v pristojnosti MJU. Zaradi preglednosti nad področjem dela ni racionalno v zakonu, ki ureja zgolj področje tajnih podatkov (na kar nakazuje tudi samo ime zakona), urejati tudi tako imenovane varovane tajne podatke.

K 6. členu je podal pripombe MNZ, ki predlaga spremembo petega odstavka – v odstavku se črta besedna zveza »velja od dneva izdaje in«. Predlagatelj je pripombo upošteval.

K 8. členu je podalo pripombe MF, in sicer da postopek prisilne poravnave ne sodi v vsebinski kontekst posledice in namena prenehanje poslovanja organizacije. Predlagatelj je pripombo upošteval v smislu, da je dikcijo dopolnil z besedo »lahko« (… 7. zoper organizacijo ni uveden ali začet postopek prisilne poravnave, stečajni, likvidacijski postopek ali drug postopek, katerega posledica ali namen je lahko prenehanje poslovanja organizacije;«).
Predlagatelj je tudi upošteval pripombo glede dikcije 8. točke, ki se sedaj glasi:
»8. organizacija na dan preverjanja pogojev izpolnjuje obvezne dajatve in druge denarne nedavčne obveznosti, ki jih pobira davčni organ v skladu s predpisi. Organizacija ne izpolnjuje pogojev iz prejšnjega stavka, če vrednost teh neplačanih zapadlih obveznosti na dan preverjanja pogojev znaša 50 eurov ali več;«.

Pripombe MNZ, da se določi veljavnost varnostnemu dovoljenju, predlagatelj ni upošteval, saj je veljavnost varnostnega dovoljenja določena v 35. členu ZTP.

K 10. členu je podal pripombe GSV. V primeru preklica varnostnega dovoljenja pristojni organ izda odločbo, ki se v skladu z določbami Zakona o splošnem upravnem postopku vroči predlagatelju (obvesti se tudi organizacijo). Posledično predlagatelj pripombe ni upošteval.

K 11. členu so podali pripombe GSV, MNZ in MORS. Vse v povezavi z določanjem upravnega in varnostnega območja se bo podrobneje uredilo v Uredbi o varovanju tajnih podatkov, katera se bo zagotovo spreminjala v bližnji prihodnosti. Glede na dejstvo, da se pojem upravnega in varnostnega območja v predlogu novele ZTP pojavi le v 39. členu, predlagatelj pojmov ni opredelil v členu, ki določa pomen izrazov v ZTP.
Pripombe MORS, da se v petem odstavku črta besedna zveza »in kdo jih sprejema«, predlagatelj ni upošteval, saj je v ta namen potrebno v sistemizaciji opredeliti delovna mesta, na katerih se lahko sprejemajo nosilci tajnih podatkov.
Pripombe MORS, da se v sedmem odstavku za prvim stavkom doda nov stavek »Postopke in ukrepe iz tega odstavka predpiše vlada.«, predlagatelj ni upošteval, saj je to zajeto že v osmem odstavku 39. člena.

K 12. členu so podali pripombe GSV, MJU in MORS. MJU je podal pripombo glede določitve prehodnega roka za izvedbo varnostnega ovrednotenja s strani nacionalnega varnostnega organa. Predlagatelj je pripombo upošteval.
MORS in GSV sta podala pripombo glede uporabe izrazov »izredne okoliščine« in »izredno stanje«- Predlagatelj je uporabil definicijo, ki jo je pripravil MORS.

K 14. členu (dostopanje do tujih tajnih podatkov) je podalo pripombe MZI, ki ugotavlja da predlog zakona določa dovoljenje za dostop do tajnih podatkov in pooblastilo za dostop do tajnih podatkov.
Glede pooblastila za dostopanje do tujih tajnih podatkov je predlagatelj sledil institucijam EU in NATO, ki tudi ne izdajajo upravnih odločb, kar je bilo tudi priporočilo inšpekcije s strani zveze Nato in EU. Pooblastila za dostop do tujih tajnih podatkov bo izdajal UVTP, dovoljenja za dostop do (nacionalnih) tajnih podatkov pa tako kot do sedaj pristojni organ iz 22. člena ZTP.

K 15. členu (vodenje evidenc) je podalo pripombe Ministrstvo za okolje in prostor (MOP), ki meni da bi veljalo ponovno razmisliti o dikciji druge alineje (DATUM IN KRAJ ROJSTVA), saj po njihovem mnenju za popolno evidenco oziroma evidenco, ki bi dosegla svoj namen navedba kraja rojstva v konkretnem primeru ni nujno potrebna. Pripombo je predlagatelj upošteval.
Predlagatelj je upošteval tudi pripombo MJU in MP glede obrazložitve navedenega člena, v delu, ki se nanaša na ZDIJZ. Pripombe na 16. člen sta podala tudi GSV in MP. Skozi dolgoletni delovni proces se je namreč pokazala potreba po vodenju še precej dodatnih evidenc, saj ima UVTP lahko le na ta način pregled nad celotnim delovnim področjem, ki je v njegovi pristojnosti.
Pripombe MP:

- pripombo o roku hrambe evidenc je predlagatelj upošteval;
- kršitev dolžnosti sporočanja podatkov in spremembe podatkov je predlagatelj sankcioniral;
- evidenca dovoljenj, evidenca zavrnjenih predlogov za izdajo dovoljenja, evidenca izdanih pooblastil za dostop do tujih tajnih podatkov itd. so evidence, ki med seboj niso povezane in tudi preklic dovoljenja ni ekvivalentno zavrnitvi izdaje dovoljenja, zato je predlagatelj predlog o vodenju razloga za preklic dovoljenja v naštetih evidencah zavrnil;
- glede evidence kriptografskega materiala velja poudariti, da se kriptografski material ne prekliče – ko poteče, se uniči in zato predlagatelj pripombe MP, da se v evidenci kriptografskega materiala doda podatke o datumu preklica materiala ter razlogih za preklic, ni upošteval.

K 19. členu je podal pripombe MJU, in sicer glede skrajšanja roka za izdajo podzakonskih aktov iz enega leta na šest mesecev. Predlagatelj je pripombo upošteval.
Iz združenja občin ni prispela nobena pripomba.

8. OBRAZLOŽITEV PREDLAGANEGA NUJNEGA POSTOPKA OBRAVNAVE PREDLOGA ZAKONA V DRŽAVNEM ZBORU

Predlagamo sprejem zakona po rednem zakonodajnem postopku.

9. PODATEK O ZUNANJEM STROKOVNJAKU OZIROMA PRAVNI OSEBI, KI JE SODELOVALA PRI PRIPRAVI PREDLOGA ZAKONA, IN ZNESKU PLAČILA ZA TA NAMEN:

- osebno ime in naziv fizične osebe ali firma in naslov pravne osebe,
- znesek plačila, ki ga je oseba iz prejšnje alineje prejela za namen priprave zakona.

Pri pripravi zakona zunanji strokovnjaki ali pravne osebe niso sodelovali.

10. NAVEDBA, KATERI PREDSTAVNIKI PREDLAGATELJA BODO SODELOVALI PRI DELU DRŽAVNEGA ZBORA IN DELOVNIH TELES

Dobran Božič, direktor, Urad Vlade RS za varovanje tajnih podatkov,
Marko Rosandič, podsekretar, Urad Vlade RS za varovanje tajnih podatkov,
Mateja Kapš, sekretarka, Urad Vlade RS za varovanje tajnih podatkov.

I. BESEDILO ČLENOV

1. člen

V Zakonu o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10 in 60/11) se besedilo 2. člena spremeni tako, da se glasi:

»Posamezni izrazi, uporabljeni v tem zakonu, imajo naslednji pomen:
1. tajni podatek je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno;
2. tajni podatek tuje države je podatek, ki ga je Republiki Sloveniji oziroma njenim organom posredovala tuja država oziroma njen organ ali mednarodna organizacija oziroma njen organ v pričakovanju, da bo ostal tajen, ter podatek, ki je rezultat sodelovanja Republike Slovenije oziroma njenih organov s tujo državo ali mednarodno organizacijo oziroma njihovimi organi in za katerega se dogovori, da mora ostati tajen;
3. dokument je vsak napisan, narisan, natisnjen, razmnožen, posnet, fotografiran, magneten, optičen ali kakšen drugačen zapis tajnega podatka;
4. medij je vsako sredstvo, ki vsebuje tajne podatke;
5. kriptografska rešitev je kriptografska strojna oziroma programska oprema ter s tem povezani sestavni deli, ki so vgrajeni v komunikacijsko-informacijski sistem;
6. določanje tajnih podatkov je dejanje ali postopek, s katerim se podatek v skladu s tem zakonom oceni za tajnega in se mu določita stopnja in rok tajnosti ali s katerim se mu stopnja tajnosti spremeni ali prekliče;
7. prenehanje tajnosti podatka je zakonita sprememba tajnega podatka v podatek, ki je dostopen v skladu s splošnimi predpisi, ki urejajo poslovanje organa;
8. dostop do tajnega podatka je seznanitev osebe s tajnim podatkom ali možnost osebe pridobiti tajni podatek;
9. varnostno preverjanje je poizvedba, ki jo v postopku pridobivanja dovoljenja za dostop do tajnih podatkov ali varnostnega dovoljenja organizacije ter v postopku vmesnega varnostnega preverjanja opravi pristojni organ in katere namen je zbrati podatke o morebitnih varnostnih zadržkih;
10. varnostni zadržki so ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo utemeljeni dvomi o zanesljivosti ali verodostojnosti osebe za varno obravnavanje in varovanje tajnih podatkov;
11. ogrožanje vitalnih interesov države je ogrožanje njene ustavne ureditve, neodvisnosti, ozemeljske celovitosti obrambne sposobnosti in javne varnosti;
12. obravnavanje tajnih podatkov je določanje, označevanje, dostop do, uporaba, evidentiranje, razmnoževanje, posredovanje, prenos, uničevanje nosilcev tajnih podatkov ter drugi ukrepi in postopki, povezani z delom s tajnimi podatki;
13. varovanje tajnih podatkov je uporaba ukrepov in postopkov za obravnavanje, hrambo, arhiviranje in nadzor nad tajnimi podatki v njihovem življenjskem ciklu, ki pripomorejo k odvračanju in odkrivanju namernega in naključnega nepooblaščenega razkritja ali izgube takih podatkov;

14. povezana oseba je zakoniti zastopnik, prokurist, član uprave, lastnik ali delničar, ki ima v lasti vsaj 25-odstotni lastniški ali upravljavski delež organizacije, in druge upravljavsko ali kapitalsko povezane osebe, ki imajo korist od dejavnosti organizacije, ki nadzirajo ali bi lahko izvajale neposredni ali posredni nadzor nad organizacijo, ter osebe, ki financirajo ali bi lahko neposredno ali posredno financirale dejavnost organizacije;
15. ponovna uporaba tajnega podatka je ponovna vsebinska obravnava tajnega podatka, zaradi česar se tajni podatek prenese iz tekoče ali stalne zbirke dokumentarnega gradiva v zbirko nerešenih zadev, zaradi izvajanja zakonsko določenih nalog organa;
16. varnostno vrednotenje je postopek preverjanja skladnosti varnostnih ukrepov z vsemi varnostnimi zahtevami;
17. varnostno ovrednotenje je zaključek postopka preverjanja skladnosti varnostnih ukrepov z vsemi varnostnimi zahtevami.
18. predstojnik organa v ministrstvu je minister in predstojnik organa v sestavi ministrstva, razen v 22.f, 35.a in 38. členu tega zakona, kjer je predstojnik organa v ministrstvu le minister.«.

2. člen

Besedilo 3. člena se spremeni tako, da se glasi:

»V zvezi z opravljanjem svoje funkcije lahko do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov dostopa:
– predsednik republike;
– predsednik vlade;
– poslanec;
– državni svetnik;
– minister in predstojnik vladne službe, ki je neposredno odgovoren predsedniku vlade;
– varuh človekovih pravic in namestnik varuha človekovih pravic;
– guverner in namestnik guvernerja Banke Slovenije;
– član Računskega sodišča;
– član Fiskalnega sveta;
– predsednik in član Državne revizijske komisije;
– sodnik;
– sodnik Ustavnega sodišča;
– državni tožilec;
– državni odvetnik in
– informacijski pooblaščenec.

Ne glede na določbo prejšnjega odstavka lahko v zvezi z opravljanjem svoje funkcije do tajnih podatkov tuje države ali mednarodne organizacije brez pooblastila za dostop do tujih tajnih podatkov dostopa:
– predsednik republike;
– predsednik vlade;
– predsednik državnega sveta;
– predsednik vrhovnega sodišča;
– poslanec in
– minister.

Osebe iz tega člena lahko dostopajo do tajnih podatkov po opravljenem osnovnem usposabljanju, ki ga izvede nacionalni varnostni organ, in s podpisom izjave, da so seznanjene s tem zakonom in drugimi predpisi, ki urejajo varovanje tajnih podatkov, ter da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi.«.

3. člen

Za 16. členom se doda nov 16.a člen, ki se glasi:

»16.a člen

Kadar je organ ali organizacija, v kateri je bila stopnja tajnosti podatka določena,

- prenehala obstajati ali poslovati in nima pravnega naslednika, ali
- na podlagi veljavnih predpisov niti organ niti organizacija ali njun pravni naslednik nista pooblaščena za določanje stopnje tajnosti,

o nadaljnjem obstoju stopnje tajnosti tajnega podatka odloča organ, ki je vsebinsko pristojen za področje, na katerega se tajni podatek nanaša.

V primeru spora o pristojnosti iz prejšnjega odstavka odloča Vlada Republike Slovenije (v nadaljnjem besedilu: vlada), če ni z zakonom drugače določeno.«.

4. člen

V četrtem odstavku 17. člena se besedilo »Vlada Republike Slovenije (v nadaljnjem besedilu: vlada)« nadomesti z besedo »Vlada«.

5. člen

Besedilo 22.g člena se spremeni tako, da se glasi:

»Postopek varnostnega preverjanja za izdajo dovoljenja se začne na pisni predlog predlagatelja za osebo, ki jo je treba varnostno preveriti (v nadaljnjem besedilu: preverjana oseba). Pisni predlog mora vsebovati osebno ime in rojstni datum preverjane osebe ter podatke o stopnji tajnosti tajnih podatkov, za dostop do katerih je dan predlog za izdajo dovoljenja.

Predlagatelj mora predlogu priložiti pisno soglasje preverjane osebe za varnostno preverjanje, dokazilo o opravljenem usposabljanju s področja varovanja tajnih podatkov, ki ne sme biti starejše od enega leta, pisno izjavo o seznanitvi s tem zakonom in predpisi, izdanimi na njegovi podlagi, ter zaprto ovojnico z izpolnjenim varnostnim vprašalnikom preverjane osebe.«.

6. člen

Besedilo 25.b člena se spremeni tako, da se glasi:

»Če je pri osebi, ki ima veljavno dovoljenje za dostop do tajnih podatkov katerekoli stopnje tajnosti, podan sum obstoja varnostnega zadržka iz 27. člena tega zakona, se opravi vmesno varnostno preverjanje.

Vmesno varnostno preverjanje se opravi na predlog predstojnika organa ali organizacije, v kateri oseba opravlja funkcijo ali izvaja naloge. Postopek vmesnega varnostnega preverjanja se lahko začne tudi po uradni dolžnosti, če pristojni organ ugotovi, da je treba glede na obstoječe dejansko stanje zaradi javne koristi začeti postopek.

Nacionalni varnostni organ lahko da pristojnemu organu predlog za vmesno varnostno preverjanje osebe, če pri nadzoru iz sedme alineje tretjega odstavka 43.b člena tega zakona ugotovi sum varnostnega zadržka iz 27. člena tega zakona. O tem mora obvestiti predstojnika organa ali organizacije, kjer je oseba, za katero predlaga vmesno varnostno preverjanje, zaposlena.

V postopku vmesnega varnostnega preverjanja lahko pristojni organ pri ugotavljanju obstoja suma varnostnega zadržka preveri katerekoli okoliščine, ki so povezane z varnostnim zadržkom in s pomočjo katerih se lahko v postopku vmesnega varnostnega preverjanja ugotovi obstoj oziroma neobstoj varnostnega zadržka.
Če pristojni organ pri vmesnem varnostnem preverjanju ugotovi varnostni zadržek, mora osebi preklicati vsa veljavna dovoljenja za dostop do tajnih podatkov. Odločba o preklicu dovoljenja za dostop do tajnih podatkov se vroči osebi, ki ji je bilo dovoljenje za dostop do tajnih podatkov preklicano, in predlagatelju postopka ter se o tem obvesti nacionalni varnostni organ.«.

7. člen

Besedilo 35.a člena se spremeni tako, da se glasi:

»Postopek izdaje varnostnega dovoljenja iz prejšnjega člena se začne na podlagi pisnega predloga predstojnika:
1. organa iz drugega odstavka 1. člena tega zakona za organizacije, ki izvajajo naročilo tega organa oziroma sodelujejo v postopku izvajanja naročila tajne narave tega organa;
2. ministrstva, pristojnega za gospodarstvo, za organizacije, ki potrebujejo varnostno dovoljenje zaradi sodelovanja na javnih razpisih tuje države ali mednarodne organizacije ali izvedbe naročila tuje države ali mednarodne organizacije;
3. nacionalnega varnostnega organa za primere, ki niso zajeti v 1. In 2. točki tega odstavka.

Iz predloga mora izhajati način obravnavanja in varovanja tajnih podatkov v okviru izvajanja naročila, ki je lahko v prostorih naročnika ali v prostorih organizacije.

Predlagatelj mora predlogu za začetek postopka varnostnega preverjanja priložiti izpolnjen varnostni vprašalnik za organizacije in naslednje listine:
1. podatke o registraciji organizacije;
2. pisno soglasje organizacije za varnostno preverjanje;
3. podatke o stopnji, vrsti in načinu obravnavanja in varovanja tajnih podatkov, za dostop do katerih je podan predlog za izdajo varnostnega dovoljenja;
4. pisno soglasje naročnika, če bo organizacija obravnavala in varovala nacionalne tajne podatke v njegovih prostorih;
5. seznam oseb in predloge za izdajo dovoljenj za dostop do tajnih podatkov zaposlenim v organizaciji, ki bodo zaradi izvedbe tajnega naročila ali sodelovanja v postopku tajnega naročila potrebovali dostop do tajnih podatkov;
6. seznam delovnih mest, kjer se zahteva dostop do tajnih podatkov;
7. pisno soglasje za preveritev podatkov iz 35.b člena tega zakona o osebah, zaposlenih v organizaciji, ki bodo zaradi izvedbe tajnega naročila oziroma sodelovanja v postopku tajnega naročila potrebovale dostop do tajnih podatkov stopnje tajnosti INTERNO.

Organizacija mora pred zaključkom postopka varnostnega preverjanja organu, pristojnemu za izdajo varnostnega dovoljenja, predložiti:
1. akt iz 38. člena tega zakona ter mnenje nacionalnega varnostnega organa o skladnosti akta s tem zakonom in predpisi, sprejetimi na njegovi podlagi;
2. mnenje nacionalnega varnostnega organa o ustreznosti varnostnotehnične opreme, vgrajene v varnostno območje, ter postopkov in ukrepov varovanja varnostnega območja, če bodo tajne podatke stopnje tajnosti ZAUPNO ali višje obravnavali in varovali v prostorih organizacije;
3. sklep, v katerem določi prostore upravnega oziroma varnostnega območja, če bo organizacija obravnavala in varovala tajne podatke v lastnih prostorih;
4. sklep o imenovanju osebe iz 4. točke drugega odstavka 35.b člena tega zakona.

Pri izdelavi akta iz 38. člena tega zakona se smiselno upoštevajo določbe drugega odstavka 38. člena glede na vrsto varnostnega dovoljenja.«.

8. člen

Besedilo 35.b člena se spremeni tako, da se glasi:

»Varnostno preverjanje organizacije se opravi tako, da pristojni organ iz drugega odstavka 35. člena tega zakona preveri navedbe v vprašalniku za varnostno preverjanje z namenom preveritve podatkov iz tretjega odstavka prejšnjega člena in izpolnjevanja pogojev iz drugega odstavka tega člena ter zbira podatke o organizaciji, na katero se podatki nanašajo, iz uradnih evidenc ali pri drugih organih, organizacijah ali osebah, ki o teh podatkih kaj vedo.

Pristojni organ v postopku varnostnega preverjanja preveri, ali:

1. organizacija izpolnjuje fizične, organizacijske in tehnične pogoje za obravnavanje in varovanje tajnih podatkov v skladu s tem zakonom in predpisi, sprejetimi na njegovi podlagi;
2. so osebe, ki bodo v organizaciji imele dostop do tajnih podatkov, varnostno preverjene in imajo dovoljenje za dostop do tajnih podatkov ali izpolnjujejo pogoje za dostop do tajnih podatkov stopnje tajnosti INTERNO;
3. organizacija zagotavlja, da bo dostop do tajnih podatkov dovoljen samo tistim osebam, ki morajo imeti vpogled v te podatke po svoji službeni dolžnosti zaradi uresničevanja naročila organa;
4. je organizacija imenovala osebo, pristojno za nadzor in usmerjanje varnostnih ukrepov v zvezi z izvajanjem naročila, usposabljanje oseb, ki imajo dostop do tajnih podatkov, poročanje pristojnemu organu o okoliščinah, ki vplivajo na izdajo varnostnega dovoljenja organizacije, in izvajanje drugih predpisanih ukrepov za varno obravnavanje in varovanje tajnih podatkov;
5. je organizacija registrirana pri pristojnem sodišču ali drugem organu;
6. organizacija ni v kazenskem postopku zaradi suma storitve kaznivega dejanja v zvezi s podkupovanjem ali zaradi takega kaznivega dejanja ni bila pravnomočno obsojena;
7. zoper organizacijo ni uveden ali začet postopek prisilne poravnave, stečajni postopek, likvidacijski postopek ali drug postopek, katerega posledica ali namen je lahko prenehanje poslovanja organizacije;
8. organizacija na dan preverjanja pogojev izpolnjuje obvezne dajatve in druge denarne nedavčne obveznosti, ki jih pobira davčni organ v Republiki Sloveniji v skladu s predpisi. Organizacija ne izpolnjuje pogojev iz prejšnjega stavka, če vrednost teh neplačanih zapadlih obveznosti na dan preverjanja pogojev znaša 50 eurov ali več;
9. organizacija ni bila kaznovana za kaznivo dejanje v zvezi s poslovanjem;
10. povezane osebe niso sodelovale oziroma ne sodelujejo z organizacijami ali skupinami, ki ogrožajo interese Republike Slovenije ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je Republika Slovenija, ali ni drugih varnostnih zadržkov glede povezanih oseb organizacije.

Pogoje iz prejšnjega odstavka ugotavlja na predlog pristojnega predlagatelja iz prvega odstavka 35.a člena tega zakona organ, pristojen za to, da se organizaciji izda varnostno dovoljenje. Pristojni organ o zaključku varnostnega preverjanja pisno obvesti nacionalni varnostni organ.

Če je lastnik organizacije v višini vsaj 25 odstotkov druga organizacija, se varnostni zadržki ugotavljajo tudi za povezane osebe druge organizacije.

Predlagatelj postopka in organizacija morata ves čas postopka sodelovati s pristojnim organom. Če predlagatelj ali organizacija ne sodelujeta s pristojnim organom, se to šteje za umik predloga.

Oseba, ki bo v organizaciji po službeni dolžnosti imela dostop do tajnih podatkov stopnje tajnosti INTERNO, mora poleg pogojev iz drugega odstavka 31.a člena tega zakona izpolnjevati še naslednje pogoje:
- da ni bila pravnomočno obsojena zaradi naklepnega kaznivega dejanja, katerega storilec se preganja po uradni dolžnosti, na nepogojno kazen zapora v trajanju več kot šest mesecev;
- da ni v kazenskem postopku zaradi kaznivega dejanja iz prejšnje alineje.

Vlada podrobneje predpiše način in postopek ugotavljanja izpolnjevanja pogojev za izdajo varnostnega dovoljenja, vrste varnostnih dovoljenj in vsebino varnostnega vprašalnika za organizacije.«.

9. člen

Besedilo 35.c člena se spremeni tako, da se glasi:

»Izdaja varnostnega dovoljenja organizaciji se zavrne ali se veljavna varnostna dovoljenja organizacije prekličejo, če organizacija ne izpolnjuje enega ali več pogojev iz drugega odstavka 35.b člena tega zakona.

Izdaja varnostnega dovoljenja organizaciji se lahko zavrne ali se veljavna varnostna dovoljenja organizacije lahko prekličejo tudi iz razlogov, ki vzbujajo utemeljen dvom glede ustreznosti obravnavanja in varovanja tajnih podatkov.«.

10. člen

Besedilo 35.d člena se spremeni tako, da se glasi:

»Če se po izdaji varnostnega dovoljenja pojavijo okoliščine, ki kažejo na to, da organizacija ne izpolnjuje več pogojev iz 35.b člena tega zakona, ali v primeru drugih ugotovitev varnostnega preverjanja, ki vzbujajo utemeljen dvom glede ustreznosti obravnavanja in varovanja tajnih podatkov, pristojni organ iz drugega odstavka 35. člena tega zakona opravi postopek vmesnega varnostnega preverjanja.

Pristojni organ iz drugega odstavka 35. člena tega zakona lahko v organizaciji ves čas veljavnosti varnostnega dovoljenja preverja izpolnjevanje pogojev za varno obravnavanje tajnih podatkov iz varnostnega dovoljenja.

Vmesno varnostno preverjanje se opravi na predlog pristojnega predlagatelja iz 35.a člena tega zakona, na predlog nacionalnega varnostnega organa ali po uradni dolžnosti, kadar pristojni organ iz drugega odstavka 35. člena tega zakona pri preverjanju izpolnjevanja pogojev iz prejšnjega odstavka ugotovi neizpolnjevanje pogojev za izdajo varnostnega dovoljenja.

Pri postopku vmesnega varnostnega preverjanja se preverijo vsi pogoji iz 35.b člena tega zakona.

Če pri vmesnem varnostnem preverjanju pristojni organ iz drugega odstavka 35. člena tega zakona ugotovi, da organizacija ne izpolnjuje več pogojev, ki jih ta zakon določa za izdajo varnostnega dovoljenja organizaciji, ji varnostno dovoljenje prekliče in o tem obvesti tudi nacionalni varnostni organ.

Če organizacija ne da soglasja za uvedbo vmesnega varnostnega preverjanja, se varnostno dovoljenje organizacije prekliče.

Do zaključka postopka vmesnega varnostnega preverjanja mora predlagatelj organizaciji onemogočiti obravnavanje in varovanje tajnih podatkov. O tem mora izdati pisni sklep in obvestiti nacionalni varnostni organ. Organizacija mora o izdanem pisnem sklepu pisno obvestiti vse naročnike, za katere izvaja naročilo, katerega izpolnitev zahteva ali vključuje dostop do tajnih podatkov.

Zoper odločbo, izdano v postopku varnostnega preverjanja organizacije, ni dovoljena pritožba, dovoljen pa je upravni spor, ki ga lahko sprožita predlagatelj ali preverjana organizacija.«.

11. člen

Besedilo 39. člena se spremeni tako, da se glasi:

»Upravno območje je prostor, določen s sklepom predstojnika organa ali organizacije, v kateri se pod določenimi pogoji obravnavajo tajni podatki do stopnje tajnosti TAJNO in hranijo tajni podatki stopnje tajnosti INTERNO.

Varnostno območje je vidno označen prostor, določen s sklepom predstojnika organa ali organizacije, v kateri se varujejo tajni podatki stopnje tajnosti ZAUPNO ali višje.

Organ ali organizacija o določitvi upravnega oziroma varnostnega območja obvesti nacionalni varnostni organ.

Tajne podatke se varuje v upravnem ali varnostnem območju na način, ki zagotavlja, da imajo dostop do teh podatkov samo osebe, ki izpolnjujejo pogoje za dostop do tajnih podatkov in ki podatke potrebujejo za izvajanje svojih delovnih nalog ali funkcij.

Vsak organ in organizacija mora določiti, kje se sprejemajo tajni podatki in kdo jih sprejema, ter o tem obvestiti nacionalni varnostni organ.

Tajni podatki se lahko pošljejo izven upravnega ali varnostnega območja samo ob upoštevanju predpisanih varnostnih ukrepov in postopkov.

Postopki in ukrepi varovanja pošiljanja tajnih podatkov izven upravnega ali varnostnega območja se predpišejo glede na stopnjo tajnosti in medij.

Vlada podrobneje predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov.

Za prejemanje in razpošiljanje tajnih podatkov Evropske Unije (v nadaljnjem besedilu: EU) in zveze Nato, se v Republiki Sloveniji vzpostavi registrski sistem.

Registrski sistem EU obsega centralni register EU, ki deluje v okviru ministrstva, pristojnega za zunanje zadeve, in podregistre EU, ki jih s sklepom določi predstojnik organa ali organizacije. Organ ali organizacija o vzpostavitvi registra EU in podregistra EU obvesti nacionalni varnostni organ.

Registrski sistem zveze Nato obsega centralni register Nato, podregistre Nato in kontrolne točke Nato. Centralni register Nato deluje v okviru ministrstva, pristojnega za obrambo. Podregistre Nato in kontrolne točke Nato s sklepom določi predstojnik organa ali organizacije. Organ ali organizacija o vzpostavitvi podregistra Nato oziroma kontrolne točke Nato, obvesti nacionalni varnostni organ.

Vlada podrobneje predpiše pogoje in način vzpostavitve centralnih registrov, podregistrov in kontrolnih točk.«.

12. člen

Za 39. členom se doda nov 39.a člen, ki se glasi:

»**39.a člen**

Tajni podatki v elektronski obliki se smejo obravnavati in hraniti le v komunikacijsko-informacijskih sistemih (v nadaljnjem besedilu: sistemi), ki imajo veljavno varnostno dovoljenje za delovanje sistema najmanj enake stopnje tajnosti, kot je najvišja stopnja tajnosti v njih obravnavanih in hranjenih podatkov.

Nacionalni varnostni organ opravi varnostno vrednotenje sistema, s katerim preveri, ali sistem izpolnjuje varnostne zahteve za varovanje tajnih podatkov do določene stopnje tajnosti. Če sistem izpolnjuje vse varnostne zahteve, nacionalni varnostni organ izda varnostno dovoljenje za delovanje sistema.

Z varnostnimi ukrepi v sistemih se zagotovi, da so tajni podatki v sistemih zaščiteni pred razkritjem, zlorabo ali izgubo, da so zagotovljene njihova celovitost, razpoložljivost in verodostojnost ter da ni možna zatajitev dostopanja do podatkov.

Varovanje tajnih podatkov v sistemih temelji na postopku obvladovanja tveganj, ki zajema identifikacijo in oceno tveganj, posledice tveganj, ukrepe za zmanjšanje tveganj na sprejemljivo raven ter odgovornost za preostala tveganja.

Vse sestavine sistemov, v katerih se obravnavajo in hranijo tajni podatki stopnje tajnosti ZAUPNO ali višje, morajo biti zaščitene proti neželenemu elektromagnetnemu sevanju.

Elektronski prenos tajnih podatkov izven upravnega ali varnostnega območja je dovoljen le z uporabo kriptografskih rešitev, ki jih je na podlagi postopka ugotavljanja ustreznosti kriptografskih rešitev odobril nacionalni varnostni organ.

Ne glede na prejšnji odstavek se lahko v izrednem ali vojnem stanju tajni podatki v elektronski obliki stopnje tajnosti INTERNO, ZAUPNO in TAJNO prenašajo v sistemih, odobrenih za nižjo stopnjo tajnosti, ali v nekriptirani obliki.

Postopek ugotavljanja ustreznosti kriptografskih rešitev za varovanje tajnih podatkov je postopek, v katerem se ugotovi varnostna ustreznost kriptografske rešitve, in se izvaja na podlagi pisnih predlogov, ki jih podajo ministrstvo, pristojno za javno upravo, ministrstvo, pristojno za notranje zadeve, ministrstvo, pristojno za obrambo, ministrstvo, pristojno za zunanje zadeve, Slovenska obveščevalno-varnostna agencija ali nacionalni varnostni organ. Postopek in vsebino dokumentacije, ki jo mora vsebovati predlog, določi vlada.

Kriptografsko rešitev lahko za organe iz prejšnjega odstavka razvije ali izdela organizacija, ki ima veljavno varnostno dovoljenje ustrezne stopnje tajnosti za varovanje tajnih podatkov na sedežu organizacije, veljavno še najmanj eno leto od vložitve vloge.

Postopek iz osmega odstavka tega člena lahko traja največ eno leto od prejema popolne vloge. Izjemoma, zaradi zahtevnosti kriptografske rešitve, se lahko postopek podaljša še za eno leto.

Če nacionalni varnostni organ ugotovi, da so predlagane kriptografske rešitve ustrezne, izda potrdilo o varnostni ustreznosti.

Obravnavanje tajnih podatkov izven varnostnega ali upravnega območja je dovoljeno z uporabo kriptografskih rešitev, za katere je izdano potrdilo o varnostni ustreznosti. Dostop do kriptografskih rešitev in podatkov mora biti ustrezno zaščiten, da ni možen nepooblaščen dostop.

Nacionalni varnostni organ izvaja naslednje naloge za zagotavljanje varovanja tajnih podatkov v sistemih:
- razvoj kriptografskih rešitev,
- varnostno vrednotenje sistemov,
- zaščita pred neželenim elektromagnetnim sevanjem,
- ugotavljanje ustreznosti kriptografskih rešitev,
- distribucija kriptografskega materiala.

Vlada podrobneje predpiše varnostne zahteve za varovanje tajnih podatkov v sistemih in fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov v sistemih.«.

13. člen

Drugi odstavek 43. člena se spremeni tako, da se glasi:

»Naloge nacionalnega varnostnega organa opravlja pristojni nacionalni organ za varnost omrežij in informacijskih sistemov.«.

14. člen

Besedilo 43.b člena se spremeni tako, da se glasi:

»Nacionalni varnostni organ skrbi za sklepanje in izvrševanje mednarodnih pogodb ter sprejetih mednarodnih obveznosti, ki jih je v zvezi z varovanjem tajnih podatkov sklenila ali sprejela Republika Slovenija, ter na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij, razen če mednarodna pogodba določa drugače.

Nacionalni varnostni organ usklajuje dejavnosti za zagotavljanje varnosti nacionalnih tajnih podatkov v tujini in tujih tajnih podatkov na območju Republike Slovenije.

V zvezi z izvrševanjem mednarodnih pogodb in sprejetih mednarodnih obveznosti nacionalni varnostni organ opravlja zlasti naslednje naloge:
– izdaja in preklicuje pooblastila za dostop do tujih tajnih podatkov;
– izdaja in preklicuje varnostna dovoljenja organizacijam za dostop do tujih tajnih podatkov;
– izdaja in preklicuje varnostna dovoljenja za sisteme in naprave za prenos, hranjenje in obdelavo tujih tajnih podatkov v skladu s sprejetimi mednarodnimi pogodbami;
– opravlja naloge organa za varnostno odobritev sistemov, organa za kriptografsko zaščito tujih tajnih podatkov, organa za razdeljevanje kriptografskega materiala in organa za zaščito pred neželenim elektromagnetnim sevanjem naprav v sistemih, v katerih se varujejo tuji tajni podatki, v skladu s sprejetimi mednarodnimi pogodbami;
– ugotavlja, ali posamezni organ ali organizacija za obravnavanje in varovanje tajnih podatkov tujih držav in mednarodnih organizacij izpolnjuje za to predpisane pogoje;
– sprejema in na svoji spletni strani objavlja navodila za izmenjavo in varovanje tajnih podatkov tuje države ali mednarodne organizacije;
– nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države ali mednarodne organizacije ter skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki so jih organi dolžni nemudoma izvršiti;
- ugotavlja ustreznost postopkov in ukrepov varovanja tujih tajnih podatkov v organih in organizacijah;
– od pristojnega inšpektorata zahteva izvedbo inšpekcijskega nadzora pri določenem organu ali organizaciji;
– izmenjuje podatke z nacionalnimi varnostnimi organi tujih držav in z mednarodnimi organizacijami.

Pred izdajo pooblastila iz prve alineje oziroma dovoljenja iz druge alineje prejšnjega odstavka lahko, kadar prejme obvestilo tujega varnostnega organa o varnostnem zadržku, od organa, pristojnega za varnostno preverjanje, zahteva vmesno varnostno preverjanje osebe ali organizacije.«.

15. člen

Besedilo 43.c člena se spremeni tako, da se glasi:

»Oseba lahko dostopa do tujih tajnih podatkov stopnje tajnosti INTERNO v skladu z 31.a členom tega zakona oziroma šestim odstavkom 35.b člena tega zakona in po podpisu izjave o seznanitvi s predpisi s področja varovanja tujih tajnih podatkov.

Nacionalni varnostni organ izda pooblastilo iz prve alineje tretjega odstavka prejšnjega člena na predlog predlagateljev iz 22.f člena tega zakona, če ima oseba veljavno dovoljenje iz 22. člena tega zakona in opravlja funkcijo ali izvaja naloge na delovnem mestu, na katerem potrebuje pooblastilo za dostop do tujih tajnih podatkov. Pooblastilo se izda z veljavnostjo za čas, ko oseba potrebuje dostop do tujih tajnih podatkov, vendar ne za dlje, kot velja dovoljenje iz 22. člena tega zakona.

Pisni predlog mora vsebovati: osebno ime, datum in kraj rojstva osebe, za katero se predlaga izdaja pooblastila za dostop do tujih tajnih podatkov, navedbo tuje države ali mednarodne organizacije, do tajnih podatkov katere naj bi imela oseba dostop, stopnjo tajnosti podatkov ter navedbo delovnega mesta.

Če oseba, ki ji je bilo izdano pooblastilo za dostop do tujih tajnih podatkov, ne izvaja več nalog, pri katerih potrebuje dostop do tujih tajnih podatkov, je predstojnik organa ali organizacije dolžan o tem takoj obvestiti nacionalni varnostni organ.

Nacionalni varnostni organ pooblastilo za dostop do tujih tajnih podatkov prekliče, ko prenehajo obstajati pogoji za njegovo izdajo iz drugega odstavka tega člena.

Organ ali organizacija, pri kateri je oseba v pogodbenem razmerju, hrani pooblastilo za dostop do tujih tajnih podatkov ali izjavo iz prvega odstavka tega člena v kadrovski evidenci te osebe.«.

16. člen

Besedilo 43.e člena se spremeni tako, da se glasi:

»Za namene izvrševanja pristojnosti in nalog po tem zakonu, drugih zakonih in obvezujočih mednarodnih pogodbah nacionalni varnostni organ upravlja naslednje evidence in obdeluje osebne podatke v njih:

1. evidenco dovoljenj, izdanih na podlagi 22. člena tega zakona, ki vsebuje naslednje podatke:
– osebno ime;
– datum rojstva;
– organ, kjer je oseba zaposlena;
– organ, ki je izdal dovoljenje;
– stopnja tajnosti podatkov, do katerih ima oseba dostop;
– številka in datum izdaje ter datum veljavnosti dovoljenja;
– datum in organ, ki je opravil preklic dovoljenja;
2. evidenco zavrnjenih predlogov za izdajo dovoljenj, ki vsebuje naslednje podatke:
– osebno ime;
– datum rojstva;
– organ, kjer je oseba zaposlena;
– organ, ki je zavrnil izdajo dovoljenja;
– datum in razlog zavrnitve izdaje dovoljenja;
3. evidenco izdanih pooblastil za dostop do tujih tajnih podatkov iz prve alineje tretjega odstavka 43.b člena tega zakona, ki vsebuje naslednje podatke:
– osebno ime;
– datum rojstva;
– organ, kjer je oseba zaposlena;
– stopnja tajnosti podatkov, do katerih ima oseba dostop;
– številka in datum izdaje ter datum veljavnosti dovoljenja;
– številka in datum izdaje pooblastila za dostop do tujih tajnih podatkov ter datum njegove veljavnosti;
4. evidenco varnostnih dovoljenj iz 35. člena tega zakona in evidenco varnostnih dovoljenj iz druge alineje tretjega odstavka 43.b člena tega zakona, ki vsebuje naslednje podatke:
– naziv in naslov organizacije;
– organ, ki je izdal varnostno dovoljenje;
– številka in datum izdaje ter datum veljavnosti varnostnega dovoljenja;
– datum, razlog in organ, ki je opravil preklic varnostnega dovoljenja;
– osebno ime, datum rojstva ter položaj osebe iz 4. točke drugega odstavka 35.b člena tega zakona;
– številka dovoljenja in stopnja tajnosti podatkov, do katerih ima oseba iz prejšnje alineje pravico dostopa, oziroma za stopnjo tajnosti INTERNO datum podpisa izjave o seznanitvi s predpisi, ki urejajo obravnavanje in varovanje tujih tajnih podatkov;
– vrsta varnostnega dovoljenja;
5. evidenco zavrnjenih predlogov za izdajo varnostnih dovoljenj iz 35. člena tega zakona, ki vsebuje naslednje podatke:
– naziv in naslov organizacije;
– organ, ki je zavrnil izdajo varnostnega dovoljenja;
– datum in razlog zavrnitve izdaje varnostnega dovoljenja;
– vrsta zavrnjenega varnostnega dovoljenja;
6. evidenco o opravljenem posebnem delu strokovnega izpita za inšpektorja iz 42.e člena tega zakona, ki vsebuje naslednje podatke:
– osebno ime;
– datum rojstva;
– organ, kjer je oseba zaposlena;
– datum in kraj opravljanja izpita;
– uspeh, dosežen na izpitu;

7. evidenco začasnih dostopov do tajnih podatkov na podlagi drugega odstavka 30. člena tega zakona, ki vsebuje naslednje podatke:
– osebno ime;
– datum in kraj rojstva;
– organ, kjer je oseba zaposlena;
– stopnja tajnosti podatkov, do katerih ima oseba dostop;
– številka in datum veljavnosti dovoljenja;
– stopnja tajnosti podatkov, do katerih ima oseba začasen dostop;
– obdobje (trajanje) začasnega dostopa;
8. evidenco upravnih in varnostnih območij v organih in organizacijah, ki vsebuje naslednje podatke:
– ime organa ali organizacije;
– naslov organa ali organizacije;
– tip prostora: upravno ali varnostno območje;
– datum izdaje sklepa o določitvi upravnega ali varnostnega območja;
– številka sklepa o določitvi upravnega ali varnostnega območja;
– številka dokumenta – mnenje o ustreznosti varnostnotehnične opreme, vgrajene v varnostno območje, ter postopkov in ukrepov varovanja varnostnega območja;
– datum preklica sklepa o določitvi upravnega ali varnostnega območja;
9. evidenco registrov, podregistrov in kontrolnih točk tujih tajnih podatkov, ki vsebuje naslednje podatke:
– organ in ime registra, podregistra ali kontrolne točke;
– datum varnostne odobritve;
– najvišja stopnja tajnih podatkov, ki se varujejo v registru, podregistru ali kontrolni točki;
– podatki o vodji registra, podregistra ali kontrolne točke: ime in priimek ter kontaktni podatki (telefonska številka in elektronski naslov);
– podatki o namestniku vodje registra, podregistra ali kontrolne točke: ime in priimek ter kontaktni podatki (telefonska številka in elektronski naslov);
10. evidenco varnostno odobrenih komunikacijsko-informacijskih sistemov, ki vsebuje naslednje podatke:
– ime organa ali organizacije;
– kontaktni podatki organa ali organizacije;
– ime sistema;
– najvišja stopnja tajnosti podatkov, ki se lahko obravnavajo v sistemu;
– najvišja stopnja tajnosti podatkov, ki se lahko hranijo v sistemu;
– način delovanja;
– ime vodje informacijske varnosti;
– ime upravljavca;
– obdobje veljavnosti dovoljenja;
11. evidenco odobrenih kriptografskih rešitev, ki vsebuje naslednje podatke:
– ime kriptografske rešitve;
– ime proizvajalca;
– najvišja stopnja tajnosti podatkov, ki se lahko kriptirajo;
– obdobje veljavnosti dovoljenja;
– številka potrdila;
12. evidenco kriptografskega materiala, ki vsebuje naslednje podatke:
– izdajatelj kriptografskega materiala (organ, naslov, skrbnik);
– prejemnik kriptografskega materiala (organ, naslov, skrbnik);
– datum dogodka;
– vrsta dogodka;
– polno ime kriptografskega materiala;
– kratko ime kriptografskega materiala;
– količina kriptografskega materiala;
– številka oziroma številke kriptografskega materiala;
– opombe.

Organi in organizacije morajo nacionalnemu varnostnemu organu poslati podatke iz prejšnjega odstavka v 15 dneh od nastanka ali spremembe podatka.

Organi in organizacije, ki izvajajo osnovno usposabljanje, vodijo evidenco izdanih dokazil o udeležbi na osnovnem usposabljanju s področja obravnavanja in varovanja tajnih podatkov, ki vsebuje naslednje podatke:
– osebno ime;
– datum rojstva;
– organ ali organizacija, kjer je oseba zaposlena oziroma ki je osebo napotila na usposabljanje;
– datum usposabljanja;
– organ ali organizacija, ki je izvedel usposabljanje;
– številka dokazila.

Nacionalni varnostni organ določi način pošiljanja podatkov iz tega člena.

Evidence iz tega člena se hranijo trajno«.

17. člen

V prvem odstavku 44. člena se besedilo »od 1.000.000 do 3.000.000 tolarjev« nadomesti z besedilom od »5.000 do 15.000 eurov«.

26. točka se spremeni tako, da se glasi:
»26. če ravna v nasprotju s četrtim in šestim odstavkom 39. člena tega zakona;«.

Za 26. točko se doda nova 26.a točka, ki se glasi:
»26.a če ravna v nasprotju s prvim odstavkom 39.a člena tega zakona;«.

28. točka se spremeni tako, da se glasi:
»28. če ne organizira notranjega nadzora nad obravnavanjem tajnih podatkov (41. člen) ali izdajatelju varnostnega dovoljenja ne omogoči preverjanja izpolnjevanja pogojev za varno obravnavanje tajnih podatkov iz varnostnega dovoljenja (35.b člen);«.

V 29. točki se beseda »drugim« nadomesti z besedo »četrtim«;

Za 30. točko se doda nova 31. točka, ki se glasi:
»31. če nacionalnemu varnostnemu organu ne sporoči podatkov oziroma spremembe podatkov v skladu z drugim odstavkom 43.e člena tega zakona.«.

V drugem odstavku se besedilo »od 200.000 do 500.000 tolarjev« nadomesti z besedilom »od 1.000 do 3.000 eurov«.

18. člen

V prvem odstavku 44.a člena se besedilo »od 500.000 do 1.000.000 tolarjev« nadomesti z besedilom »od 2.000 do 5.000 eurov«.

V drugem odstavku se besedilo »od 100.000 do 300.000 tolarjev« nadomesti z besedilom »od 500 do 2.000 eurov«.

19. člen

V prvem odstavku 45. člena se besedilo »od 100.000 do 200.000 tolarjev« nadomesti z besedilom »od 500 do 1.000 eurov«.

PREHODNE IN KONČNE DOLOČBE

20. člen

Vlada Republike Slovenije v šestih mesecih od uveljavitve tega zakona izda predpise iz sedmega odstavka spremenjenega 35.b člena, osmega in dvanajstega odstavka spremenjenega 39. člena in štirinajstega odstavka novega 39.a člena zakona.

Nacionalni varnostni organ v skladu z drugim odstavkom novega 39.a člena zakona opravi varnostno vrednotenje vseh sistemov, v katerih se obravnavajo tajni podatki, v dveh letih od uveljavitve tega zakona.

21. člen

Do vzpostavitve pristojnega organa za varnost omrežij in informacijskih sistemov iz spremenjenega drugega odstavka 43. člena zakona opravlja naloge nacionalnega varnostnega organa Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

22. člen

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

II. OBRAZLOŽITEV ČLENOV

K 1. členu:

Skladno s pospešenim razvojem informacijske tehnologije je vedno več poudarka na varnem obravnavanju tajnih podatkov v komunikacijsko-informacijskih sistemih, kjer ima bistven pomen kriptografija. V povezavi s tem je predlagana dopolnitev 2. člena ZTP, in sicer z vpeljavo pojma »kriptografska rešitev«.

Prav tako se v 2. členu ZTP vpelje pojem »varnostno ovrednotenje«, ki označuje postopek pred izdajo varnostne odobritve uporabe komunikacijsko-informacijskega sistema kot tudi odobritve uporabe kriptografskih rešitev za varovanje tajnih podatkov.

Tajni podatek stopnje tajnosti ZAUPNO ali višje se lahko obravnava tudi zunaj varnostnega območja, če je prostor, v katerem se obravnava, fizično ali tehnično varovan, dostop do prostora pa je nadzorovan. Po končani obdelavi pa je treba tajni podatek vedno vrniti v varnostno območje. Dejstvo, da je tajni podatek stopnje tajnosti ZAUPNO ali višje treba vedno hraniti v varnostnem območju, je zahtevalo definiranje dveh pojmov, in sicer obravnavanje tajnega podatka, ki obsega tako imenovano rokovanje s tajnim podatkom, in varovanje tajnega podatka. Definicija pojma »varovanje tajnih podatkov« zajema tako obravnavanje tajnih podatkov kot tudi hranjenje in arhiviranje tajnih podatkov, skratka vse postopke in ukrepe v življenjskem ciklu tajnega podatka (od nastanka do uničenja tajnega podatka), da se prepreči nepooblaščeno razkritje tajnega podatka.

Glede na to, da se zaradi izvršitve naročila organa tajne podatke lahko posreduje tudi organizaciji, mora slednja izpolnjevati določene organizacijske, tehnične in fizične pogoje za varno obravnavanje tajnih podatkov. V povezavi s tem se je pokazala tudi potreba po preverjanju tako imenovanih povezanih oseb in posledično seveda po opredelitvi pomena izraza »povezana oseba« − to je oseba, ki ima v lasti določen lastniški ali upravljavski delež organizacije in bi lahko izvajala neposredni ali posredni nadzor nad organizacijo oziroma bi lahko vplivala na njeno dejavnost.

Dosedanja praksa je pokazala tudi na potrebo po opredelitvi pojma »ponovna uporaba« tajnega podatka. Sprememba opredeljuje, da gre pri ponovni uporabi za vsebinsko obravnavanje tajnega podatka (sam poseg in seznanitev z vsebino dokumenta), ne pa za tehnično opravilo (prenos tajnega podatke iz ene zbirke v drugo), pri katerem dejanske seznanitve z vsebino tajnega podatka ni.

Da bi se izognili dvomu, kdo je neposredno pristojna oseba za podajanje predlogov za postopek varnostnega preverjanja za izdajo dovoljenja za dostop do tajnih podatkov (minister, predstojnik organa v sestavi ministrstva, glavni inšpektor …), se je nedvomno pokazala tudi potreba po opredelitvi pojma »predstojnik organa«, kot ga predvideva ta zakon.

K 2. členu:

Državni zbor RS je na seji 10. 7. 2015 sprejel Zakon o fiskalnem pravilu. Zakon določa, da je Fiskalni svet samostojen in neodvisen državni organ, ki pripravlja in javno objavlja ocene, ki lahko vključujejo tudi priporočila v zvezi s skladnostjo javnofinančne politike s fiskalnimi pravili. RS se je z ratifikacijo mednarodne pogodbe o stabilnosti, usklajevanju in upravljanju v ekonomski in monetarni uniji zavezala k ustanovitvi Fiskalnega sveta. Poslanstvo slednjega je izvajanje neodvisnega nadzora nad javnofinančno politiko države. Z delovanjem je Fiskalni svet

začel v marcu 2017, ko so bili v državnem zboru z dvotretjinsko večino imenovani vsi trije člani, ki imajo status državnega funkcionarja. Glede na naloge, ki jih Zakon o fiskalnem pravilu nalaga Fiskalnemu svetu, menimo, da bi lahko za funkcionarje Fiskalnega sveta veljale enake pravice glede dostopanja do tajnih podatkov, kot jih imajo v zvezi z opravljanjem svoje funkcije osebe, ki so eksplicitno navedene v 3. členu trenutno veljavnega ZTP.

Zdaj veljavni 3. člen ZTP namreč določa osebe, ki lahko v zvezi z opravljanjem svoje funkcije dostopajo do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov. Osebe dobijo dovoljenje z začetkom opravljanja funkcije oziroma opravljanja dela in podpisom izjave, da so seznanjene z ZTP in drugimi predpisi, ki urejajo varovanje tajnih podatkov, ter da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi. Krog oseb, ki lahko do tajnih podatkov zaradi opravljanja svoje funkcije ali delovnih dolžnosti dostopajo brez dovoljenja za dostop do tajnih podatkov, je po slovenskih predpisih enormno širok in precej odstopa od primerljivih ureditev v državah članicah EU in zveze Nato, kjer je omejen le na ključne nosilce oblasti. S spremembo predpisov zveze Nato in EU so te iste osebe dobile tudi dostop brez dovoljenja za dostop do tajnih podatkov zveze Nato in EU (tuji tajni podatki), zato je bila RS od inšpekcije zveze Nato in EU vsakokrat opozorjena na preširok obseg izjem.

Ker se krog izjem na nacionalni ravni ne krči, in zaradi opozoril inšpekcijskih nadzorov na področju tujih tajnih podatkov, novela eksplicitno določa ozek krog oseb (ključne nosilce oblasti), ki bodo imele omogočen dostop tudi do tujih tajnih podatkov brez dovoljenja za dostop do tujih tajnih podatkov. S predlagano spremembo je dostop do tujih tajnih podatkov brez opravljenega varnostnega preverjanja omogočen le državnim funkcionarjem na najvišjih položajih, to je predsedniku republike, predsedniku vlade, državnega zbora in predsedniku vrhovnega sodišča ter ministrom in poslancem. Predlog spremembe 3. člena je tako kljub vsemu primerljiv z ureditvami, ki jih imajo v drugih državah članicah zveze Nato in EU, in v popolnosti odpravlja vse zadržke inšpekcijskih pregledov, ki sta jih izvedla zveza Nato in EU.

Osebe, ki bodo imele dostop do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov, in sicer tako nacionalnih kot tujih tajnih podatkov, pa bodo morale pred dostopom do tajnih podatkov opraviti osnovno usposabljanje, ki ga bo izvedel nacionalni varnostni organ, in podpisati izjavo, da so seznanjene z ZTP in drugimi predpisi, ki urejajo varovanje tajnih podatkov, ter da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi, kar je vsebina določbe tretjega odstavka istega člena. Glede na dejstvo, da je eden izmed pogojev za dostopanje do tujih tajnih podatkov tudi usposabljanje (osebe, ki lahko do tujih tajnih podatkov dostopajo v skladu nacionalnimi predpisi, torej brez dovoljenja, niso izvzete), je v progam osnovnega usposabljanja s področja tajnih podatkov med drugim vključeno tudi obravnavanje in varovanje tujih tajnih podatkov. UVTP meni, da je usposabljanje s področja tajnih podatkov najboljši način seznanitve s tem, kako ravnati s tovrstnimi podatki.

K 3. členu:

Državni organi se že dalj časa ukvarjajo z odbiranjem gradiva ter pripravo arhivskega gradiva za predajo v pristojni arhiv. V te postopke spada tudi ponovna ocena potrebe po nadaljnjem obstoju tajnosti podatkov. Nemalokrat se je izkazalo, da trenutno veljavni ZTP ne poda zadostnih usmeritev, saj se lahko obravnava gradivo avtorjev, ki ne obstajajo več ali pa njihovi pravni nasledniki niso več pooblaščeni za določanje stopenj tajnosti dokumentov. V nekaterih primerih obstaja tudi prenos vsebinskega področja dela na drug organ, zaradi česar lahko avtor ali njegov pravni naslednik morda upravičeno zavrne izdelavo ponovne ocene.

Na podlagi navedenega je treba zdaj veljavni ZTP dopolniti na način, da se opredeli ocenjevalca potrebe po nadaljnjem obstoju stopnje tajnosti tudi z vsebinskega vidika, saj avtor podatka ali njegov pravni naslednik za to po veljavnih predpisih nista pooblaščena. Kot primer lahko navedemo šole, krajevne skupnosti, različna podjetja … Ker v posameznih primerih lahko obstaja tudi spor o pristojnosti, predlagamo, da v takih primerih odloči vlada.

K 4. členu:

Sprememba je zgolj redakcijske narave.

K 5. členu:

Prvi odstavek člena opredeljuje vsebino predloga za začetek varnostnega preverjanja osebe za namen izdaje dovoljenja za dostop do tajnih podatkov (v nadaljnjem besedilu: predlog). Predlog mora vsebovati ime in priimek (osebno ime) ter rojstne podatke preverjane osebe, da jo je mogoče individualno ločiti od drugih oseb. V posameznih organih se pojavijo primeri, ko ima več oseb, ki potrebujejo dovoljenje za dostop do tajnih podatkov, enako ime in priimek. Ker je rojstni datum osebni podatek, ga je treba predpisati z zakonom, in ne s podzakonskim aktom (uredbo), kot je določeno zdaj.

Drugi odstavek eksplicitno navaja, da je predlagatelj postopka varnostnega preverjanja dolžan predlogu priložiti dokazilo o usposabljanju s področja tajnih podatkov, ki ne sme biti starejše od enega leta (Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov). Zdaj veljavni 22.g člen ZTP je mogoče interpretirati tudi v smislu, da mora predlagatelj predlogu vedno priložiti tudi dokazilo o opravljenem osnovnem usposabljanju s področja tajnih podatkov. Kadar bo oseba, ki ima dovoljenje za dostop do tajnih podatkov, tudi po preteku njegove veljavnosti potrebovala dostop do tajnih podatkov, bo moral pristojni predlagatelj najmanj tri mesece pred iztekom njegove veljavnosti pristojnemu organu predlagati uvedbo postopka za izdajo novega dovoljenja. Ko ima oseba še veljavno dovoljenje za dostop do tajnih podatkov in gre ponovno v postopek varnostnega preverjanje, dokazila o osnovnem usposabljanju s področja tajnih podatkov ni treba priložiti, saj je predstojnik organa in organizacije dolžan enkrat letno zagotoviti dodatno usposabljanje oseb, ki posedujejo dovoljenje za dostop do tajnih podatkov.

V primeru vmesnega varnostnega preverjanja za potrditev veljavnosti dovoljenja je ravno tako treba priložiti dokazilo o udeležbi na osnovnem usposabljanju s področja varovanja tajnih podatkov, ki ne sme biti starejše od enega leta.

K 6. členu

Predlagana dopolnitev sedanjega 25.b člena omogoča začetek postopka vmesnega varnostnega preverjanja tudi po uradni dolžnosti zaradi zavarovanja javne koristi in omogoča preverjanje katerekoli okoliščine, ki je povezana z varnostnim zadržkom. Omogoča tudi preklic vseh dovoljenj (tudi nižjih stopenj), ki so bila izdana preverjani osebi, česar zdaj veljavne določbe ne omogočajo.

K 7. členu:

Vsebina člena natančno opredeljuje začetek postopka izdaje varnostnega dovoljenja organizaciji, pristojne predlagatelje in listine, ki jih mora vsebovati predlog za začetek postopka varnostnega preverjanja.

Predstojnik ministrstva, pristojnega za gospodarstvo, je pristojni predlagatelj za izdajo varnostnega dovoljenja tistim organizacijam, ki to dovoljenje potrebujejo zaradi sodelovanja na javnih razpisih tuje države ali mednarodne organizacije ali zaradi izvedbe naročila tuje države ali mednarodne organizacije. S to spremembo se odpravlja nejasnost oziroma razlaga, da je predstojnik ministrstva, pristojnega za gospodarstvo, pristojni predlagatelj tudi za organizacije, ki potrebujejo varnostno dovoljenje zaradi sodelovanja na javnih razpisih, ki jih objavljajo slovenski naročniki. V teh primerih je pristojni predlagatelj predstojnik organa iz drugega odstavka 1. člena tega zakona. Dodaja se tudi določilo, da lahko predlog za izdajo varnostnega dovoljenja za organizacijo poda predstojnik nacionalnega varnostnega organa. S tem se smiselno prenaša določilo iz 22.f člena, ki takšno možnost že dopušča pri predlogu za uvedbo varnostnega preverjanja oseb, ki želijo pridobiti dovoljenje za dostop do tajnih podatkov.

Obravnavani člen v drugem odstavku predlagatelja zavezuje, da mora v predlogu opredeliti način obravnavanja tajnih podatkov v okviru izvajanja naročila, ki lahko poteka prostorih naročnika ali v prostorih organizacije. S tem določilom se ureja dosedanja zakonska pomanjkljivost na področju tako imenovane industrijske varnosti, ki je predvidevala izdajanje varnostnih dovoljenj organizacijam zgolj v primerih, ko se tajni podatki organizacijam

posredujejo v fizični obliki oziroma v njihove prostore. S predlagano ureditvijo se tudi zvišuje raven varnostnih standardov na področju industrijske varnosti, ki bodo tako skladni z mednarodnimi varnostnimi standardi in tujo prakso na tem področju. Poleg tega se vgrajuje racionalnost na področju varnostnih dovoljenj, saj organizaciji, ki zaradi narave tajnega naročila tajnih podatkov ne bo obravnavala v lastnih prostorih, fizičnih in tehničnih pogojev za varovanje tajnih podatkov ni treba izpolnjevati. Zaradi preteklih zakonskih določil so namreč mnoge organizacije v izgradnjo oziroma vzpostavitev in varovanje upravnih in varnostnih območij vlagale velika finančna sredstva, čeprav tega za izvajanje konkretnih tajnih naročil dejansko niso potrebovale.

Z določilom, da je treba predlogu za začetek varnostnega preverjanja priložiti pisno soglasje naročnika, če bo organizacija tajne podatke obravnavala v njegovih prostorih, je v zakon vgrajena varovalka, ki preprečuje, da bi organizacije lahko same odločale o tem, ali morajo za izvedbo tajnih naročil vzpostaviti fizične in tehnične pogoje za varovanje tajnih podatkov ali ne, saj je mogoče predvidevati, da bi se organizacije zato, da bi se izognile stroškom, v večini primerov odločale za varnostna dovoljenja, za katera vzpostavitev upravnih oziroma varnostnih območij v lastnih prostorih ni potrebna. Navsezadnje pa je samo naročnik tisti, ki lahko na podlagi vsebine naročila opredeli potreben način obravnavanja tajnih podatkov v okviru le-tega.

Uvaja se institut tako imenovanega »varnostnega dovoljenja za obravnavanje tajnih podatkov pri naročniku«. Čeprav se tovrstna varnostna dovoljenja v RS že izdajajo, saj sledimo direktivi zveze Nato o industrijski varnosti, ki predpisuje, da se organizacijam, ki nimajo vzpostavljenih fizičnih in tehničnih pogojev za obravnavanje in hranjenje tajnih podatkov v lastnih prostorih, izda tovrstno varnostno dovoljenje, v RS ta možnost zakonsko še ni bila urejena. Takšno ureditev imajo v svoji nacionalni zakonodaji tudi primerljive evropske države.

Prav tako je na novo uveden varnostni vprašalnik za organizacije, ki ga bo organizacija morala izpolniti za potrebe izvedbe postopka varnostnega preverjanja (kot je že zdaj urejeno za varnostno preverjanje oseb).

K 8. členu:

Člen natančno določa vsebino varnostnega preverjanja za izdajo varnostnega dovoljenja oziroma pogoje, ki jih mora organizacija izpolnjevati, da omenjeno dovoljenje pridobi.

Največjo novost pomeni podrobnejša ureditev preverjanja lastniške strukture organizacije in tako imenovanih povezanih oseb, to je oseb, ki imajo v lasti določen lastniški ali upravljavski delež organizacije, oziroma drugih oseb, ki nadzirajo ali bi lahko izvajale neposredni ali posredni nadzor nad organizacijo oziroma bi lahko vplivale na njeno dejavnost. Z določili, ki se nanašajo na obveznost pristojnih organov, da preverijo, ali povezane osebe niso sodelovale oziroma ali ne sodelujejo z organizacijami ali skupinami, ki ogrožajo vitalne interese RS ali držav članic političnih, obrambnih in varnostnih zvez, katerih članica je RS, se v zakonodajo vnaša jasnejša podlaga za varnostno preverjanje lastniške strukture organizacije. S preteklo ureditvijo namreč ni bil podrobno opredeljen obseg potrebnega preverjanja tako imenovanega ozadja poslovanja organizacije, ki bi lahko bilo v nasprotju z varnostnimi, političnimi ali gospodarskimi interesi RS.

Za ugotavljanje izpolnjevanja pogojev je pristojen tisti organ, v pristojnosti katerega je tudi izdaja varnostnega dovoljenja organizaciji.

S konkretno navedbo odstotkovne vrednosti lastništva organizacije (če je lastnik organizacije v višini vsaj 25 odstotkov druga družba), ki pomeni nekakšno začetno osnovo za potrebo po varnostnem preverjanju tudi povezanih oseb te lastniške družbe, se vzpostavlja enoten kriterij za vse organe, pristojne za vodenje postopka varnostnega preverjanja organizacij.

V petem odstavku so določeni pogoji, ki jih morajo, poleg pogojev iz drugega odstavka 31.a člena ZTP, izpolnjevati osebe, ki bodo v organizaciji imele dostop do tajnih podatkov stopnje tajnosti INTERNO. Namen določbe je izenačiti pogoje za dostopanje do tajnih podatkov stopnje tajnosti INTERNO za zaposlene v organih in za zaposlene organizacijah.

K 9. členu:

Prvi odstavek natančno določa, da se v primerih, ko organizacija ne izpolnjuje enega ali več pogojev iz 35.b člena ZTP, izdaja varnostnega dovoljenja organizaciji zavrne oziroma se veljavna varnostna dovoljenja organizacije prekličejo. Izdaja varnostnega dovoljenja se organizaciji lahko zavrne ali se veljavna varnostna dovoljenja organizacije lahko prekličejo tudi iz razlogov, ki vzbujajo utemeljen dvom glede ustreznosti obravnavanja in varovanja tajnih podatkov. V praksi se namreč dogaja, da organizacija izpolnjuje predpisane pogoje ob pričetku postopka varnostnega preverjanja, vendar se naknadno izkaže, da se v organizaciji postopki in ukrepi varovanja tajnih podatkov ne izvajajo dosledno. Velikokrat se v organizaciji zamenja odgovorna oseba iz 35.b člena zakona, organizacija preseli sedež poslovanja ali se statusno preoblikuje, zamenja se lastniška struktura, dokumentacija, ki vsebuje tajne podatke, se več ne hrani na način, ki onemogoča dostop do tajnih podatkov osebam, ki nimajo potrebe po seznanitvi z vsebino tajnega podatka…in organizacija o tem ne obvesti organ, pristojen za izdajo varnostnega dovoljenja, in nacionalni varnostni organ.

K 10. členu:

Prvi odstavek pristojni organ zavezuje, da opravi postopek vmesnega varnostnega preverjanja vselej, ko se pri organizaciji, ki ji je bilo izdano varnostno dovoljenje, pojavijo okoliščine, ki vzbujajo sum, da organizacija ne izpolnjuje več pogojev iz 35.b člena tega zakona, oziroma so se v postopku varnostnega preverjanja pojavile druge ugotovitve, ki vzbujajo utemeljene dvome, povezane z varnostjo tajnih podatkov.

Novost je tudi to, da lahko izdajatelj varnostnega dovoljenja v organizaciji ves čas veljavnosti varnostnega dovoljenja preverja izpolnjevanje pogojev za varno obravnavanje tajnih podatkov iz varnostnega dovoljenja.

Velikokrat se v organizaciji zamenja odgovorna oseba iz 35.b člena zakona, organizacija preseli sedež poslovanja ali se statusno preoblikuje, zamenja se lastniška struktura, dokumentacija, ki vsebuje tajne podatke, se več ne hrani na način, ki onemogoča dostop do tajnih podatkov osebam, ki nimajo potrebe po seznanitvi z vsebino tajnega podatka…in organizacija o tem ne obvesti organ, pristojen za izdajo varnostnega dovoljenja, in nacionalni varnostni organ.

V nadaljevanju člen opredeljuje pristojne predlagatelje vmesnega varnostnega preverjanja in jih zavezuje, da do zaključka postopka vmesnega varnostnega preverjanja organizaciji onemogočijo dostop do tajnih podatkov. O tem so dolžni izdati pisni sklep in obvestiti tudi nacionalni varnostni organ, organizacija pa je zavezana, da o izdanem pisnem sklepu obvesti vse naročnike, za katere izvaja tajno naročilo.

Zoper zavrnitveno odločbo v postopku izdaje varnostnega dovoljenja organizacije oziroma zoper preklic obstoječih varnostnih dovoljenj organizacije ni dovoljena pritožba. Pravno varstvo je zagotovljeno v skladu z Zakonom o splošnem upravnem postopku (Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 126/07, 65/08, 8/10, 47/09 – odl. US, 48/09 – popr.).

K 11. členu:

Člen določa prostor, tako imenovano upravno in varnostno območje, kjer se lahko tajni podatki obravnavajo, ter način pošiljanja tajnih podatkov izven omenjenih območij. Do zdaj je to urejala uredba, čeprav gre z vidika fizične varnosti tajnih podatkov za enega od osnovnih pogojev. Omogočen je prožnejši način obravnavanja tajnih podatkov, predvsem v povezavi z varovanjem tajnih podatkov v komunikacijsko-informacijskih sistemih.

Opredeljeni sta tudi točka, kjer se sprejemajo vsa sredstva, ki vsebujejo tajne podatke (mediji), in oseba, pooblaščena za sprejem teh medijev. V tem kontekstu je potrebno določiti delovna mesta, na katerih lahko javni uslužbenci sprejemajo nosilce tajnih podatkov. Osebi se izda poimensko pooblastilo.

Z uvedbo registrskih sistemov Evropske Unije in zveze Nato sledimo Sklepu Sveta o varnostnih predpisih za varovanje tajnih podatkov EU (2013/488/EU) ter direktivi zveze Nato o varovanju tajnih podatkov (AC/35-D/2002-REV4), ki v državah članicah predpisujeta vzpostavitev registrov, odgovornih za sprejem in distribucijo tajnih podatkov EU in zveze NATO. S

predlagano dopolnitvijo se urejajo tudi umeščenost centralnih registrov ter pogoji za vzpostavitev podregistrov in kontrolnih točk, kar do zdaj v RS zakonsko še ni bilo urejeno.

K 12. členu:

Člen obravnava varovanje tajnih podatkov v komunikacijsko-informacijskih sistemih (v nadaljnjem besedilu: sistemi ali KIS). Varovanje mora ustrezati stopnji tajnosti v sistemih obravnavanih oziroma hranjenih tajnih podatkov in stopnji njihove zaščite v smislu zagotavljanja celovitosti, razpoložljivosti in zaupnosti. Celovitost pomeni varovanje točnosti in popolnosti tajnih podatkov ter sistemov s preprečevanjem nepooblaščenih sprememb, razpoložljivost pomeni zagotavljanje, da so informacije in računalniške storitve na voljo pooblaščenim uporabnikom, kadar jih potrebujejo, zaupnost pa pomeni zagotavljanje dostopa do tajnih podatkov in do sistema samo osebam s potrebo po seznanitvi s temi podatki.

Predlog člena določa potrebo po izvedbi postopka varnostne odobritve – vrednotenja sistemov, v katerih se obravnavajo oziroma hranijo tajni podatki. V elektronski obliki se lahko tajni podatki obravnavajo oziroma hranijo le v sistemih, za katere je bilo izdano ustrezno varnostno dovoljenje za delovanje. V varnostnem dovoljenju za delovanje se določi najvišja stopnja tajnosti podatkov, ki se lahko obravnavajo oziroma hranijo v posameznem sistemu.

Varnostno dovoljenje za delovanje sistema, v katerem se obravnavajo oziroma hranijo tajni podatki, izda nacionalni varnostni organ.

Varovanje tajnih podatkov v sistemih temelji na postopku obvladovanja tveganja. To je postopek, na podlagi katerega sistematično ugotovimo sestavine sistema, jih opredelimo glede na stopnjo tajnosti v njih obravnavanih in hranjenih tajnih podatkov, opravimo pregled groženj, ki so jim podvrženi, ter ocenimo tveganja, ki nastanejo. Ta ocena je temelj za kasnejše ukrepanje, saj nam pove, kje so največje varnostne vrzeli v sistemu. Na podlagi te ocene se tudi odloči, katera tveganja so sprejemljiva. Pri sprejemanju tveganj je potrebno zagotoviti, da se sprejmejo preostala tveganja, to je tista tveganja, ki niso bila predmet obravnave tveganj ali pa se je pri obravnavi tveganj odločilo, da se jih v danem trenutku sprejme takšna kot so.

Vse sestavine sistemov, v okviru katerih se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje, morajo biti zaščitene proti neželenemu elektromagnetnemu sevanju (TEMPEST). Le-to se pojavlja v obliki elektromagnetnega valovanja, ki ga oddajajo komunikacijsko-informacijske naprave med obratovanjem. Ti moteči signali omogočajo nenadzorovano odtekanje tajnih podatkov iz sistema, zato je treba vse elemente sistemov, v okviru katerih se obravnavajo podatki stopnje tajnosti ZAUPNO, TAJNO in STROGO TAJNO, zaščititi proti temu neželenemu elektromagnetnemu sevanju.

Prenos tajnih podatkov v sistemih izven upravnih in varnostnih območij je dovoljen le z uporabo kriptografskih rešitev, ki jih odobri nacionalni varnostni organ. S tem je določen popoln nadzor nad kriptografskimi rešitvami, ki se uporabljajo za varovanje tajnih podatkov. Kriptografske rešitve vključujejo strojno oziroma programsko opremo ter s tem povezane sestavne dele, ki so vgrajeni v komunikacijsko informacijski sistem, ter so kritična točka pri varovanju tajnih podatkov. S tem se zagotavlja zaupnost in celovitost tajnih podatkov pri prenosu med različnimi deli sistema oziroma med sistemi. Pomembno je, da so odobrene kriptografske rešitve pod nadzorom nacionalnega varnostnega organa.

Nacionalni varnostni organ preverja ustreznosti kriptografskih rešitev za varovanje tajnih podatkov v okviru postopka ugotavljanja ustreznosti kriptografskega materiala, s katerim se ugotovi varnostna ustreznost kriptografske rešitve. Postopki ugotavljanja ustreznosti kriptografskih rešitev se izvajajo le na podlagi pisnih predlogov, ki jih podajo ministrstvo, pristojno za javno upravo, ministrstvo, pristojno za notranje zadeve, ministrstvo, pristojno za obrambo, ministrstvo, pristojno za zunanje zadeve, Slovenska obveščevalno-varnostna agencija ali nacionalni varnostni organ. Postopek in vsebino dokumentacije, ki jo mora vsebovati predlog, določi vlada.

Člen nadalje določa, da za zgoraj navedene organe kriptografske rešitve lahko razvija in izdeluje le organizacija, ki ima veljavno varnostno dovoljenje ustrezne stopnje tajnosti za varovanje tajnih podatkov na sedežu organizacije, veljavno še najmanj eno leto od vložitve vloge.

Zaradi pomembnosti kriptografskih rešitev za nacionalno varnost in strokovne zahtevnosti lahko postopek ugotavljanja ustreznosti kriptografskih rešitev traja eno leto od prejema popolne vloge. Ta rok se lahko izjemoma, zaradi tehnične zahtevnosti kriptografske rešitve, podaljša še za eno leto.

Nadalje je v členu opredeljena tudi možnost, da se v izrednem ali vojnem stanju tajni podatki v elektronski obliki stopnje tajnosti INTERNO, ZAUPNO in TAJNO prenašajo v sistemih odobrenih za nižjo stopnjo tajnosti ali v nekriptirani obliki.

Člen opredeljuje tudi pogoje, ki omogočajo delo s tajnimi podatki na terenu, kar se je izkazalo za neizogibno predvsem v slovenski vojski in policiji. Gre za obravnavanje in ne hranjenje tajnih podatkov. Slednje je namreč dovoljeno le v upravnem oziroma varnostnem območju. Z ustrezno opremo, ki ima potrdilo za tovrstno uporabo, in z dodatnimi varnostnimi ukrepi, uporabnik lahko ustvari pogoje enakovredne upravnemu oziroma varnostnemu območju brez formalne razglasitve upravnega oziroma varnostnega območja in na terenu dobi na primer vpogled v tajne podatke.

S tem členom se določa tudi, da nacionalni varnostni organ opravlja naloge organov s področja varovanja tajnih podatkov v sistemih. Enak oziroma podoben koncept postavitve in umestitve navedenih organov uporabljata zveza Nato in EU ter tudi večina držav članic obeh asociacij. UVTP kot krovni nacionalni varnostni organ že zdaj v skladu s sklepom Vlade RS št. 38600-3/2009/21 z dne 8. 4. 2010 opravlja koordinacijo varnostnih organov (MO, MNZ – Policija in SOVA), ki na podlagi obstoječih normativnih aktov opravljajo naloge s področja informacijske varnosti. S predlagano ureditvijo bo UVTP postal krovno koordinacijsko telo, konkretne naloge pa se bodo še naprej opravljale v okviru posameznih organov. Navedeni sklep je UVTP pripravil v sodelovanju s Komisijo za informacijsko varnost, ministrstvom, pristojnim za obrambo, ministrstvom, pristojnim za notranje zadeve, ministrstvom, pristojnim za zunanje zadeve, ministrstvom, pristojnim za javno upravo, in Slovensko obveščevalno-varnostno agencijo, ob upoštevanju mnenja Sekretariata Sveta za nacionalno varnost.

K 13. členu:

Popravek drugega odstavka trenutno veljavnega 43. člena ZTP je potreben iz razloga, da bo najkasneje do 1. 1. 2019 naloge UVTP v celoti prevzel na novo ustanovljeni organ, in sicer tako imenovani pristojni nacionalni organ za varnost omrežij in informacijskih sistemov, ki bo ustanovljen v skladu s predlogom Zakona o informacijski varnosti.

K 14. členu:

Člen določa temeljne naloge nacionalnega varnostnega organa na področju obravnavanja in varovanja nacionalnih tajnih podatkov v tujini in tujih tajnih podatkov v RS.

V tem členu so hkrati podrobneje navedene pristojnosti UVTP pri izvrševanju mednarodnih pogodb in sprejetih mednarodnih obveznosti v okviru sodelovanja z ustreznimi organi tujih držav in mednarodnih organizacij. Pri tem so jasneje opredeljene nekatere njegove funkcije in pristojnosti, ki mu zagotavljajo izvajanje njegovih obveznosti do pristojnih varnostnih organov tujih držav in mednarodnih organizacij. V ta sklop spada tudi pooblastilo, da lahko od pristojnega inšpektorata zahteva izvedbo inšpekcijskega nadzora pri določenem organu ali organizaciji.
UVTP pri izvrševanju mednarodnih pogodb in sprejetih mednarodnih obveznosti v okviru sodelovanja z ustreznimi organi tujih držav in mednarodnih organizacij opravlja tudi naloge organa, pristojnega za šifrirno zaščito podatkov, organa za razdeljevanje šifrirnega materiala in organa za zaščito pred neželenim elektromagnetnim sevanjem naprav v KIS, v katerih se obravnavajo tuji tajni podatki. S tem se zagotavlja celovitost področja obravnavanja tujih tajnih podatkov v KIS.

Nadalje je s tem členom določena pristojnost UVTP za izdajo in preklic pooblastila fizični osebi za dostop do tujih tajnih podatkov, varnostnega dovoljenja organizaciji za dostop do tujih tajnih podatkov in varnostnega dovoljenja za sisteme in naprave za prenos, hranjenje in obdelavo tujih tajnih podatkov v skladu s sprejetimi mednarodnimi pogodbami. Z izdanim pooblastilom za dostop do tujih tajnih podatkov se fizični osebi dovoli dostop do tajnih podatkov zveze Nato oziroma EU, seveda v skladu s potrebo po seznanitvi s tujim tajnim podatkom. UVTP izda varnostno dovoljenje organizaciji za dostop do tujih tajnih podatkov.

K 15. členu:

Člen ureja dostop do tujih tajnih podatkov stopnje tajnosti INTERNO, in sicer tako za osebe, zaposlene v organu, kot tudi za osebe, zaposlene v organizaciji, ter daje pravno podlago za hranjenje pooblastila za dostop do tujih tajnih podatkov ali podpisane izjave v kadrovski evidenci osebe.

Pogoj za pridobitev pooblastila za dostop do tujih tajnih podatkov je, da ima oseba veljavno nacionalno dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti in da opravlja funkcijo ali izvaja naloge na delovnem mestu, na katerem je določeno, da se dostopa do tajnih podatkov tuje države ali mednarodne organizacije. Funkcija ali zasedba določenega delovnega mesta, na katerem se dostopa do tujih tajnih podatkov, je osnova za izpolnitev pogoja potrebe po seznanitvi s tajnim podatkom (*need to know*), ki je opredeljen v varnostni politiki EU in Nata. Če oseba nima potrebe po seznanitvi ali se ji prekliče nacionalno dovoljenje za dostop do tajnih podatkov, je treba pooblastilo za dostop do tujih tajnih podatkov preklicati. Slednje je mogoče le na podlagi pisnega obvestila (obrazložitve) predstojnika organa ali organizacije, da je pri tej osebi na konkretnem delovnem mestu prenehala potreba po seznanitvi s tujimi tajnimi podatki oziroma je bilo osebi preklicano nacionalno dovoljenje.

Obrazložitev velja tudi za izdajo in preklic varnostnega dovoljenja organizaciji za dostop do tujih tajnih podatkov in izdajo ter preklic varnostnega dovoljenja za sisteme in naprave za prenos, hranjenje in obdelavo tujih tajnih podatkov v skladu s sprejetimi mednarodnimi pogodbami (druga in tretja alineja tretjega odstavka 43.b člena tega zakona).
Tretji odstavek opredeljuje vsebino predloga za izdajo pooblastila za dostop do tujih tajnih podatkov. Predlog mora med drugim vsebovati ime in priimek (osebno ime) ter rojstne podatke preverjane osebe, da jo je mogoče individualno ločiti od drugih oseb. V posameznih organih se pojavijo primeri, ko ima več oseb, ki potrebujejo pooblastilo za dostop do tujih tajnih podatkov, enako ime in priimek. Ker je rojstni datum osebni podatek, ga je treba predpisati z zakonom, in ne s podzakonskim aktom (uredbo), kot je bilo to urejeno do zdaj.

K 16. členu:

UVTP je pristojen tudi za vodenje evidenc na področju tajnih podatkov. Drugi predpisi in praktične izkušnje so pokazali na potrebo po vodenju še dodatnih evidenc, in sicer:

- evidence zavrnjenih predlogov za izdajo dovoljenj,
- evidence zavrnjenih predlogov za izdajo varnostnih dovoljenj,
- evidence o opravljenih posebnih delih strokovnega izpita za inšpektorja,
- evidence izdanih potrdil o udeležbi na osnovnem usposabljanju s področja varovanja tajnih podatkov,
- evidence upravnih in varnostnih območij v organih in organizacijah,
- evidence registrov, podregistrov in kontrolnih točk tujih tajnih podatkov,
- evidence varnostno odobrenih KIS,
- evidence odobrenih šifrirnih rešitev in
- evidenco kriptografskega materiala.

Na podlagi vodenja dodatnih evidenc bo UVTP imel pregled nad celotnim delovnim področjem, ki je v njegovi pristojnosti.

V tem členu je torej določeno, katere evidence vodi UVTP. Določeni sta tudi njihova vsebina in dolžnost organov ter organizacij z vidika posredovanja podatkov UVTP za njegove evidence.
Hkrati se na novo določa, da mora evidenco izdanih potrdil o udeležbi na osnovnem usposabljanju s področja varovanja tajnih podatkov voditi tudi vsak organ in vsaka organizacija, ki izvaja omenjeno usposabljanje.

Za dostop do podatkov iz prvega odstavka 43.e člena ZTP-ja, ki vsebujejo osebne podatke oseb, obstajajo zadržki iz prvega odstavka 6. člena ZDIJZ, saj gre za informacije, ki niso javno dostopne. Izjema so zgolj tri evidence, in sicer evidenca odobrenih šifrirnih rešitev in evidenca varnostnih dovoljenj iz 35. člena ZTP ter evidenca varnostnih dovoljenj iz druge alineje tretjega odstavka 43.b člena ZTP – zadnji navedeni sta v noveli združeni v eno evidenco. To velja tudi v primeru, ko so podatki in gradivo iz tega odstavka odstopljeni drugemu organu. S tem se zavarujejo predvsem tista delovna mesta, katerih tajnost delovanja je pogoj za učinkovito izvedbo nalog. Če bi bili navedeni podatki informacija javnega značaja, bi bila s tem lahko ogrožena varnost javnih uslužbencev in njihovih bližnjih. Ustvarjanje in vodenje podatkov o javnih uslužbencih zunaj organa njihove zaposlitve bi lahko ogrozilo varnost in izvajanje nalog organa, razkritje javnih uslužbencev pa bi povzročilo motnje pri delovanju oziroma dejavnosti organa. Sporna je zlasti kombinacija podatkov, ki bi jih lahko kdo pridobil iz evidenc (na primer osebno ime, datum in kraj rojstva, organ, kjer je oseba zaposlena). Problematične so tudi kombinacije podatkov, ki jih lahko kdo zahteva in na ta način pridobi sezname javnih uslužbencev, zaposlenih pri posameznem organu.

K 17. do 19. členu:

S spremembami navedenih členov se nomotehnično uskladijo zneski denarnih glob (pretvorba iz tolarjev v evre), pri čemer se zneski pri pretvorbi valut zaokrožijo.

V novi 27. točki 16. člena je predpisana globa v primeru nezagotavljanja varovanja tajnih podatkov, obravnavanih v posameznem KIS.

Popravka v 26. in 29. točki 16. člena sta zgolj redakcijske narave.

Predlagana dopolnitev z 31. točko se nanaša na dopolnitev 43.e člena in dolžnost sporočanja podatkov UVTP s strani organov.

Predlagana sprememba se nanaša na dopolnitev 35.d člena in je potrebna zaradi učinkovitega izvajanja preverjanja izpolnjevanja pogojev za varno obravnavanje tajnih podatkov iz varnostnega dovoljenja.

K 20. členu:

V prehodni določbi zakon zavezuje Vlado RS, da najkasneje v šestih mesecih po uveljavitvi tega zakona izda predpis oziroma ustrezno spremeni in dopolni že obstoječi predpis, s katerim predpiše način in postopek ugotavljanja izpolnjevanja pogojev za izdajo varnostnega dovoljenja organizaciji (sedmi odstavek 35.b člena), predpis, s katerim predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov v fizični obliki na splošno (osmi odstavek 39. člena), ter predpis, s katerim predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov v KIS (prvi odstavek 39.a člena).

Če bo organizacija, ki poseduje varnostno dovoljenje, tudi po preteku njegove veljavnosti ali po preteku dobe, določene v pogodbi o naročilu (nova pogodba, novo naročilo), potrebovala dostop do tajnih podatkov, se jo preveri v skladu z določbami tega zakona.

K 21. členu:

Glede na dejstvo, da bo pristojni nacionalni organ za varnost omrežij in informacijskih sistemov ustanovljen najkasneje do 1.1. 2019, kar bo določal predlog Zakona o informacijski varnosti, UVTP do tega trenutka nadaljuje s svojim delom po ustaljenih postopkih.

K 22. členu:

S tem členom je določen datum uveljavitve zakona.

III. BESEDILO ČLENOV, KI SE SPREMINJAJO IN DOPOLNJUJEJO

ZAKON O TAJNIH PODATKIH

2. člen

Posamezni izrazi, uporabljeni v tem zakonu, imajo naslednji pomen:
1. tajni podatek je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno;
2. tajni podatek tuje države je podatek, ki ga je Republiki Sloveniji oziroma njenim organom posredovala tuja država oziroma njen organ ali mednarodna organizacija oziroma njen organ v pričakovanju, da bo ostal tajen, ter podatek, ki je rezultat sodelovanja Republike Slovenije oziroma njenih organov s tujo državo ali mednarodno organizacijo oziroma njihovimi organi, in za katerega se dogovori, da mora ostati tajen;
3. dokument je vsak napisan, narisan, natisnjen, razmnožen, posnet, fotografiran, magneten, optičen ali kakšen drugačen zapis tajnega podatka;
4. medij je vsako sredstvo, ki vsebuje tajne podatke;
5. določanje tajnih podatkov je dejanje ali postopek, s katerim se podatek v skladu s tem zakonom oceni za tajnega in se mu določi stopnja in rok tajnosti;
6. prenehanje tajnosti podatka je zakonita sprememba tajnega podatka v podatek, ki je dostopen v skladu s splošnimi predpisi, ki urejajo poslovanje organa;
7. dostop je seznanitev osebe s tajnim podatkom ali možnost osebe pridobiti tajni podatek na podlagi dovoljenja za dostop do tajnih podatkov;
8. varnostno preverjanje osebe je poizvedba, ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi pristojni organ, in katere namen je zbrati podatke o morebitnih varnostnih zadržkih;
9. varnostni zadržki so ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo dvomi o zanesljivosti in lojalnosti osebe, ki naj bi dobila dovoljenje za dostop do tajnih podatkov;
10. ogrožanje vitalnih interesov države je ogrožanje njene ustavne ureditve, neodvisnosti, ozemeljske celovitosti in obrambne sposobnosti;
11. obravnavanje tajnih podatkov je določanje, označevanje, dostop do, uporaba, evidentiranje, razmnoževanje, posredovanje, prenos, uničevanje nosilcev tajnih podatkov, hramba, arhiviranje ter drugi ukrepi in postopki, s katerimi se zagotavlja njihova varnost.

3. člen

V zvezi z opravljanjem svoje funkcije lahko do tajnih podatkov brez dovoljenja za dostop do tajnih podatkov (v nadaljnjem besedilu: dovoljenje) dostopa:
– predsednik republike;
– predsednik vlade;
– poslanec;
– državni svetnik;
– župan in občinski svetnik;
– minister in predstojnik vladne službe, ki je neposredno odgovoren predsedniku vlade;
– varuh človekovih pravic in njegov namestnik;
– guverner, namestnik in vice guverner centralne banke;
– član računskega sodišča;
– sodnik;
– predsednik in člani Državne revizijske komisije;
– državni tožilec;
– generalni državni pravobranilec in
– informacijski pooblaščenec.

Osebe iz prejšnjega odstavka dobijo dovoljenje z začetkom funkcije oziroma opravljanja dela in podpisom izjave, da so seznanjene s tem zakonom in drugimi predpisi, ki urejajo varovanje tajnih podatkov, in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi.

17. člen

Vsak tajni podatek oziroma vsak dokument, ki vsebuje tajne podatke, mora biti označen s stopnjo tajnosti in s podatki o organu, če to že sicer ni razvidno.

Oznake iz prejšnjega odstavka se uporabijo na način, ki ustreza vrsti in lastnostim medija.

Podatek oziroma dokument se mora obravnavati kot tajen, tudi če je označen le s stopnjo tajnosti.

Vlada Republike Slovenije (v nadaljnjem besedilu: vlada) podrobneje predpiše načine in oblike označevanja tajnosti podatkov oziroma dokumentov.

22.g člen

Postopek za izdajo dovoljenja se začne na pisni predlog predlagatelja za osebo, ki jo je treba varnostno preveriti (v nadaljnjem besedilu: preverjana oseba), in mora vsebovati podatke o stopnji tajnosti tajnih podatkov, za dostop do katerih je dan predlog za izdajo dovoljenja.

Predlagatelj mora predlogu priložiti pisno soglasje preverjane osebe za varnostno preverjanje, dokazilo o opravljenem usposabljanju s področja obravnavanja tajnih podatkov, pisno izjavo o seznanitvi s tem zakonom in predpisi, izdanimi na njegovi podlagi, ter zaprto ovojnico z izpolnjenim varnostnim vprašalnikom preverjane osebe.

25.b člen

Če je pri osebi, ki ima dovoljenje za dostop do tajnih podatkov, podan sum obstoja varnostnega zadržka iz 27. člena tega zakona, se opravi vmesno varnostno preverjanje.

Vmesno varnostno preverjanje se opravi na predlog predstojnika organa ali organizacije, v kateri oseba opravlja funkcijo ali izvaja naloge, ob smiselni uporabi določb 22.a člena tega zakona.

Nacionalni varnostni organ lahko da pristojnemu organu predlog za vmesno varnostno preverjanje osebe, če pri nadzoru iz šeste alinee tretjega odstavka 43.b člena tega zakona ugotovi sum varnostnega zadržka iz 27. člena tega zakona. O tem mora obvestiti predstojnika organa ali organizacije, kjer je oseba, za katero predlaga vmesno varnostno preverjanje, zaposlena.

35.a člen

Postopek izdaje varnostnega dovoljenja iz prejšnjega člena tega zakona se začne na podlagi pisnega predloga predstojnika:
1. organa iz drugega odstavka 1. člena tega zakona za organizacije, ki izvajajo naročila tega organa;
2. ministrstva, pristojnega za gospodarstvo, za organizacije, ki potrebujejo varnostno dovoljenje zaradi sodelovanja na javnih razpisih ali izvedbe naročila tuje države ali mednarodne organizacije.

Predlagatelj iz 2. točke prejšnjega odstavka lahko pred vložitvijo predloga pridobi mnenje ministrstva, pristojnega za delovno področje, na katerem deluje organizacija.

Predlagatelj mora predlogu za začetek postopka varnostnega preverjanja priložiti naslednje listine, s katerimi predlagana organizacija dokazuje izpolnjevanje pogojev za priznanje sposobnosti za varno obravnavanje tajnih podatkov:

1. da je registrirana pri pristojnem sodišču ali drugem organu – izpisek iz sodne ali druge ustrezne evidence;
2. da ni v kazenskem postopku zaradi suma storitve kaznivega dejanja v zvezi s podkupovanjem ali da zaradi takega kaznivega dejanja ni bila pravnomočno obsojena – potrdilo ministrstva, pristojnega za pravosodje, da organizacija ni vpisana v kazensko evidenco;
3. da ni zoper njo uveden ali začet postopek prisilne poravnave, stečajni ali likvidacijski postopek, drug postopek, katerega posledica ali namen je prenehanje poslovanja organizacije – izpisek iz sodne ali druge enakovredne evidence;
4. da je poravnala davke in prispevke v skladu s predpisi države, kjer ima svoj sedež, ali da je organizacija, ki ima sedež v tujini, poravnala v Republiki Sloveniji tiste dajatve, ki bi jih morala poravnati – potrdilo, ki ga izda davčni ali drug pristojni organ države, kjer ima organizacija svoj sedež;
5. da ni bila kaznovana za dejanje v zvezi s poslovanjem oziroma so posledice sodbe že izbrisane – potrdilo ministrstva, pristojnega za pravosodje, da organizacija ni vpisana v kazensko evidenco;
6. dokazilo o lastniški strukturi organizacije – izpisek iz sodne ali druge ustrezne evidence.

Pristojni organ iz drugega odstavka prejšnjega člena lahko v postopku izdaje varnostnega dovoljenja, z namenom preveritve podatkov iz prejšnjega odstavka in izpolnjevanja pogojev iz prvega odstavka 35.b člena tega zakona, zbira podatke od organizacije, na katero se podatki nanašajo, ali pri drugih organih, organizacijah ali osebah, ki o teh podatkih kaj vedo.

35.b člen

Pristojni organ izda organizaciji varnostno dovoljenje, če:
1. organizacija izpolnjuje fizične, organizacijske in tehnične pogoje za varovanje tajnih podatkov v skladu s tem zakonom in predpisi, sprejetimi na njegovi podlagi;
2. so osebe, ki bodo v organizaciji po službeni dolžnosti imele dostop do tajnih podatkov, varnostno preverjene in imajo dovoljenje za dostop do tajnih podatkov;
3. organizacija zagotovi, da bo dostop do tajnih podatkov dovoljen samo tistim osebam, ki morajo imeti vpogled v te podatke po svoji službeni dolžnosti zaradi uresničevanja naročila organa;
4. imenuje osebo, pristojno za nadzor in usmerjanje varnostnih ukrepov v zvezi z izvajanjem naročila, usposabljanje oseb, ki imajo dostop do tajnih podatkov, poročanje pristojnemu organu o okoliščinah, ki vplivajo na izdajo varnostnega dovoljenja in izvajanje drugih predpisanih ukrepov za varno obravnavanje tajnih podatkov.
Oseba, ki bo v organizaciji po službeni dolžnosti imela dostop do tajnih podatkov stopnje tajnosti INTERNO, mora poleg pogojev iz drugega odstavka 31.a člena tega zakona izpolnjevati še naslednje pogoje:
– da ni bila pravnomočno obsojena zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti, in da ni bila obsojena na nepogojno kazen zapora v trajanju več kot šest mesecev;
– da ni v kazenskem postopku zaradi kaznivega dejanja iz prejšnje alinee.

Pogoje iz prejšnjega odstavka ugotavlja organ, pristojen za izdajo varnostnega dovoljenja organizaciji, v kateri bo oseba dostopala do tajnih podatkov.

Vlada podrobneje predpiše način in postopek ugotavljanja izpolnjevanja pogojev za izdajo varnostnega dovoljenja.

35.c člen

Pristojni organ lahko organizaciji zavrne izdajo varnostnega dovoljenja, če ne izpolnjuje pogojev za priznanje sposobnosti iz tretjega odstavka 35.a člena tega zakona.

Organizaciji, ki ne izpolnjuje pogojev iz prvega odstavka prejšnjega člena, pristojni organ varnostnega dovoljenja ne izda.

35.d člen

Če po izdaji varnostnega dovoljenja nastopijo okoliščine, ki kažejo na to, da organizacija ne izpolnjuje več pogojev za priznanje sposobnosti iz tretjega odstavka 35.a člena ali pogojev iz prvega odstavka 35.b člena tega zakona, opravi pristojni organ iz drugega odstavka 35. člena tega zakona postopek vmesnega varnostnega preverjanja.

Vmesno varnostno preverjanje se opravi na predlog pristojnega predlagatelja iz 35.a ali 43.b člena tega zakona.

Nacionalni varnostni organ lahko da predlog za vmesno varnostno preverjanje, če pri nadzoru iz šeste alinee tretjega odstavka 43.b člena tega zakona ugotovi okoliščine, ki kažejo na to, da organizacija več ne izpolnjuje pogojev za izdajo varnostnega dovoljenja.

Postopek vmesnega varnostnega preverjanja je enak postopku varnostnega preverjanja za izdajo varnostnega dovoljenja. Če pri vmesnem varnostnem preverjanju pristojni organ ugotovi, da organizacija ne izpolnjuje več pogojev, ki jih ta zakon določa za izdajo varnostnega dovoljenja, ji varnostno dovoljenje prekliče. O preklicu varnostnega dovoljenja obvesti tudi nacionalni varnostni organ.

Zoper zavrnitev izdaje varnostnega dovoljenja in njegov preklic je dovoljen upravni spor.

39. člen

Tajne podatke se mora v organih hraniti na način, ki zagotavlja, da imajo dostop do teh podatkov samo osebe, ki imajo dovoljenje za dostop do tajnih podatkov, in ki podatke potrebujejo za izvajanje svojih delovnih nalog ali funkcij.

Tajni podatki se lahko pošljejo izven prostorov organa samo ob upoštevanju predpisanih varnostnih ukrepov in postopkov, ki morajo zagotoviti, da jih prejme oseba, ki ima dovoljenje za dostop do tajnih podatkov in je do teh podatkov upravičena.

Postopki in ukrepi varovanja pošiljanja tajnih podatkov izven prostorov organa se predpišejo glede na stopnjo tajnosti teh podatkov.

Organi tajnih podatkov ne smejo prenašati ali posredovati po nezaščitenih komunikacijskih sredstvih.

Vlada podrobneje predpiše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje tajnih podatkov.

43. člen

Izvajanje tega zakona in drugih predpisov, sprejetih na njegovi podlagi ter mednarodnih pogodb, ki jih je sklenila Republika Slovenija, spremlja in usklajuje nacionalni varnostni organ, razen, če mednarodna pogodba ne določa drugače.

Naloge nacionalnega varnostnega organa opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

43.b člen

Nacionalni varnostni organ skrbi za izvrševanje mednarodnih pogodb in sprejetih mednarodnih obveznosti, ki jih je v zvezi z obravnavanjem in varovanjem tajnih podatkov sklenila ali sprejela

Republika Slovenija, ter na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij, razen če mednarodna pogodba določa drugače.

Nacionalni varnostni organ usklajuje dejavnosti za zagotavljanje varnosti nacionalnih tajnih podatkov v tujini in tujih tajnih podatkov na območju Republike Slovenije.

V zvezi z izvrševanjem mednarodnih pogodb in sprejetih mednarodnih obveznosti nacionalni varnostni organ opravlja zlasti naslednje naloge:
– izdaja in preklicuje dovoljenja fizičnim osebam za dostop do tujih tajnih podatkov;
– izdaja in preklicuje varnostna dovoljenja organizacijam za dostop do tujih tajnih podatkov;
– izdaja in preklicuje varnostna dovoljenja za sisteme in naprave za prenos, hranjenje in obdelavo tujih tajnih podatkov v skladu s sprejetimi mednarodnimi pogodbami;
– potrjuje izpolnjevanje predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa ali organizacije tujim državam in mednarodnim organizacijam;
– izdaja navodila za ravnanje s tajnimi podatki tuje države ali mednarodne organizacije;
– nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države ali mednarodne organizacije in skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki so jih organi dolžni nemudoma izvršiti;
– od pristojnega inšpektorata zahteva izvedbo inšpekcijskega nadzora pri določenem organu ali organizaciji;
– izmenjuje podatke z nacionalnimi varnostnimi organi tujih držav in z mednarodnimi organizacijami.

Pred izdajo dovoljenja iz prve in druge alinee prejšnjega odstavka lahko, kadar prejme obvestilo tujega varnostnega organa o varnostnem zadržku, od organa, pristojnega za varnostno preverjanje, zahteva vmesno varnostno preverjanje osebe ali organizacije.

43.c člen

Nacionalni varnostni organ izda dovoljenje iz prve alinee tretjega odstavka prejšnjega člena na predlog predlagateljev iz 22.f člena tega zakona, če ima oseba veljavno dovoljenje iz 22. člena tega zakona in opravlja funkcijo ali izvaja naloge na delovnem mestu, na katerem potrebuje dovoljenje za dostop do tujih tajnih podatkov. Dovoljenje se izda z veljavnostjo za čas, ko oseba potrebuje dostop do tujih tajnih podatkov, vendar ne dlje, kot velja dovoljenje iz 22. člena tega zakona.

Če oseba, ki ji je bilo izdano dovoljenje za dostop do tujih tajnih podatkov, ne izvaja več nalog, pri katerih potrebuje dostop do tujih tajnih podatkov, je predstojnik organa ali organizacije dolžan o tem takoj obvestiti nacionalni varnostni organ.

Nacionalni varnostni organ dovoljenje za dostop do tujih tajnih podatkov prekliče, ko prenehajo pogoji za njegovo izdajo iz prvega odstavka tega člena.

43.e člen

Za namene izvrševanja pristojnosti in nalog po tem zakonu, drugih zakonih in obvezujočih mednarodnih pogodbah vodi in obdeluje nacionalni varnostni organ naslednje evidence:

1. evidenco dovoljenj, izdanih na podlagi 22. člena tega zakona, ki vsebuje naslednje podatke:
– osebno ime;
– datum in kraj rojstva;
– organ, kjer je oseba zaposlena;
– organ, ki je izdal dovoljenje;
– stopnja tajnosti podatkov, do katerih ima oseba dostop;
– številka in datum izdaje ter datum veljavnosti dovoljenja;
– datum, razlog in organ, ki je opravil preklic dovoljenja;
– datum, razlog in organ, ki je zavrnil izdajo dovoljenja;
– datum in organ, ki je izdal sklep iz 25.c člena tega zakona;

2. evidenco izdanih dovoljenj fizičnim osebam za dostop do tujih tajnih podatkov iz prve alinee tretjega odstavka 43.b člena tega zakona, ki vsebuje naslednje podatke:
– osebno ime;
– datum in kraj rojstva;
– organ, kjer je oseba zaposlena;
– stopnja tajnosti podatkov, do katerih ima oseba dostop;
– številka in datum izdaje ter datum veljavnosti dovoljenja;
– številka in datum izdaje dovoljenja za dostop do tujih tajnih podatkov ter datum njegove veljavnosti;
3. evidenco varnostnih dovoljenj iz 35. člena tega zakona, ki vsebuje naslednje podatke:
– naziv in naslov organizacije;
– organ, ki je izdal varnostno dovoljenje;
– številka in datum izdaje ter datum veljavnosti varnostnega dovoljenja;
– datum, razlog in organ, ki je opravil preklic varnostnega dovoljenja;
– datum, razlog in organ, ki je zavrnil izdajo varnostnega dovoljenja;
– osebno ime, datum in kraj rojstva ter položaj osebe iz 4. točke prvega odstavka 35.b člena tega zakona;
– številka dovoljenja in stopnja tajnosti podatkov, do katerih ima oseba iz prejšnje alinee pravico dostopa;
4. evidenco varnostnih dovoljenj iz druge alinee tretjega ostavka 43.b člena tega zakona, ki vsebuje naslednje podatke:
– naziv in naslov organizacije;
– organ, ki je izdal varnostno dovoljenje;
– datum, razlog in organ, ki je opravil preklic varnostnega dovoljenja organizaciji za dostop do tujih tajnih podatkov;
– datum, razlog in organ, ki je zavrnil izdajo varnostnega dovoljenja organizaciji za dostop do tujih tajnih podatkov;
– osebno ime, datum in kraj rojstva ter položaj osebe iz 4. točke prvega odstavka 35.b člena tega zakona;
– številka dovoljenja in stopnja tajnosti podatkov, do katerih ima oseba iz prejšnje alinee pravico dostopa;
5. evidenco začasnih dostopov do tajnih podatkov na podlagi drugega odstavka 30. člena tega zakona, ki vsebuje naslednje podatke:
– osebno ime;
– datum in kraj rojstva;
– organ, kjer je oseba zaposlena;
– stopnja tajnosti podatkov, do katerih ima oseba dostop;
– številka in datum veljavnosti dovoljenja;
– stopnja tajnosti podatkov, do katerih ima oseba začasen dostop;
– obdobje (trajanje) začasnega dostopa.

Evidence iz tega člena se hranijo trajno.

44. člen

Z globo od 1.000.000 do 3.000.000 tolarjev se kaznuje za prekršek pravna oseba ali samostojni podjetnik posameznik:
1. če dovoli dostop do tajnih podatkov osebi, ki ni podpisala izjave (drugi odstavek 3. člena, drugi odstavek 31.a člena);
2. če prenese pooblastilo za določanje tajnosti podatku na tretjo osebo (tretji odstavek 10. člena);
3. če pri določanju stopnje tajnosti podatku ne oceni možnih škodljivih posledic za varnost države ali za njene politične ali gospodarske koristi, če bi bil podatek razkrit nepoklicani osebi (11. člen);
4. če ravna v nasprotju z 12. členom tega zakona;
5. če ravna v nasprotju s 14. členom tega zakona;
6. če spremeni stopnjo tajnosti podatku v nasprotju s 16. členom tega zakona;
7. če tajnega podatka oziroma dokumenta ne označi s predpisanimi oznakami (17. člen);
8. če prenehanja tajnosti podatku oziroma dokumentu ne določi skladno z 18. členom tega zakona;

9. če v nasprotju z 18. členom tega zakona brez utemeljenih razlogov spremeni način, ki je določen za prenehanje tajnosti;
10. če o izdaji ali preklicu dovoljenja za dostop osebe do tajnih podatkov ne obvesti nacionalnega varnostnega organa (22. člen, drugi odstavek 26. člena);
11. če ne predlaga vmesnega varnostnega preverjanja osebe (drugi in tretji odstavek 25.b člena, drugi odstavek 25.c člena);
12. če začasno ne onemogoči dostopa do tajnih podatkov osebi, za katero postopek vmesnega varnostnega preverjanja še ni zaključen (četrti odstavek 25.c člena);
13. če ne hrani dovoljenja in izjave v kadrovski evidenci (28. člen);
14. če ne vodi evidence dovoljenj za dostop do tajnih podatkov (29. člen);
15. če dovoli dostop do tajnih podatkov v nasprotju s prvim odstavkom 31. člena tega zakona;
16. če osebo razreši dolžnosti varovanja tajnosti podatkov v nasprotju s 33. členom;
17. če dovoli posredovanje tajnih podatkov organizaciji v nasprotju s prvim odstavkom 35. člena tega zakona;
18. če o izdaji varnostnega dovoljenja organizaciji ne obvesti nacionalnega varnostnega organa (drugi odstavek 35. člena);
19. če ne predlaga vmesnega varnostnega preverjanja organizacije (prvi in drugi odstavek 35.d člena);
20. če dovoli dostop do tajnih podatkov osebam v nasprotju s 3. točko prvega odstavka 35.b člena tega zakona;
21. če ne imenuje osebe iz 4. točke prvega odstavka 35.b člena tega zakona;
22. če ravna v nasprotju s 36. členom tega zakona;
23. če ravna v nasprotju s 37. členom tega zakona;
24. če ne izda akta iz četrtega odstavka 38. člena tega zakona;
25. če ne zagotovi usposabljanja oseb s področja obravnavanja tajnih podatkov v skladu s prvim odstavkom 25. člena, drugim odstavkom 31.a člena in tretjim odstavkom 38. člena tega zakona;
26. če ravna v nasprotju s prvim, drugim in četrtim odstavkom 39. člena tega zakona;
27. če ravna v nasprotju z drugim in tretjim odstavkom 40. člena tega zakona;
28. če ne organizira notranjega nadzora nad obravnavanjem tajnih podatkov (41. člen);
29. če ravna v nasprotju z drugim odstavkom 43.c člena tega zakona;
30. če ravna v nasprotju s četrtim odstavkom 43.d člena tega zakona.
Z globo od 200.000 do 500.000 tolarjev se kaznuje tudi odgovorna oseba državnega organa, organa samoupravne lokalne skupnosti, pravne osebe ali samostojnega podjetnika posameznika, ki stori prekršek iz prejšnjega odstavka.

44.a člen

Z globo od 500.000 do 1.000.000 tolarjev se kaznuje za prekršek pravna oseba ali samostojni podjetnik posameznik:
1. če ravna v nasprotju s prvim in drugim odstavkom 15. člena tega zakona;
2. če pri določitvi stopnje tajnosti podatku prekorači pristojnosti iz pooblastila za določanje tajnih podatkov;
3. če ne ravna v skladu s tretjim odstavkom 18. člena tega zakona;
4. če opusti dolžnost iz drugega odstavka 25.d člena tega zakona;
5. če najmanj tri mesece pred iztekom veljavnosti dovoljenja ne predlaga uvedbe postopka za izdajo novega dovoljenja osebi, ki bo po preteku veljavnosti dovoljenja to še vedno potrebovala (prvi odstavek 26. člena);
6. če ravna v nasprotju z drugim odstavkom 28. člena tega zakona;
7. če dopusti, da oseba dostopa do tajnih podatkov v nasprotju s 30. členom tega zakona;
8. če osebi omogoči dostop do tajnih podatkov višje stopnje, kot ima dovoljenje, ali omogoči pridobitev tajnega podatka prej in v večjem obsegu, kot je to potrebno za opravljanje delovnih nalog ali funkcije (drugi odstavek 31. člena).
Z globo od 100.000 do 300.000 tolarjev se kaznuje tudi odgovorna oseba državnega organa, organa samoupravne lokalne skupnosti, pravne osebe ali samostojnega podjetnika posameznika, ki stori prekršek iz prejšnjega odstavka.

45. člen

Z globo od 100.000 do 200.000 tolarjev se kaznuje za prekršek posameznik:

1. če ravna v nasprotju z 8. členom tega zakona;
2. če določi stopnjo tajnosti podatku oziroma dokumentu, pa za to ni pooblaščen (10. člen);
3. če opusti svojo dolžnost iz prvega odstavka 25.d člena tega zakona;
4. če dostopa do tajnih podatkov v nasprotju s prvim odstavkom 31. člena tega zakona;
5. če uporablja tajne podatke za druge namene kot za izvajanje določenih delovnih nalog ali funkcije (33. člen);
6. če posreduje tajne podatke v nasprotju s 34. členom tega zakona;
7. če posreduje tajne podatke organizaciji, ki nima varnostnega dovoljenja (prvi odstavek 35. člena);
8. če osebi omogoči dostop do tajnih podatkov v nasprotju s 3. točko prvega odstavka 35.b člena tega zakona;
9. če ne izvaja postopkov in ukrepov za obravnavanje tajnih podatkov, predpisanih s tem zakonom in predpisi, sprejetimi na njegovi podlagi;
10. če ne obvesti pooblaščene osebe o izgubi ali nepooblaščenem razkritju tajnega podatka oziroma posredovanju tajnega podatka nepoklicani osebi (40. člen).