REPUBLIKA SLOVENIJA
MINISTRSTVO ZA ZUNANJE ZADEVE

Prešernova cesta 25, 1000 Ljubljana

T: 01 478 2000
F: 01 478 2340, 01 478 2341
E: gp.mzz@gov.si
www.mzz.gov.si

Številka: 5611-43/2014/3 (114/10)
Ljubljana, 7. april 2014
EVA 2014-1811-0065
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE Gp.gs@gov.si

ZADEVA: Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Ciper o izmenjavi in medsebojnem varovanju tajnih podatkov – predlog za obravnavo

1. Predlog sklepov vlade:

Na podlagi tretjega odstavka 75. člena Zakona o zunanjih zadevah (Uradni list RS, št. 113/03 - uradno prečiščeno besedilo, 20/06 – ZNOMCMO, 76/08, 108/09 in 80/10 – ZUTD) in drugega odstavka 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 in 47/13) je Vlada Republike Slovenije na ..... seji dne ..... sprejela naslednji sklep:

Vlada Republike Slovenije je določila besedilo Predloga zakona o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Republike Ciper o izmenjavi in medsebojnem varovanju tajnih podatkov, sklenjenega 19. 2. 2014 v Ljubljani, in ga predloži Državnemu zboru Republike Slovenije.

Sklep prejmejo:
- Ministrstvo za zunanje zadeve,
- Urad Vlade RS za varovanje tajnih podatkov.

Priloga:
- predlog zakona z obrazložitvijo

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

(Navedite razloge, razen za predlog zakona o ratifikaciji mednarodne pogodbe, ki se obravnava po nujnem postopku – 169. člen Poslovnika državnega zbora.)

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- Borut Mahnič, generalni direktor Direktorata za mednarodno pravo in zaščito interesov Ministrstva za zunanje zadeve;
- Mihael Zupančič, vodja Sektorja za mednarodno pravo Ministrstva za zunanje zadeve.

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

(Navedite imena in priimke ter imena pravnih oseb.)
(Navedite s tem povezane stroške, ki bremenijo javnofinančna sredstva.)

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

- Karl Erjavec, minister za zunanje zadeve;
- Bogdan Benko, državni sekretar Ministrstva za zunanje zadeve;
- Boris Mohar, direktor Urada Vlade RS za varovanje tajnih podatkov;
- Borut Mahnič, generalni direktor Direktorata za mednarodno pravo in zaščito interesov Ministrstva za zunanje zadeve;
- Tatjana Balorda, sekretarka na Uradu Vlade RS za varovanje tajnih podatkov;
- Mihael Zupančič, vodja Sektorja za mednarodno pravo Ministrstva za zunanje zadeve.

5. Kratek povzetek gradiva:		
Sporazum ustvarja podlago za vzajemno posredovanje in varovanje izmenjanih tajnih podatkov tako na področju obrambe, širše javne uprave kot na področju gospodarskega sodelovanja.		
6. Presoja posledic za:		
a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	NE
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	NE
c)	administrativne posledice	NE
č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	NE
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	NE
e)	socialno področje	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	NE
7.a Predstavitev ocene finančnih posledic nad 40.000 EUR: (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
SKUPAJ				
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 na ukrepih oziroma projektih sprejetih proračunov,

- obveznosti za druga javnofinančna sredstva (drugi viri), ki niso načrtovana na 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 (npr. 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:

Gradivo nima nikakršnih učinkov na področjih iz tretje alineje tretjega odstavka 8. člena Poslovnika Vlade RS, oziroma ima zanemarljive finančne učinke (pod 40 000 € v tekočem in naslednjih treh letih).

8. Predstavitev sodelovanja javnosti:

Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	NE

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

(Če je odgovor DA, navedite:
Datum objave: ……
V razpravo so bili vključeni:

- nevladne organizacije,
- predstavniki zainteresirane javnosti,
- predstavniki strokovne javnosti,
- občine in združenja občin ali pa navedite, da se gradivo ne nanaša nanje.

Mnenja, predlogi in pripombe z navedbo predlagateljev (imen in priimkov fizičnih oseb, ki niso poslovni subjekti, ne navajajte):

Upoštevani so bili:

- v celoti,
- večinoma,

– delno, – niso bili upoštevani. Bistvena mnenja, predlogi in pripombe, ki niso bili upoštevani, ter razlogi za neupoštevanje: Poročilo je bilo dano …….. Javnost je bila vključena v pripravo gradiva v skladu z Zakonom o …, kar je navedeno v predlogu predpisa.)

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

Karl Erjavec
MINISTER

EVA 2014-1811-0065
PREDLOG

ZAKON O RATIFIKACIJI
Sporazuma med Vlado Republike Slovenije in Vlado Republike Ciper o izmenjavi in medsebojnem varovanju tajnih podatkov

1. člen

Ratificira se Sporazum med Vlado Republike Slovenije in Vlado Republike Ciper o izmenjavi in medsebojnem varovanju tajnih podatkov, sklenjen 19. 2. 2014 v Ljubljani.

2. člen

Besedilo sporazuma se v izvirniku v slovenskem in angleškem jeziku glasi[1]:

[1] Grška jezikovna različica je na vpogled v Sektorju za mednarodno pravo MZZ.

SPORAZUM

med Vlado Republike Slovenije in
Vlado Republike Ciper
o izmenjavi in medsebojnem varovanju tajnih podatkov

Vlada Republike Slovenije in Vlada Republike Ciper, v nadaljevanju "pogodbenici", sta se

v želji, da bi zagotovili varovanje tajnih podatkov, izmenjanih med njima ali med javnimi in zasebnimi subjekti v njuni pristojnosti,

ob spoznanju, da lahko dobro sodelovanje zahteva izmenjavo tajnih podatkov med pogodbenicama,

dogovorili:

1. člen

Pomen izrazov

V tem sporazumu izrazi pomenijo:

1. "prejemnik" – pristojni organ, ki prejme tajne podatke;

2. "pristojni organ" – javni ali zasebni subjekt v pristojnosti pogodbenice, ki je pooblaščen za ravnanje s tajnimi podatki in njihovo hrambo v skladu z notranjo zakonodajo te pogodbenice, vključno s pristojnim varnostnim organom;

3. "pristojni varnostni organ" – državni organ iz prvega odstavka 3. člena, ki ga določi pogodbenica za splošno izvajanje tega sporazuma in ustrezen nadzor nad vsemi njegovimi vidiki;

4. "izvajalec" – posameznik, pravna oseba ali organizacijska enota s sposobnostjo za sklepanje pogodb;

5. "pogodba s tajnimi podatki" – pogodba ali podpogodba, ki zahteva dostop do tajnih podatkov;

6. "tajni podatek" – podatek v kakršni koli obliki, ki se prenese ali nastane med pogodbenicama ali pristojnima organoma in ga je treba po notranji zakonodaji pogodbenice varovati pred nepooblaščenim razkritjem ali drugim ogrožanjem ter ga je kot takega določila in ustrezno označila pogodbenica;

7. "varnostno dovoljenje organizacije" – odločitev po varnostnem preverjanju organizacije, da izvajalec, ki je pravna oseba, izpolnjuje pogoje za ravnanje s tajnimi podatki v skladu z notranjo zakonodajo pogodbenice;

8. "potreba po seznanitvi" – načelo, po katerem se posamezniku lahko dovoli dostop do določenih tajnih podatkov le v povezavi z njegovimi uradnimi dolžnostmi ali zaradi opravljanja določene naloge;

9. "dovoljenje za dostop do tajnih podatkov" – odločitev po varnostnem preverjanju osebe v skladu z notranjo zakonodajo, na podlagi katere je posameznik pooblaščen za dostop do tajnih podatkov stopnje tajnosti, ki je navedena na dovoljenju, in za ravnanje z njimi;

10. "naročnik" – vladni organ, ki namerava skleniti ali sklene pogodbo s tajnimi podatki na ozemlju druge pogodbenice;

11. "tretja stran" – država, vključno z javnim ali zasebnim subjektom ali posameznikom v njeni pristojnosti, ali mednarodna organizacija, ki ni pogodbenica tega sporazuma.

2. člen

Stopnje tajnosti

Pogodbenici soglašata, da so naslednje stopnje tajnosti enakovredne in ustrezajo stopnjam tajnosti, določenim v njuni notranji zakonodaji:

Republika Slovenija	Republika Ciper	Angleška ustreznica
STROGO TAJNO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
TAJNO	ΑΠΟΡΡΗΤΟ	SECRET
ZAUPNO	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
INTERNO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

3. člen

Pristojna varnostna organa

1. Pristojna varnostna organa za namen tega sporazuma sta:

   a. za Republiko Slovenijo: nacionalni varnostni organ (Urad Vlade Republike Slovenije za varovanje tajnih podatkov);

   b. za Republiko Ciper: nacionalni varnostni organ (Ministrstvo za obrambo).

2. Pristojna varnostna organa lahko sklepata dogovore o izvajanju določb tega sporazuma.

3. Pogodbenici se po diplomatski poti obveščata o vseh poznejših spremembah nacionalnih varnostnih organov.

4. člen

Načela varovanja tajnih podatkov

1. Pogodbenici v skladu s tem sporazumom in svojo notranjo zakonodajo sprejmeta ustrezne ukrepe za varovanje tajnih podatkov.

2. Pogodbenici za podatke iz prvega odstavka zagotovita najmanj enako varovanje, kot ga uporabljata za svoje tajne podatke ustrezne stopnje tajnosti iz 2. člena.

3. Za splošno izvajanje tega sporazuma in ustrezen nadzor nad vsemi njegovimi vidiki sta odgovorna pristojna nacionalna varnostna organa, ki ju določita pogodbenici.

4. Do prejetih tajnih podatkov lahko dostopajo le osebe, ki imajo potrebo po seznanitvi, so bile varnostno preverjene in/ali pooblaščene za dostop do tovrstnih podatkov ter ustrezno poučene o varovanju tajnih podatkov v skladu z notranjo zakonodajo pogodbenice.

5. Pogodbenica zagotovi, da se izvajajo ustrezni ukrepi za varovanje tajnih podatkov, ki se obdelujejo, hranijo ali prenašajo v komunikacijskih in informacijskih sistemih. Ti ukrepi zagotavljajo zaupnost, celovitost, razpoložljivost, in kadar je mogoče, nezatajljivost in verodostojnost tajnih podatkov ter ustrezno raven odgovornosti in sledljivosti dejanj, povezanih s temi podatki.

6. Stopnjo tajnosti spremeni ali prekliče le pristojni organ, ki jo je določil. O vsaki spremembi ali preklicu stopnje tajnosti je prejemnik nemudoma obveščen.

7. Pogodbenici si priznavata dovoljenja za dostop do tajnih podatkov in varnostna dovoljenja organizacij. Pri tem se glede stopenj tajnosti uporablja 2. člen.

5. člen

Omejitve pri uporabi tajnih podatkov

1. Prejeti tajni podatki se uporabljajo izključno za namene in po pogojih za dajanje tajnih podatkov ali v skladu z omejitvami njihove uporabe, kot se določi ob prenosu tajnih podatkov.

2. Pogodbenica tajnih podatkov ne sme dati tretji strani brez predhodnega pisnega soglasja pristojnega varnostnega organa druge pogodbenice, ki je določila ustrezno stopnjo tajnosti.

6. člen

Pogodbe s tajnimi podatki

1. Naročnik lahko sklene pogodbo s tajnimi podatki z izvajalcem druge pogodbenice.

2. V primeru iz prvega odstavka naročnik pristojnemu varnostnemu organu svoje pogodbenice predloži zaprosilo, naj pristojni varnostni organ druge pogodbenice zaprosi za pisno potrdilo, da je izvajalec pooblaščen za dostop do tajnih podatkov določene stopnje tajnosti.

3. Potrdilo iz drugega odstavka zagotavlja, da izvajalec izpolnjuje merila za varovanje tajnih podatkov, določena v notranji zakonodaji pogodbenice, na ozemlju katere je izvajalec.

4. Če izvajalec prej ni bil pooblaščen za dostop do tajnih podatkov določene stopnje tajnosti, pristojni varnostni organ, ki naj bi izdal potrdilo, nemudoma uradno obvesti pristojni varnostni organ druge pogodbenice, da bodo na njegovo zahtevo izvedena dejanja v skladu s tretjim odstavkom.

5. Izvajalec do prejema potrdila iz drugega in tretjega odstavka nima dostopa do tajnih podatkov.

6. Naročnik izvajalca uradno obvesti o varnostnih zahtevah, ki so potrebne za izvajanje pogodbe s tajnimi podatki ter še zlasti vključujejo seznam tajnih podatkov in pravila o določanju stopnje tajnosti podatkov, ki nastanejo med izvajanjem pogodbe s tajnimi podatki. Izvod takih dokumentov se pošlje pristojnemu varnostnemu organu.

7. Pristojni varnostni organ pogodbenice, na katere ozemlju se bo izvajala pogodba s tajnimi podatki, zagotovi, da izvajalec varuje tajne podatke v skladu s prejetimi varnostnimi zahtevami in notranjo zakonodajo svoje pogodbenice.

8. Pristojna varnostna organa zagotovita, da vsi morebitni podizvajalci izpolnjujejo enake pogoje za varovanje tajnih podatkov, kot so bili predpisani za izvajalca.

7. člen

Prenos tajnih podatkov

1. Prenos tajnih podatkov poteka po diplomatski poti ali drugih zaščitenih poteh, ki zagotavljajo varovanje pred nepooblaščenim razkritjem in o katerih se dogovorita pristojna varnostna organa. Prejemnik pisno potrdi prejem tajnih podatkov.

2. Tajni podatki INTERNO/ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/RESTRICTED se lahko pošiljajo po pošti ali z drugo dostavno službo v skladu z notranjo zakonodajo.

8. člen

Razmnoževanje in prevajanje tajnih podatkov

1. Podatki stopnje STROGO TAJNO/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TOP SECRET se razmnožujejo le s predhodnim pisnim dovoljenjem pristojnega organa pogodbenice, ki je tem podatkom določil stopnjo tajnosti.

2. Tajni podatki se razmnožujejo v skladu z notranjo zakonodajo pogodbenic. Razmnoženi podatki se varujejo enako kot izvirniki. Število izvodov je omejeno na najmanjšo količino, potrebno za uradne namene.

3. Tajne podatke prevajajo ustrezno varnostno preverjeni posamezniki. Vsak prevod vsebuje ustrezno navedbo v jeziku prevoda, da prevod vsebuje tajne podatke druge pogodbenice. Prevod se varuje enako kot izvirnik.

9. člen

Uničevanje tajnih podatkov

1. Tajni podatki se uničijo v skladu z notranjo zakonodajo pogodbenice, tako da jih ni mogoče več delno ali v celoti obnoviti.

2. Tajni podatki z oznako STROGO TAJNO/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TOP SECRET se ne smejo uničiti. Vrnejo se pristojnemu organu pogodbenice, ki je podatkom določil stopnjo tajnosti.

3. V kriznih razmerah, ko ni mogoče varovati ali vrniti tajnih podatkov, se ti takoj uničijo. Prejemnik o uničenju čim prej obvesti pristojni varnostni organ druge pogodbenice.

10. člen

Obiski

1. Za obiske, pri katerih je potreben dostop do tajnih podatkov, se zahteva predhodno dovoljenje pristojnega varnostnega organa pogodbenice gostiteljice.

2. Dovoljenje iz prvega odstavka se izda samo osebam, ki jih je določila pogodbenica in so v skladu z njeno notranjo zakonodajo pooblaščene za dostop do tajnih podatkov

3. Zaprosilo za obisk se predloži ustreznemu nacionalnemu varnostnemu organu vsaj 20 dni pred začetkom obiska. Vsebuje te podatke, ki se uporabljajo samo za obisk:

   a. namen, datum in program obiska, vključno z najvišjo stopnjo tajnosti podatkov, ki bodo obravnavani;

   b. ime in priimek obiskovalca, datum in kraj rojstva, državljanstvo ter številko potnega lista ali osebne izkaznice;

   c. položaj obiskovalca skupaj z imenom institucije ali organizacije, ki jo obiskovalec zastopa;

   d. veljavnost in stopnjo tajnosti obiskovalčevega dovoljenja za dostop do tajnih podatkov;

   e. ime in naslov organizacije, ki bo obiskana;

   f. ime in priimek, podatki za stike ter položaj osebe, ki bo obiskana;

   g. datum in podpis pristojnega varnostnega organa.

4. Pristojni organi zagotovijo varstvo osebnih podatkov obiskovalca v skladu s svojo notranjo zakonodajo.

5. Tajni podatki, ki so dostopni med obiskom, se varujejo v skladu z določbami tega sporazuma.

11. člen

Kršitev varovanja tajnosti

1. Ob kršitvi varovanja tajnosti, katere posledica je nepooblaščeno razkritje, odtujitev ali izguba tajnih podatkov, ali sumu take kršitve pristojni varnostni organ prejemnika čim prej obvesti pristojni varnostni organ druge pogodbenice in začne ustrezno preiskavo.

2. Kadar varovanje tajnosti krši tretja stran, pristojni varnostni organ pogodbenice, ki je dala podatke, sprejme vse potrebne ukrepe, s katerimi zagotovi začetek dejanj, predpisanih v prvem odstavku.

3. Pristojni varnostni organ pogodbenice, ki je dala tajne podatke, na podlagi zaprosila sodeluje pri preiskavi v skladu s prvim odstavkom. Obveščen mora biti o ugotovitvah preiskave in prejeti končno poročilo o razlogih za škodo in njenih razsežnostih.

12. člen

Stroški

Vsaka pogodbenica krije svoje stroške, ki nastanejo pri izvajanju tega sporazuma.

13. člen

Posvetovanja

1. Pristojna varnostna organa pogodbenic se uradno obveščata o vseh spremembah svoje notranje zakonodaje, ki se nanaša na varovanje tajnih podatkov.

2. Pristojna varnostna organa pogodbenic se na zaprosilo enega od njiju med seboj posvetujeta, da zagotovita tesno sodelovanje pri izvajanju določb tega sporazuma.

3. Pristojna varnostna organa pogodbenic se obiskujeta zaradi dogovarjanja o postopkih in standardih varovanja tajnih podatkov.

4. Pristojna varnostna organa se takoj obvestita o vsaki spremembi medsebojno priznanih dovoljenj za dostop do tajnih podatkov in varnostnih dovoljenj organizacij.

5. Na zaprosilo si pristojna varnostna organa pomagata pri izvajanju postopkov varnostnega preverjanja.

14. člen

Reševanje sporov

1. Spori zaradi razlage ali uporabe tega sporazuma se rešujejo neposredno s pogajanji in/ali posvetovanji med pristojnima varnostnima organoma pogodbenic.

2. Če spora ni mogoče rešiti v skladu s prvim odstavkom, se reši po diplomatski poti.

15. člen

Končne določbe

1. Sporazum začne veljati prvi dan drugega meseca po datumu, ko se pogodbenici po diplomatski poti uradno obvestita, da so bili končani vsi potrebni notranjepravni postopki za začetek njegove veljavnosti.

2. Sporazum je sklenjen za nedoločen čas. Pogodbenica ga lahko odpove s pisnim obvestilom drugi pogodbenici. V tem primeru sporazum preneha veljati šest mesecev po datumu obvestila o odpovedi.

3. Ob prenehanju veljavnosti tega sporazuma se vsi tajni podatki, preneseni na njegovi podlagi, še naprej varujejo v skladu z njegovimi določbami.

4. Sporazum se lahko spremeni s pisnim soglasjem pogodbenic. Spremembe začnejo veljati v skladu s prvim odstavkom.

Sestavljeno v Ljubljani, 19. februarja 2014 v dveh izvirnikih v slovenskem, grškem in angleškem jeziku, pri čemer so vsa besedila enako verodostojna. Pri različni razlagi prevlada angleško besedilo.

Za Vlado **Republike Slovenije**	**Za Vlado** **Republike Ciper**
Boris Mohar l.r.	Demetrakis Demetriou l.r

AGREEMENT

Between the Government of the Republic of Slovenia and the Government of the Republic of Cyprus on the Exchange and Mutual Protection of Classified Information

The Government of the Republic of Slovenia and the Government of the Republic of Cyprus hereinafter referred to as ´´the Parties´´;

Wishing to ensure the protection of Classified Information exchanged between the Parties or between public and private entities under their jurisdiction;

Realizing that good cooperation may require the exchange of Classified Information between the Parties;

Have agreed as follows:

Article 1

Definitions

For the purposes of this Agreement these terms shall mean the following:

1. ´´ Recipient´´ - the Competent Authority receiving the Classified Information;

2. ´´Competent Authority´´ - public or private entity under jurisdiction of any Party authorized to handle and store Classified Information in accordance with the national legislation of its Party, including the Competent Security Authority;

3. ´´Competent Security Authority´´ - state authority, designated by the Party as responsible for the general implementation and the relevant controls of all aspects of this Agreement as referred to in Article 3 Paragraph 1;

4. ´´Contractor´´ - an individual, a legal entity or an organizational unit, which has the capacity to conclude contracts;

5. ´´Classified Contract´´ - a contract or a subcontract, which requires access to Classified Information;

6. ´´Classified Information´´ - any information, regardless of its form, which is transmitted or generated between the Parties or Competent Authorities and requires, under the national legislation of either Party, the protection against unauthorized disclosure or other compromise and is designated as such and marked appropriately by a Party;

7. ˝Facility Security Clearance˝ - A determination following an investigative procedure certifying that a contractor which is a legal entity fulfils the conditions of handling Classified Information in accordance with the national legislation of one of the Parties;

8. ″Need-to-know″ - a principle by which access to specific Classified Information may be granted to an individual only in connection with his/her official duties or for the performance of a specific task;

9. ″Personnel Security Clearance″ - A determination following an investigative procedure in accordance with the national legislation, on the basis of which an individual is authorised to have access to and to handle Classified Information up to the level defined in the clearance;

10. ´´Principal´´ - a governmental body, which intends to conclude or concludes a Classified Contract in the territory of the other Party;

11. ″Third Party″ - a state, including any public or private entity or individual under its jurisdiction, or an international organization which is not a Party to this Agreement.

Article 2

Security Classification Levels

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in their national legislation:

Republic of Slovenia	Republic of Cyprus	English Equivalent
STROGO TAJNO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
TAJNO	ΑΠΟΡΡΗΤΟ	SECRET
ZAUPNO	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
INTERNO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

Article 3

Competent Security Authorities

1. For the purposes of this Agreement, the Competent Security Authorities shall be:

   a. for the Republic of Slovenia: National Security Authority (Government Office for the Protection of Classified Information);

   b. for the Republic of Cyprus: National Security Authority (Ministry of Defence).

2. The Competent Security Authorities may conclude implementation agreements for the purposes of the implementation of the provisions hereof.

3. The Parties shall inform each other through diplomatic channels of any subsequent changes of the National Security Authorities.

Article 4

Principles of Classified Information Protection

1. In accordance with this Agreement and their national legislation, the Parties shall adopt appropriate measures aimed at the protection of Classified Information.

2. The Parties shall provide for the information referred to in paragraph 1 at least the same protection as applicable to their own Classified Information under the relevant security classification level, pursuant to Article 2.

3. The National Security Authorities designated by the Parties are responsible for the general implementation and the relevant controls of all aspects of this Agreement.

4. Received Classified Information shall be accessible only to those persons who have a need-to-know, who have been security cleared and/or who have been authorized to have access to such information as well as briefed in the scope of Classified Information protection according to the national legislation of their Party.

5. Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and where applicable, non-repudiation and authenticity of Classified Information as well as an appropriate level of accountability and traceability of actions in relation to that information.

6. The security classification level shall be changed or removed only by the Competent Authority, which has granted it. The Recipient shall be immediately notified on every change or removal of security classification level.

7. The Parties shall mutually recognise their respective Personnel and Facility Security Clearances. To this effect, Article 2 regarding the security classification levels shall apply accordingly.

Article 5

Restriction of use of classified information

1. Received Classified Information shall be used exclusively for the purposes and under conditions of release or limitations on the use of the Classified Information, defined at the transmission thereof.

2. Either Party shall not release Classified Information to Third Party without a prior written consent of the Competent Security Authority of the other Party, which granted adequate security classification level.

Article 6

Classified Contracts

1. The Principal may conclude a Classified Contract with the Contractor of the other Party.

2. In the case referred to in Paragraph 1, the Principal shall submit a request to the Competent Security Authority of its Party to ask the Competent Security Authority of the other Party for issuing a written assurance that the Contractor is authorized to have access to Classified Information of the specified security classification level.

3. The issuing of the assurance referred to in Paragraph 2 shall guarantee that the Contractor fulfils the criteria in the scope of the protection of Classified Information, as provided in the applicable national legislation of the Party, in the territory of which the Contractor is located.

4. If the Contractor has not been previously authorized to have access to Classified Information of the specified security classification level, the Competent Security Authority which is to issue the assurance, shall immediately notify the Competent Security Authority of the other Party, that upon its request, the actions referred to in Paragraph 3 will be undertaken.

5. Classified Information shall not be accessible to the Contractor until the receipt of the assurance referred to in Paragraphs 2 and 3.

6. The Principal shall notify the Contractor of the security requirements necessary to perform the Classified Contract, which include in particular a list of Classified Information and rules of classification of the information originated during the performance of the Classified Contract. The copy of such documents shall be transmitted to the Competent Security Authority.

7. The Competent Security Authority of the Party in whose territory the Classified Contract is to be performed shall ensure that the Contractor protects Classified Information in accordance with the received security requirements and national legislation of its Party.

8. The Competent Security Authorities shall ensure that any possible subcontractors shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted through diplomatic channels or through other secured channels ensuring protection against unauthorized disclosure, agreed upon between the Competent Security Authorities. The Recipient shall confirm the receipt of Classified Information in writing.

2. Information classified as INTERNO/ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/RESTRICTED may be transmitted also by post or another delivery service in accordance with the national legislation.

Article 8

Reproduction and Translation of Classified Information

1. Information classified as STROGO TAJNO/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TOP SECRET shall be reproduced only after a prior written permission issued by the Competent Authority of the party which classified this information.

2. Reproduction of Classified Information shall be pursuant to the national legislation of each of the Parties. Reproduced information shall be placed under the same protection as the originals. Number of copies shall be reduced to minimum required for official purposes.

3. Any translation of Classified Information shall be made by properly security cleared individuals. All translations shall bear an appropriate note in the language into which they have been translated, stating that they contain Classified Information of the other Party. The translation shall be placed under the same protection as the originals.

Article 9

Destruction of Classified Information

1. Classified Information shall be destroyed according to the national legislation of the Parties, in such a manner as to eliminate the partial or total reconstruction of the same.

2. Classified Information marked as STROGO TAJNO/АКРΩΣ АПОРРНТО/TOP SECRET shall not be destroyed. It shall be returned to the Competent Authority of the party which classified this information.

3. In case of a crisis situation in which it is impossible to protect or return Classified Information such information shall be destroyed immediately. The Recipient shall inform the Competent Security Authority of the other Party about this destruction as soon as possible.

Article 10

Visits

1. Visits necessitating access to Classified Information shall be subject to prior permission of the Competent Security Authority of the host Party.

2. The permission referred to in Paragraph 1 shall be granted exclusively to the persons authorized to have access to Classified Information pursuant to the national legislation of the Party designating such a person.

3. A request for visit shall be submitted to the relevant National Security Authority at least 20 days prior to the commencement of the visit. The request for the visit shall include the following data that shall be used for the purpose of the visit only:

a. purpose, date and program of the visit including the highest security classification level of Classified Information to be involved;

b. name and surname of the visitor, date and place of birth, citizenship, passport number or identity card number;

c. position of the visitor together with the name of the institution or organization which he or she represents;

d. the validity and certification of the level of Personnel Security Clearance held by the visitor;

e. name and address of the organization to be visited;

f. name, surname, contact data and position of the person to be visited;

g. the date and signature of the Competent Security Authority.

4. The Competent Authorities shall ensure the protection of the personal data of the visitor pursuant to their national legislation.

5. Classified Information accessible during the visit shall be protected pursuant to the provisions of this Agreement.

Article 11

Breach of Security

1. In case of Breach of Security, resulting in unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a breach, the Competent Security Authority of the Recipient shall inform the Competent Security Authority of the other Party, as soon as possible, and initiate the appropriate investigation.

2. If a breach of security arises in a Third Party, the Competent Security Authority of the Party which has provided the information to the Third Party shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 are initiated.

3. The Competent Security Authority of the Party which provided such information shall, upon request, cooperate in the investigation in accordance with Paragraph 1. It shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damage.

Article 12

Expenses

Each Party shall cover its own expenses resulting from the implementation of this Agreement.

Article 13

Consultation

1. The Competent Security Authorities of the Parties shall notify each other of any amendments to their national legislation concerning the protection of Classified Information.

2. The Competent Security Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions hereof.

3. Competent Security Authorities of the Parties shall exchange visits to discuss the procedures and standards for the protection of Classified Information.

4. The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized Personnel and Facility Security Clearances.

5. Upon request, the Competent Security Authorities shall assist each other in carrying out security clearance procedures.

Article 14

Settlement of Disputes

1. Any disputes concerning the interpretation or application of this Agreement shall be settled by direct negotiations and/or consultations between the Competent Security Authorities of the Parties.

2. If the settlement of a dispute can not be reached in the manner referred to in Paragraph 1, such a dispute shall be settled through diplomatic channels.

Article 15

Final Provisions

1. This Agreement shall enter into force on the first day of the second month following the date on which the Parties notify each other, through diplomatic channels, that all necessary internal procedures for the entry into force of this Agreement have been completed.

2. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party upon giving a written notice to the other Party. In such a case this Agreement shall expire six months after the date of the termination notice.

3. In case of termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

4. This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1.

Done at Ljubljana on 19 February 2014 in two originals, each in Slovenian, Greek and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

For the Government of the Republic of Slovenia	**For the Government of the Republic of Cyprus**
Boris Mohar (s)	Demetrakis Demetriou (s)

3. člen

Za izvajanje sporazuma skrbi Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

4. člen

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

OBRAZLOŽITEV

Vlada Republike Slovenije je sprejela pobudo za sklenitev Sporazuma med Vlado Republike Slovenije in Vlado Republike Ciper o izmenjavi in medsebojnem varovanju tajnih podatkov št. 02205-7/2012/3 z dne 25. 10. 2012.

Sporazum je podlaga za kakršno koli dejavnost, ki vključuje izmenjavo tajnih podatkov med pogodbenicama, njunimi državnimi organi ali javnimi in zasebnimi subjekti.

Opredeljuje izraze, ki se uporabljajo v besedilu: prejemnik, pristojni organ, pristojni varnostni organ, izvajalec, pogodba s tajnimi podatki, tajni podatek, varnostno dovoljenje organizacije, potreba po seznanitvi, dovoljenje za dostop do tajnih podatkov, naročnik in tretja stran.
Sporazum določa pristojna varnostna organa in dolžnost obveščanja o spremembi slednjih ter opredeljuje razvrstitev tajnih podatkov in enakovrednost nacionalnih oznak stopenj tajnosti v Republiki Sloveniji in Republiki Cipru.
Sporazum nadalje določa varovanje izmenjanih tajnih podatkov. Pri varovanju tajnih podatkov je najpomembnejše načelo, da pogodbenici v skladu z notranjimi zakoni in predpisi izvajata do prejetih tajnih podatkov enakovredne varnostne ukrepe, ki se izvajajo do lastnih tajnih podatkov enakovredne stopnje tajnosti.
Dostop do tajnih podatkov je dovoljen le osebam, ki morajo biti seznanjene s temi podatki zaradi izvajanja uradnih dolžnosti ali pristojnosti z namenom, ki je predviden ob njihovem posredovanju, in ki so za to pravilno pooblaščene v skladu z notranjimi zakoni in predpisi države vsake od pogodbenic.
Pogodbenici si medsebojno priznavata dovoljenja za dostop do tajnih podatkov in varnostna dovoljenja organizacij.
Opredeljen je način ter pogoji za prenos tajnih podatkov. Prenos nosilcev tajnih podatkov se izvaja po diplomatski poti ali drugih varnih poteh, ki jih obojestransko dogovorita nacionalna varnostna organa, pri najnižji stopnji tajnosti pa tudi po pošti ali drugi dostavni službi.
Prejete nosilce tajnih podatkov pooblaščeni organ/organizacija, ki odgovarja za njihov prejem, označi z ustreznimi nacionalnimi oznakami stopnje tajnosti, ki so primerljive v skladu z določili sporazuma.
Določen je tudi način razmnoževanja, prevajanja in uničevanja tajnih podatkov ter postopki določanja tajnih podatkov.
Pogodbe, ki jih sklenejo pooblaščeni organi/organizacije, vsebujejo posebno prilogo, ki določa seznam tajnih podatkov, ki so predvideni za posredovanje in stopnjo njihove tajnosti, posebnosti varovanja tajnih podatkov in njihovega obravnavanja ter način reševanja spornih situacij in obveznosti glede povrnitve možne škode zaradi zlorabe tajnih podatkov.
O kršitvi varovanja tajnih podatkov, ki jo ugotovi pooblaščeni organ/organizacija ali pristojni organ ene pogodbenice, in ki je povzročila ali lahko povzroči zlorabo tajnih podatkov, se nemudoma obvesti pristojni organ druge pogodbenice.
Za obiske, ki zahtevajo dostop do tajnih podatkov države druge pogodbenice, je potrebno pridobiti soglasje pristojnega organa države gostiteljice.
Pristojna organa izmenjujeta notranje zakone in predpise svojih držav s področja varovanja tajnih podatkov, ki so potrebni za izvajanje tega sporazuma.
Spori glede razlage in uporabe določb tega sporazuma se rešujejo s pogajanji in posvetovanji med pristojnima varnostnima organoma. Sporazum se sklene za nedoločen čas.

Sklenjeni mednarodni sporazum bo ustvaril podlago za vzajemno posredovanje in varovanje izmenjanih tajnih podatkov tako na področju obrambe, širše javne uprave kot na področju gospodarskega sodelovanja.

Sporazum med Vlado Republike Slovenije in Vlado Republike Ciper o izmenjavi in medsebojnem varovanju tajnih podatkov je bil podpisan 19. februarja 2014 v Ljubljani.

Predlog Zakona o ratifikaciji sporazuma ni bil uvrščen v normativni program dela Vlade Republike Slovenije za leto 2014.

Predlagamo, da sporazum ratificira Državni zbor Republike Slovenije.

Zakon o ratifikaciji začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije – Mednarodne pogodbe.

Za izvajanje sporazuma ni potrebno spreminjati obstoječih ali sprejemati novih predpisov.

Sporazum ni predmet usklajevanja s pravnim redom Evropske unije.

Uresničevanje sporazuma neposredno ne zahteva posebnih finančnih sredstev.