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: 5611-2/2022/4
Ljubljana, 10. 2. 2022
EVA: 2022-1811-0001
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE Gp.gs@gov.si

ZADEVA: Zakon o ratifikaciji Sporazuma med Vlado Republike Slovenije in Vlado Helenske republike o medsebojnem varovanju izmenjanih tajnih podatkov – *predlog za obravnavo*

1. Predlog sklepov vlade:

Na podlagi četrtega odstavka 75. člena Zakona o zunanjih zadevah (Uradni list RS, št. 113/03 – uradno prečiščeno besedilo, 20/06 – ZNOMCMO, 76/08, 108/09, 80/10 – ZUTD, 31/15 in 30/18 – ZKZaš) in drugega odstavka 2. člena ter 21. 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, 65/14 in 55/17) 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 Helenske republike o medsebojnem varovanju izmenjanih tajnih podatkov, podpisanega 4. 10. 2021 v Atenah, in ga predloži Državnemu zboru Republike Slovenije.

Mag. Janja Garvas Hočevar
vršilka dolžnosti generalnega sekretarja

Sklep prejmejo:
- Državni zbor Republike Slovenije
- Ministrstvo za zunanje zadeve
- Urad Vlade Republike Slovenije 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:

/

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

- dr. Marko Rakovec, generalni direktor Direktorata za mednarodno pravo in zaščito interesov in glavni pravni svetovalec v Ministrstvu za zunanje zadeve,
- Mateja Štrumelj-Piškur, vodja Sektorja za mednarodno pravo v Ministrstvu za zunanje zadeve.

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

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

- dr. Anže Logar, minister za zunanje zadeve,
- Igor Eršte, direktor Urada Vlade Republike Slovenije za varovanje tajnih podatkov,
- Gašper Dovžan, državni sekretar v Ministrstvu za zunanje zadeve,

- dr. Marko Rakovec, generalni direktor Direktorata za mednarodno pravo in zaščito interesov in glavni pravni svetovalec v Ministrstvu za zunanje zadeve,
- Mateja Štrumelj Piškur, vodja Sektorja za mednarodno pravo v Ministrstvu za zunanje zadeve,
- dr. Milan Tarman, sekretar,
- Maja Semolič Jarc, sekretarka.

5. Kratek povzetek gradiva:

Sporazum med Vlado Republike Slovenije in Vlado Helenske republike o medsebojnem varovanju izmenjanih tajnih podatkov je bil podpisan 4. 10. 2021 v Atenah.

Predstavlja pravno podlago za izvajanje nalog državnih organov in poslovanje gospodarskih subjektov, ki pri svojem delu izmenjujejo tajne podatke na različnih področjih bilateralnega sodelovanja. Določa pogoje za izmenjavo tajnih podatkov in načine njihovega varovanja.

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)	administrativne posledice	DA/NE
č)	gospodarstvo, zlasti 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:
(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:

(Samo če izberete NE pod točko 6.a.)

Kratka obrazložitev

Izvajanje sporazuma ne bo imelo finančnih posledic.

8. Predstavitev sodelovanja z združenji občin:

Vsebina predloženega gradiva (predpisa) vpliva na: - pristojnosti občin, - delovanje občin, - financiranje občin.	DA/<u>NE</u>

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: DA/<u>NE</u>
- Združenju občin Slovenije ZOS: DA/<u>NE</u>
- Združenju mestnih občin Slovenije ZMOS: DA/<u>NE</u>

Predlogi in pripombe združenj so bili upoštevani:

- v celoti,
- večinoma,
- delno,

– niso bili upoštevani. Bistveni predlogi in pripombe, ki niso bili upoštevani.

9. Predstavitev sodelovanja javnosti:	
Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	DA/NE
(Če je odgovor DA, navedite: Datum objave: …… V razpravo so bili vključeni: – nevladne organizacije, – predstavniki zainteresirane javnosti, – predstavniki strokovne javnosti. – . 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.)	
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

Gašper Dovžan
DRŽAVNI SEKRETAR

PREDLOG
EVA: 2022-1811-0001

ZAKON
O RATIFIKACIJI SPORAZUMA MED VLADO REPUBLIKE SLOVENIJE IN VLADO HELENSKE REPUBLIKE O MEDSEBOJNEM VAROVANJU IZMENJANIH TAJNIH PODATKOV

1. člen

Ratificira se Sporazum med Vlado Republike Slovenije in Vlado Helenske republike o medsebojnem varovanju izmenjanih tajnih podatkov, sklenjen 4. oktobra 2021 v Atenah.

2. člen

Sporazum se v slovenskem in angleškem jeziku glasi:

SPORAZUM
MED
VLADO
REPUBLIKE SLOVENIJE
IN
VLADO
HELENSKE REPUBLIKE
O MEDSEBOJNEM VAROVANJU
IZMENJANIH TAJNIH PODATKOV

Vlada Republike Slovenije

in

Vlada Helenske republike,

v nadaljnjem besedilu: "pogodbenici",

sta se:

v želji, da bi zagotovili varovanje tajnih podatkov, izmenjanih med njima ali med javnimi in zasebnimi subjekti pod njuno jurisdikcijo,

ob upoštevanju nacionalnih interesov in varnosti držav pogodbenic,

1. ČLEN
NAMEN

Pogodbenici v skladu s svojo zakonodajo sprejmeta vse ustrezne ukrepe, da bi zagotovili varovanje tajnih podatkov, ki se prenesejo ali nastanejo po tem sporazumu.

2. ČLEN
OPREDELITEV IZRAZOV

Za namene tega sporazuma se uporabljajo naslednje opredelitve izrazov:

tajni podatek: podatek, ki se ne glede na obliko prenese ali nastane med pogodbenicama po notranji zakonodaji pogodbenic in v interesu nacionalne varnosti zahteva varovanje pred nepooblaščenim razkritjem ali drugim ogrožanjem ter je bil kot tak določen in ustrezno označen;

pogodbenica izvora: pogodbenica, vključno z javnimi ali zasebnimi subjekti pod njeno jurisdikcijo, ki daje tajne podatke pogodbenici prejemnici;

pogodbenica prejemnica: pogodbenica, vključno z javnimi ali zasebnimi subjekti pod njeno jurisdikcijo, ki prejema tajne podatke od pogodbenice izvora;

potreba po seznanitvi: načelo, po katerem se posamezniku ali posameznici lahko dovoli dostop do tajnih podatkov le za opravljanje njegovih ali njenih uradnih dolžnosti ali nalog;

dovoljenje za dostop do tajnih podatkov: odločitev po varnostnem preverjanju 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;

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

izvajalec: posameznik ali pravna oseba s pravno sposobnostjo za sklepanje pogodb;

pogodba s tajnimi podatki: pogodba ali podizvajalska pogodba, vključno s pogajanji pred sklenitvijo pogodbe, ki vsebuje tajne podatke ali vključuje dostop do njih;

tretja stran: država, vključno z javnim ali zasebnim subjektom pod njeno jurisdikcijo, ali mednarodna organizacija, ki ni pogodbenica tega sporazuma.

3. ČLEN
PRISTOJNI VARNOSTNI ORGANI

(1) Nacionalna varnostna organa, ki sta ju pogodbenici imenovali za odgovorna za splošno izvajanje tega sporazuma, sta

v Republiki Sloveniji:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov (NVO),

v Helenski republiki:
Nacionalni varnostni organ (NVO), Generalštab Helenske nacionalne obrambe (HNDGS), Združeni vojaški obveščevalni sektor (JMID).

(2) Nacionalna varnostna organa drug drugega uradno obvestita o vseh pristojnih varnostnih organih, odgovornih za izvajanje tega sporazuma.

(3) Pogodbenici se po diplomatski poti uradno obveščata o vseh poznejših spremembah svojih nacionalnih varnostnih organov.

4. ČLEN
STOPNJE TAJNOSTI

(1) Vsi tajni podatki, dani na podlagi tega sporazuma, so označeni z ustrezno stopnjo tajnosti v skladu z notranjo zakonodajo pogodbenic.

(2) Enakovredne stopnje tajnosti so:

V REPUBLIKI SLOVENIJI	V HELENSKI REPUBLIKI	V ANGLEŠKEM JEZIKU
STROGO TAJNO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
TAJNO	ΑΠΟΡΡΗΤΟ	SECRET

ZAUPNO	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
INTERNO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

5. ČLEN
DOSTOP DO TAJNIH PODATKOV

(1) Dostop do tajnih podatkov je dovoljen samo tistim posameznikom, ki imajo potrebo po seznanitvi, so bili poučeni o ravnanju s tajnimi podatki in njihovem varovanju ter so za to pravilno pooblaščeni v skladu z notranjo zakonodajo.

(2) Pogodbenici medsebojno priznavata dovoljenja za dostop do tajnih podatkov in varnostna dovoljenja organizacij. Pri tem se uporablja drugi odstavek 4. člena.

6. ČLEN
VAROVANJE TAJNIH PODATKOV

(1) Pogodbenici zagotavljata za tajne podatke iz tega sporazuma enako varovanje kot za svoje tajne podatke enakovredne stopnje tajnosti.

(2) Pristojni varnostni organ pogodbenice izvora:

a) zagotovi, da so tajni podatki označeni z ustrezno stopnjo tajnosti v skladu z njegovo notranjo zakonodajo, in

b) obvesti pogodbenico prejemnico o vseh pogojih za dajanje tajnih podatkov ali omejitvah njihove uporabe in o vseh poznejših spremembah stopnje tajnosti.

(3) Pristojni varnostni organ pogodbenice prejemnice:

a) zagotovi, da so tajni podatki označeni z enakovrednimi stopnjami tajnosti v skladu z drugim odstavkom 4. člena, in

b) zagotovi, da se stopnja tajnosti ne spremeni brez predhodnega pisnega dovoljenja pogodbenice izvora.

(4) Vsaka pogodbenica zagotovi, da se sprejmejo ustrezni ukrepi za varovanje tajnih podatkov, ki se obdelujejo, hranijo ali prenašajo v informacijsko-komunikacijskih sistemih. S temi ukrepi se zagotovijo zaupnost, celovitost, razpoložljivost, in kadar je primerno, nezatajljivost in verodostojnost tajnih podatkov ter ustrezna raven odgovornosti in sledljivosti dejanj, povezanih s takimi podatki.

7. ČLEN
OMEJITEV UPORABE TAJNIH PODATKOV

(1) Pogodbenica prejemnica tajne podatke uporabi izključno za namen, za katerega so ji bili dani, in v skladu z omejitvami, ki jih je navedla pogodbenica izvora.

(2) Pogodbenica prejemnica ne daje tajnih podatkov tretji strani brez predhodnega pisnega soglasja pogodbenice izvora.

8. ČLEN
PRENOS TAJNIH PODATKOV

(1) Prenos tajnih podatkov med pogodbenicama poteka po diplomatski poti ali po drugih varnih poteh, ki jih obojestransko odobrita njuna nacionalna varnostna organa v skladu z notranjo zakonodajo.

(2) Prenos tajnih podatkov stopnje INTERNO lahko poteka tudi po pošti ali prek druge dostavne službe v skladu z notranjo zakonodajo.

9. ČLEN
RAZMNOŽEVANJE, PREVAJANJE IN UNIČENJE TAJNIH PODATKOV

(1) Vse kopije in prevodi imajo ustrezno stopnjo tajnosti ter se varujejo enako kot tajni podatki v izvirniku. Prevodi in število kopij so omejeni na najmanjšo količino, ki je potrebna za uradne namene.

(2) Vsak prevod se označi s stopnjo tajnosti tajnih podatkov v izvirniku in vsebuje ustrezno navedbo v jeziku prevoda, da vsebuje tajne podatke pogodbenice izvora.

(3) Tajni podatki v izvirniku in prevodu z oznako stopnje STROGO TAJNO se razmnožujejo izključno s pisnim dovoljenjem pogodbenice izvora.

(4) Tajni podatki z oznako stopnje STROGO TAJNO se ne uničijo. Ko niso več potrebni, se vrnejo pogodbenici izvora.

(5) Tajne podatke stopnje TAJNO ali nižje stopnje pogodbenica prejemnica, ko jih ne potrebuje več, uniči v skladu z notranjo zakonodajo.

(6) Če v kriznih razmerah tajnih podatkov, ki se prenesejo ali nastanejo po tem sporazumu, ni mogoče varovati ali vrniti, se ti takoj uničijo. O njihovem uničenju pogodbenica prejemnica čim prej uradno obvesti nacionalni varnostni organ pogodbenice izvora.

10. ČLEN
POGODBE S TAJNIMI PODATKI

(1) Nacionalni varnostni organ pogodbenice prejemnice zagotovi, da se tajni podatki v zvezi s pogodbo s tajnimi podatki dajo izvajalcem, podizvajalcem ali morebitnim izvajalcem, potem ko:

a) se zagotovi, da so izvajalec, podizvajalec ali morebitni izvajalec in njegove organizacije zmožni tajne podatke ustrezno varovati;

b) se izda organizacijam ustrezno varnostno dovoljenje in

c) imajo osebe, ki opravljajo naloge, pri katerih je potreben dostop do tajnih podatkov, ustrezno dovoljenje za dostop do tajnih podatkov.

(2) Pogodbenica prejemnica zagotovi, da so vse osebe, ki imajo dostop do tajnih podatkov, seznanjene s svojo odgovornostjo in dolžnostmi glede varovanja tajnih podatkov v skladu z notranjo zakonodajo.

(3) Nacionalni varnostni organ pogodbenice izvora lahko zahteva inšpekcijski pregled varovanja tajnih podatkov v organizaciji, da se zagotovi stalno izpolnjevanje varnostnih standardov v skladu z notranjo zakonodajo.

(4) Pogodba s tajnimi podatki vsebuje določbe o varnostnih zahtevah in stopnji tajnosti vsakega njenega vidika ali dela. Kopija takega dokumenta se predloži nacionalnima varnostnima organoma pogodbenic.

11. ČLEN
OBISKI

(1) Obiski, pri katerih je potreben dostop do tajnih podatkov, se odobrijo na podlagi predhodnega dovoljenja nacionalnega varnostnega organa pogodbenice gostiteljice.

(2) Zaprosilo za obisk se predloži pristojnemu nacionalnemu varnostnemu organu vsaj 30 dni pred začetkom obiska. Zaprosilo za obisk vsebuje naslednje podatke, ki se uporabljajo izključno za namen obiska:

a) ime in priimek obiskovalca, datum in kraj rojstva, državljanstvo in številko osebne izkaznice ali potnega lista;

b) delovno mesto obiskovalca s podatki o delodajalcu, ki ga obiskovalec zastopa;

c) podatke o projektu, pri katerem obiskovalec sodeluje;

d) veljavnost in stopnjo tajnosti obiskovalčevega dovoljenja za dostop do tajnih podatkov, če je potrebno;

e) ime, naslov, telefonsko številko/številko telefaksa in elektronski naslov organizacije, v kateri bo obisk, ter ime osebe za stike v tej organizaciji;

f) namen obiska, vključno z najvišjo stopnjo tajnosti obravnavanih tajnih podatkov;

g) datum in trajanje obiska. Pri večkratnih obiskih se navede celotno obdobje, v katerem bodo potekali;

h) datum in podpis nacionalnega varnostnega organa pošiljatelja.

(3) V nujnih primerih se nacionalna varnostna organa lahko dogovorita o krajšem obdobju za predložitev zaprosila za obisk.

(4) Nacionalna varnostna organa se lahko dogovorita o seznamu obiskovalcev, ki imajo pravico do večkratnih obiskov. Seznam velja za začetno obdobje, ki ni daljše od 12 mesecev in se lahko podaljša za nadaljnje obdobje, ki ni daljše od 12 mesecev. Zaprosilo za večkratne obiske se

predloži v skladu z drugim odstavkom tega člena. Ko je seznam potrjen, se sodelujoče organizacije o obiskih lahko dogovarjajo neposredno.

(5) Vsaka pogodbenica zagotavlja varstvo osebnih podatkov obiskovalcev v skladu z notranjo zakonodajo.

(6) Vsi tajni podatki, ki jih dobi obiskovalec, veljajo za tajne podatke po tem sporazumu.

12. ČLEN
SODELOVANJE PRI VAROVANJU TAJNIH PODATKOV

(1) Zaradi doseganja in ohranjanja primerljivih varnostnih standardov nacionalna varnostna organa na zaprosilo drug drugemu zagotovita informacije o svojih državnih varnostnih standardih, postopkih in praksah za varovanje tajnih podatkov. V ta namen se nacionalna varnostna organa lahko obiskujeta.

(2) Pristojni varnostni organi se obveščajo o izjemnih varnostnih tveganjih, ki lahko ogrozijo dane tajne podatke ali sisteme za varovanje tajnih podatkov.

(3) Nacionalna varnostna organa si na zaprosilo pomagata pri izvajanju postopkov varnostnega preverjanja. Izmenjata si podatke o morebitnih varnostnih zadržkih, pomembnih v postopku varnostnega preverjanja.

(4) Nacionalna varnostna organa se takoj obvestita o vsaki spremembi pri dovoljenjih za dostop do tajnih podatkov in varnostnih dovoljenjih organizacij.

13. ČLEN
KRŠITEV VAROVANJA TAJNOSTI

(1) Ob kršitvi varovanja tajnosti, katere posledica je nepooblaščeno razkritje, odtujitev ali izguba tajnih podatkov, ali sumu take kršitve nacionalni varnostni organ pogodbenice prejemnice o tem takoj pisno obvesti nacionalni varnostni organ pogodbenice izvora.

(2) Pristojni organi pogodbenice prejemnice sprejmejo vse ustrezne ukrepe v skladu z notranjo zakonodajo, da omejijo posledice kršitve iz prvega odstavka tega člena in preprečijo nadaljnje kršitve. Na zaprosilo druga pogodbenica zagotovi ustrezno pomoč; obvesti se o izidu postopkov in ukrepih, sprejetih zaradi kršitve.

(3) Ob kršitvi varovanja tajnosti v tretji strani nacionalni varnostni organ pogodbenice pošiljateljice nemudoma sprejme ukrepe iz drugega odstavka tega člena.

14. ČLEN
STROŠKI

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

15. ČLEN
REŠEVANJE SPOROV

Spore zaradi razlage ali uporabe tega sporazuma pogodbenici rešujeta z medsebojnimi posvetovanji in pogajanji ter jih ne predložita v reševanje državnemu ali mednarodnemu sodišču ali tretji strani.

16. ČLEN
KONČNE DOLOČBE

(1) Sporazum začne veljati prvi dan drugega meseca po prejemu zadnjega uradnega obvestila, s katerim se pogodbenici po diplomatski poti obvestita, da so izpolnjene njune notranjepravne zahteve za začetek njegove veljavnosti.

(2) Sporazum se lahko spremeni z medsebojnim pisnim soglasjem pogodbenic. Spremembe začnejo veljati v skladu s prvim odstavkom tega člena.

(3) Sporazum se sklene za nedoločen čas. Pogodbenica ga lahko odpove s pisnim uradnim obvestilom, poslanim po diplomatski poti drugi pogodbenici. V tem primeru sporazum preneha veljati šest mesecev po dnevu, ko druga pogodbenica prejme obvestilo o odpovedi.

(4) Ob prenehanju veljavnosti tega sporazuma se vsi tajni podatki, izmenjani na podlagi tega sporazuma, še naprej varujejo v skladu z njegovimi določbami in se na zaprosilo vrnejo pogodbenici izvora.

(5) Za izvajanje tega sporazuma se lahko sklenejo dodatni dogovori.

V potrditev tega sta podpisana, ki sta bila za to pravilno pooblaščena, podpisala ta sporazum.

Sklenjeno v Atenah 4. oktobra 2021 v dveh izvirnikih v slovenskem, grškem in angleškem jeziku, pri čemer so vsa besedila enako verodostojna. Ob različnih razlagah prevlada angleško besedilo.

Za Vlado **Republike Slovenije**	**Za Vlado** **Helenske republike**
N.E. Matjaž Longar l.r.	Generalmajor Dimitrios Choupis l.r.

AGREEMENT
BETWEEN
THE GOVERNMENT OF
THE REPUBLIC OF SLOVENIA
AND
THE GOVERNMENT OF
THE HELLENIC REPUBLIC
ON MUTUAL PROTECTION
OF EXCHANGED CLASSIFIED INFORMATION

The Government of the Republic of Slovenia

and

the Government of the Hellenic Republic

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,

In respect of the national interests and security of the Contracting States,

Have agreed as follows:

ARTICLE 1
OBJECTIVE

The Parties shall, in accordance with their respective laws and regulations, take all appropriate measures to ensure the protection of Classified Information which is transmitted or generated under this Agreement.

ARTICLE 2
DEFINITIONS

For the purposes of this Agreement, the following definitions shall apply:

Classified Information: any information, regardless of its form, which is transmitted or generated between the Parties under the national laws and regulations of either Party, and which, in the interests of national security, requires protection against unauthorised disclosure or other compromise, and is designated as such and marked appropriately;

Originating Party: the Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party;

Recipient Party: the Party, including any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party;

Need-to-Know: a principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties or tasks;

Personnel Security Clearance: a determination, following a security clearance process in accordance with national laws and regulations, on the basis of which an individual is authorised to access to and handle Classified Information up to the level defined in the clearance;

Facility Security Clearance: a determination following a security clearance process certifying that a contractor which is a legal entity fulfils the conditions to handle Classified Information in accordance with the national laws and regulations of the respective Party;

Contractor: an individual or legal entity possessing the legal capacity to conclude contracts;

Classified Contract: a contract or a subcontract, including pre-contractual negotiations, which contains Classified Information or involves access to such information;

Third Party: any state, including any public or private entity under its jurisdiction, or an international organisation that is not a Party to this Agreement.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

(1) The National Security Authorities designated by the Parties as responsible for the general implementation of this Agreement are:

In the Republic of Slovenia:
The Office of the Government of the Republic of Slovenia for the Protection of Classified Information (NSA),

In the Hellenic Republic:
National Security Authority (NSA), Hellenic National Defence General Staff (HNDGS), Joint Military Intelligence Division (JMID).

(2) The National Security Authorities shall notify each other of any other competent security authorities responsible for the implementation of this Agreement.

(3) The Parties shall notify each other, through diplomatic channels, of any subsequent changes to their respective National Security Authorities.

ARTICLE 4
SECURITY CLASSIFICATION LEVELS

(1) Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws and regulations of the Parties.

(2) The following security classification levels shall be equivalent:

IN THE REPUBLIC OF SLOVENIA	IN THE HELLENIC REPUBLIC	IN THE ENGLISH LANGUAGE

STROGO TAJNO	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
TAJNO	ΑΠΟΡΡΗΤΟ	SECRET
ZAUPNO	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
INTERNO	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

(1) Access to Classified Information shall be limited to individuals who have a Need-to-Know, who have been briefed on handling and protecting Classified Information, and who are duly authorised thereto in accordance with national laws and regulations.

(2) The Parties shall mutually recognise their Personnel Security Clearances and Facility Security Clearances. The second paragraph of Article 4 shall apply accordingly.

ARTICLE 6
PROTECTION OF CLASSIFIED INFORMATION

(1) The Parties shall afford to Classified Information under this Agreement the same protection as to their own Classified Information with the corresponding security classification level.

(2) The competent security authority of the Originating Party shall:

a) ensure that Classified Information is marked with an appropriate security classification level in accordance with its national laws and regulations, and

b) inform the Recipient Party of any conditions of release or limitations on the use of Classified Information, and of any subsequent changes in security classification level.

(3) The competent security authority of the Recipient Party shall:

a) ensure that Classified Information is marked with an equivalent level of security classification in accordance with the second paragraph of Article 4, and

b) ensure that the security classification level is not changed without a prior written authorization by the Originating Party.

(4) Each Party shall ensure that appropriate measures are taken to protect 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.

ARTICLE 7
RESTRICTION ON THE USE OF CLASSIFIED INFORMATION

(1) The Recipient Party shall use Classified Information solely for the purpose for which it has been released and within the limitations stated by the Originating Party.

(2) The Recipient Party shall not release Classified Information to a Third Party without a prior written consent from the Originating Party.

ARTICLE 8
TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified Information shall be transmitted between the Parties through diplomatic channels or through other secure channels mutually approved by their National Security Authorities in accordance with national laws and regulations.

(2) Classified Information at the RESTRICTED level may also be transmitted by post or another delivery service in accordance with national laws and regulations.

ARTICLE 9
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) All reproductions and translations shall bear appropriate security classification levels and shall be protected in the same way as the original Classified Information. Translations and the number of reproductions shall be limited to the minimum amount required for official purposes.

(2) All translations shall be marked with the security classification level of the original Classified Information, and shall contain suitable annotation in the language of translation indicating that they contain Classified Information of the Originating Party.

(3) Classified Information marked with the TOP SECRET level, both the original and translation, shall be reproduced only upon the written permission of the Originating Party.

(4) Classified Information marked with the TOP SECRET level shall not be destroyed. When no longer required, it shall be returned to the Originating Party.

(5) Classified Information at the SECRET level or below shall be destroyed when it is no longer considered necessary by the Recipient Party, in accordance with national laws and regulations.

(6) If a crisis situation makes it impossible to protect or return Classified Information transmitted or generated under this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall notify the National Security Authority of the Originating Party of its destruction as soon as possible.

ARTICLE 10
CLASSIFIED CONTRACTS

(1) The National Security Authority of the Recipient Party shall ensure that Classified Information related to a Classified Contract is released to Contractors, subcontractors or prospective contractors after:

a) it has been ensured that the Contractor, subcontractor or prospective contractor and its facilities are able to provide suitable protection for the Classified Information;

b) the facilities have an appropriate Facility Security Clearance and
c) persons who perform functions which require access to Classified Information have appropriate Personnel Security Clearance.

(2) The Recipient Party shall ensure that all persons having access to Classified Information are informed of their responsibilities and obligation to protect the Classified Information in accordance with national laws and regulations.

(3) The National Security Authority of the Originating Party may request that a security inspection regarding the protection of Classified Information be undertaken at a facility to ensure continuing compliance with security standards in accordance with national laws and regulations.

(4) A Classified Contract shall contain provisions on the security requirements and on the security classification level of each aspect or element of the Classified Contract. A copy of such document shall be submitted to the National Security Authorities of the Parties.

ARTICLE 11
VISITS

(1) Visits requiring access to Classified Information shall be subject to the prior authorisation of the National Security Authority of the host Party.

(2) A request for visit shall be submitted to the competent National Security Authority at least 30 days prior to the commencement of the visit. The request for visit shall include the following information, which shall be used only for the purpose of the visit:

a) first and last name of the visitor, date and place of birth, nationality and identity card/passport number;

b) position of the visitor, with a specification of the employer that the visitor represents;

c) a specification of the project in which the visitor is a participant;

d) the validity and classification level of the visitor's Personnel Security Clearance, if required;

e) name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;

f) the purpose of the visit, including the highest security classification level of Classified Information to be involved;

g) the date and duration of the visit. In the case of recurring visits, the total period covered by the visits shall be stated;

h) date and signature of the sending National Security Authority.

(3) In urgent cases, the National Security Authorities may agree on a shorter period for the submission of a request for visit.

(4) The National Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding 12 months and may be extended for a further period not exceeding 12 months. The request for recurring visits shall be submitted in accordance with the second paragraph of this Article. Once a list has been approved, visits may be arranged directly between the facilities involved.

(5) Each Party shall guarantee the protection of personal data of visitors in accordance with national laws and regulations.

(6) Any Classified Information acquired by a visitor shall be considered as Classified Information under this Agreement.

ARTICLE 12
CO-OPERATION ON THE PROTECTION OF CLASSIFIED INFORMATION

(1) In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. For this purpose, the National Security Authorities may visit each other.

(2) The competent security authorities shall inform each other of exceptional security risks that may endanger released Classified Information or Classified Information protection systems.

(3) On request, the National Security Authorities shall assist each other in carrying out a security clearance process. They shall exchange information on possible security concerns that are of importance in the security clearance process.

(4) The National Security Authorities shall promptly inform each other about any changes in Personnel and Facility Security Clearances.

ARTICLE 13
BREACH OF SECURITY

(1) In the event of a security breach resulting in the unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a breach, the National Security Authority of the Recipient Party shall immediately inform the National Security Authority of the Originating Party thereof in writing.

(2) The competent authorities of the Recipient Party shall take all appropriate measures under its national laws and regulations to limit the consequences of the breach referred to in the first paragraph of this Article and to prevent further breaches. On request, the other Party shall provide appropriate assistance; it shall be informed of the outcome of the proceedings and measures taken due to the breach.

(3) When a breach of security has occurred in a Third Party, the National Security Authority of the sending Party shall take the measures referred to in the second paragraph of this Article without delay.

ARTICLE 14
EXPENSES

Each Contracting Party shall bear its own costs incurred in the course of implementing this Agreement.

ARTICLE 15
RESOLUTION OF DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultation and negotiation between the Parties and shall not be referred to any national or international tribunal or Third Party for settlement.

ARTICLE 16
FINAL PROVISIONS

(1) This Agreement shall enter into force on the first day of the second month following the receipt of the last notification with which the Parties inform each other, through diplomatic channels, that the internal legal requirements for its entry into force have been fulfilled.

(2) This Agreement may be amended by the mutual, written consent of the Parties. Such amendments shall enter into force in accordance with the first paragraph of this Article.

(3) This Agreement shall be concluded for an indefinite period. Either Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels. In such a case, the validity of this Agreement shall expire six months after the day on which the other Party received notice of termination.

(4) In the event of termination of this Agreement, any Classified Information exchanged in accordance with this Agreement shall continue to be protected in accordance with the provisions set forth herein and, on request, returned to the Originating Party.

(5) Additional arrangements may be concluded for the implementation of this Agreement.

In witness whereof, the undersigned, duly authorised to this effect, have signed this Agreement.

Done at Athens on 4 October 2021 in two originals in the Slovenian, Greek, and English languages, each text being equally authentic. In case of divergence of interpretation, the English text shall prevail.

For the Government of the Republic of Slovenia	**For the Government of the Hellenic Republic**

H.E. Matjaž Longar (s)

Major General Dimitrios Choupis (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 na 16. redni seji dne 24. 1. 2019 sprejela Pobudo za sklenitev Sporazuma med Vlado Republike Slovenije in Vlado Helenske republike o medsebojnem varovanju izmenjanih tajnih podatkov. Odbor za zunanjo politiko Državnega zbora je pobudo potrdil dne 20. 3. 2019.

S sklenitvijo bilateralnega sporazuma o izmenjavi in medsebojnem varovanju tajnih podatkov se ustvarja pravna podlaga za izvajanje nalog državnih organov in poslovanje gospodarskih subjektov, ki pri svojem delu izmenjujejo tajne podatke na različnih področjih bilateralnega sodelovanja.

V sporazumu je po opredelitvi namena in uporabe sporazuma opisan pomen izrazov, ki se uporabljajo v besedilu: kršitev varovanja tajnosti, pogodba s tajnimi podatki, tajni podatek, izvajalec, varnostno dovoljenje organizacije, potreba po seznanitvi, pogodbenica izvora, dovoljenje za dostop do tajnih podatkov, pogodbenica prejemnica in tretja stran. Sporazum določa pristojna varnostna organa, dolžnost obveščanja o drugih pristojnih varnostnih organih in njihovi spremembi. V nadaljevanju sporazum določa razvrstitev tajnih podatkov po stopnji tajnosti in primerljivosti klasifikacij v Republiki Sloveniji in Helenski republiki v slovenskem, grškem in angleškem jeziku. Dostop do tajnih podatkov je dovoljen le tistim posameznikom, za katere velja načelo potrebe po seznanitvi ter so za to pravilno pooblaščeni v skladu z notranjimi zakoni in predpisi.

Določena so načela varovanja izmenjanih tajnih podatkov. Sporazum predpisuje, da pogodbenici zagotavljata prejetim tajnim podatkom enako raven varovanja kakor svojim lastnim tajnim podatkom enakovredne stopnje tajnosti. Določeno je tudi varovanje tajnih podatkov v komunikacijsko-informacijskih sistemih. Pogodbenici si medsebojno priznavata dovoljenja za dostop do tajnih podatkov in varnostna dovoljenja organizacij. Opredeljeni so postopki in ravnanje pri pogodbah s tajnimi podatki. Pogodbenici morata zagotoviti, da se tajni podatki posredujejo izvajalcu šele takrat, ko se zagotovi, da je izvajalec zmožen podatke ustrezno varovati, kar pomeni, da ima organizacija ustrezno varnostno dovoljenje, da imajo osebe, ki opravljajo dolžnosti, pri katerih je potreben dostop do tajnih podatkov, ustrezno dovoljenje za dostop do tajnih podatkov in so vse osebe, ki imajo dostop do tajnih podatkov, seznanjene s svojo odgovornostjo za varovanje podatkov in dolžnostjo njihovega varovanja v skladu z ustreznimi zakoni in predpisi pogodbenice prejemnice. Tajni podatki se prenašajo med pogodbenicama po diplomatskih ali po drugih varnih poteh, ki jih obojestransko dogovorita njuna nacionalna varnostna organa. Določena so pravila za razmnoževanje, prevajanje in uničevanje tajnih podatkov. Vsi izvodi in prevodi so označeni z ustrezno oznako stopnje tajnosti in so varovani kot tajni podatki izvirnika. Za obiske med pogodbenicama, ki vključujejo dostop do tajnih podatkov, je potrebno predhodno dovoljenje nacionalnega varnostnega organa gostiteljice. Zaradi doseganja in ohranjanja primerljivih varnostnih standardov nacionalna varnostna organa na podlagi zaprosila drug drugemu zagotovita informacije o svojih nacionalnih varnostnih standardih, postopkih in praksah za varovanje tajnih podatkov. Na podlagi zaprosila si nacionalna varnostna organa pomagata pri izvajanju postopkov varnostnega preverjanja. Ob kršitvi varovanja tajnosti nacionalni varnostni organ, v državi katerega se je pojavila kršitev varovanja tajnosti, o tem čim prej pisno obvesti nacionalni varnostni organ druge pogodbenice in zagotovi sprejem vseh ukrepov v skladu z notranjimi zakoni in predpisi, da omeji posledice kršitve. Vsaka pogodbenica krije svoje stroške, ki nastanejo pri izvajanju tega sporazuma. Spore glede razlage ali uporabe tega sporazuma pogodbenici rešujeta z medsebojnimi posvetovanji in pogajanji. Sporazum se sklene za nedoločen čas. Veljati začne prvi dan drugega meseca po prejemu zadnjega uradnega obvestila, s katerim se pogodbenici po diplomatski poti obvestita, da so izpolnjene njune notranjepravne zahteve, potrebne za začetek veljavnosti tega sporazuma.

Sporazum med Vlado Republike Slovenije in Vlado Helenske republike o medsebojnem varovanju izmenjanih tajnih podatkov je bil podpisan 4. oktobra 2021 v Atenah.

V skladu s četrtim odstavkom 75. člena Zakona o zunanjih zadevah (Uradni list RS, št. 113/03 – uradno prečiščeno besedilo, 20/06 – ZNOMCMO, 76/08, 108/09, 80/10 – ZUTD, 31/15 in 30/18 – ZKZaš) 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 veljavnih ali sprejemati novih predpisov.

Sporazum ni predmet usklajevanja s pravnim redom Evropske unije.

Uresničevanje sporazuma neposredno ne zahteva posebnih finančnih sredstev.