ACCORDO
TRA
IL GOVERNO DELLA REPUBBLICA ITALIANA
E
IL GOVERNO DELLA REPUBBLICA DI SLOVENIA
PER LO SCAMBIO E LA RECIPROCA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

Il Governo della Repubblica Italiana e il Governo della Repubblica di Slovenia (qui di seguito denominate "le Parti"),

Desiderando assicurare la protezione delle Informazioni Classificate scambiate tra le Parti o tra entità pubbliche o private sotto la loro giurisdizione, in accordo con le leggi ed i regolamenti nazionali.

Riconoscendo l'esigenza di concordare regole di sicurezza comuni per la protezione delle Informazioni Classificate, anche in relazione alla possibilità di attuare accordi di cooperazione tecnica e di sviluppare attività contrattuali tra le Parti,

hanno concordato quanto segue:

Articolo 1
Scopo

Entrambe le parti, in conformità con le leggi ed i regolamenti nazionali e nel rispetto degli interessi nazionali e di sicurezza, intraprendono tutte le misure appropriate per assicurare la protezione delle informazioni classificate scambiate o prodotte in ottemperanza all'Accordo.

Articolo 2
Definizioni

Per gli scopi di questo Accordo, i seguenti termini significano:

a) **Informazione Classificata**: ogni informazione, a prescindere dalla sua forma, trasmessa o generata tra le Parti, cui è stata assegnata una classifica di segretezza in conformità con le leggi ed i regolamenti delle Parti;

b) **Parte Originatrice:** la Parte, inclusa anche ogni entità pubblica o privata sotto la sua giurisdizione, che cede Informazioni Classificate alla Parte Ricevente;

c) **Parte Ricevente:** la Parte, inclusa anche ogni entità pubblica o privata sotto la sua giurisdizione, che riceve Informazioni Classificate dalla Parte Originatrice;

d) **Necessità di conoscere**: il principio secondo il quale un individuo è autorizzato ad accedere alle Informazioni Classificate solamente in relazione al proprio incarico ed alle proprie funzioni ufficiali;

e) **Certificato di Abilitazione di Sicurezza Personale:** una determinazione positiva adottata all'esito di controlli in conformità con le leggi ed i regolamenti nazionali, sulla base della quale una persona è autorizzata a trattare Informazioni Classificate fino al livello indicato nel provvedimento;

f) **Certificato di Abilitazione di Sicurezza industriale**: una determinazione positiva adottata all'esito di controlli, che attesta che un operatore economico con capacità giuridica soddisfa i requisiti per la trattazione delle Informazioni Classificate in conformità con le leggi ed i regolamenti di una delle Parti;

g) **Contraente**: un ente pubblico o privato in possesso della capacità giuridica di concludere contratti;

h) **Contratto Classificato**: un contratto con un contraente o un sub contraente, che contiene o implica la conoscenza di Informazioni Classificate;

i) **Parte Terza**: uno Stato, incluso anche ogni ente pubblico o privato sotto la sua giurisdizione, o un'organizzazione internazionale che non è una Parte di questo Accordo.

j) **Visite**: Accesso a enti pubblici o privati, per le finalità di quest'Accordo, che includano la gestione di Informazioni Classificate.

Articolo 3
Autorità Competenti per la Sicurezza

1) Le Autorità Nazionali per la Sicurezza, designate dalle Parti in qualità di responsabili per l'attuazione generale e per l'espletamento dei controlli pertinenti a tutti gli aspetti dell'Accordo sono:

Per la Repubblica Italiana:
Presidenza del Consiglio dei Ministri – Autorità Nazionale per la Sicurezza - Dipartimento Informazioni per la Sicurezza (DIS), UCSe.

Per la Repubblica di Slovenia:
Government Office for the Protection of Classified Information – National Security Authority

2) Le Autorità Nazionali per la Sicurezza si comunicano reciprocamente le eventuali altre Competenti Autorità di Sicurezza responsabili per l'attuazione di questo Accordo.

3) Le Parti si informano reciprocamente attraverso canali diplomatici in merito ad ogni successivo cambiamento relativo alle Autorità Nazionali per la Sicurezza.

4) Allo scopo di assicurare e mantenere uno standard di sicurezza equivalente, le Autorità Nazionali di Sicurezza, su richiesta, forniranno reciprocamente informazioni in merito agli standard di sicurezza nazionali, alle procedure, alle attività per la protezione di Informazioni Classificate. A tale scopo le Autorità Nazionali di Sicurezza potranno organizzare reciproche visite.

5) Le Autorità Competenti per la Sicurezza assicurano un severo e vincolante rispetto a questo Accordo da parte di ogni ente pubblico o privato delle Parti, in conformità con le leggi e regolamenti nazionali.

Articolo 4
Livelli di classifiche di segretezza

1) Le Informazioni Classificate rilasciate ai sensi di quest'Accordo sono identificate con il livello di segretezza appropriato in conformità con le leggi e regolamenti nazionali delle rispettive Parti.

2) I seguenti livelli di classifica di segretezza sono equivalenti:

Per la Repubblica Italiana	Per la Repubblica di Slovenia
SEGRETISSIMO	STROGO TAJNO
SEGRETO	TAJNO
RISERVATISSIMO	ZAUPNO
RISERVATO	INTERNO

Articolo 5
Principi per la protezione delle Informazioni Classificate

1) Le Parti assicurano alle Informazioni Classificate cui si riferisce quest'Accordo lo stesso livello di protezione assegnato alle proprie Informazioni Classificate con il corrispondente livello di classifica.

2) L'Autorità Competente di Sicurezza della Parte Originatrice deve:

a) assicurare all'Informazione Classificata un livello di classifica di segretezza adeguato in conformità con le proprie leggi e regolamenti nazionali, e
b) informare la Parte Ricevente di ogni condizione di rilascio o limitazione sull'uso delle Informazioni Classificate e di ogni conseguente cambiamento del livello di classifica.

3) L'Autorità Competente di Sicurezza della Parte Ricevente deve:

a) assicurare all'Informazione Classificata un livello di classifica di segretezza equivalente in conformità con le disposizioni dell'art 4, paragrafo 2 dell'Accordo, e

b) assicurare che il livello di classifica di segretezza sia cambiato solo previa autorizzazione scritta della Parte Originatrice.

c) utilizzare l'Informazione Classificata solo per gli scopi per cui è stata rilasciata e solo entro le limitazioni previste dalla Parte Originatrice.

d) non cedere Informazioni Classificate a Parti Terze senza il preventivo consenso scritto della Parte Originatrice.

Articolo 6
Accesso alle Informazioni Classificate ed alle Abilitazioni Personali di Sicurezza

1) L'accesso alle Informazioni Classificate di livello RISERVATISSIMO/ZAUPNO e superiore viene autorizzato solo a coloro che hanno Necessità di Conoscere e sono in possesso dell'Abilitazione Personale di Sicurezza di livello adeguato.

2) L'accesso alle Informazioni Classificate RISERVATO/INTERNO è limitato a persone che hanno Necessità di Conoscere e che sono state preventivamente istruite.

3) Le Parti riconosceranno vicendevolmente le Abilitazioni Personali di Sicurezza, secondo quanto previsto dal paragrafo 2 dell'Art 4.

4) A richiesta, le Autorità Nazionali per la Sicurezza, in conformità con le leggi e regolamenti nazionali, si forniranno reciproca assistenza scambiandosi dati rilevanti sulle procedure per il rilascio delle Abilitazioni di Sicurezza Personali ed Industriali.

5) Le Autorità Nazionali per la Sicurezza si informano tempestivamente sui cambiamenti relativi alle Abilitazioni di Sicurezza reciprocamente riconosciute.

Articolo 7
Protezione delle Informazioni Classificate nei Sistemi di Comunicazione e Trasmissione

1) Le Parti assicurano l'adozione di tutte le misure necessarie alla protezione delle Informazioni Classificate trattate, conservate o trasmesse mediante sistemi di comunicazione ed informazione. Tali misure devono assicurare la riservatezza, integrità, disponibilità e quando possibile, la non-disconoscibilità e l'autenticità delle Informazioni Classificate come anche un livello adeguato di contabilizzazione e tracciabilità delle azioni che interessano tali informazioni.

2) A tal fine le Parti assicurano che tali Informazioni Classificate scambiate sono conservate, trattate e protette in conformità con le rispettive leggi ed i regolamenti nazionali.

3) Le Parti riconoscono reciprocamente gli atti ufficiali di approvazione che riguardano strumenti e meccanismi impiegati per le comunicazioni ed i sistemi d'informazione, approvati dalle competenti Autorità Nazionali per la Sicurezza.

Articolo 8
Trasmissione delle Informazioni Classificate

1) Le Informazioni Classificate sono trasmesse tra le Parti attraverso canali diplomatici e altri canali sicuri approvati dalle Autorità Nazionali per la Sicurezza in conformità con le leggi ed i regolamenti nazionali.
2) Le Informazioni Classificate "SEGRETISSIMO/STROGO TAJNO" sono trasmesse solo attraverso canali diplomatici.
3) Le Informazioni Classificate "RISERVATO/INTERNO" sono trasmesse anche per posta o mediante altro servizio di consegna in conformità con le leggi ed i regolamenti nazionali.
4) In caso di consegne di rilevante quantità contenenti Informazioni Classificate, le Autorità Nazionali per la Sicurezza decidono congiuntamente ed approvano, caso per caso, le procedure del trasporto.

Articolo 9
Riproduzione, traduzione e distruzione delle Informazioni Classificate

1) Tutte le riproduzioni e le traduzioni devono essere contrassegnate in modo adeguato e protette come le Informazioni Classificate originali. Le traduzioni ed il numero di copie deve essere limitato al minimo necessario per gli scopi ufficiali.

2) Tutte le traduzioni devono essere contrassegnate con il livello originale di classifica e devono recare una appropriata annotazione, nella lingua utilizzata per la traduzione, che attesti la presenza di Informazioni Classificate della Parte Originatrice.

3) Le Informazioni Classificate di livello "SEGRETISSIMO/STROGO TAJNO", devono essere tradotte o riprodotte solo previa autorizzazione scritta della Parte Originatrice.

4) Le Informazioni Classificate di livello "SEGRETISSIMO/STROGO TAJNO" non devono essere distrutte. Le stesse devono essere riconsegnate alla Parte Originatrice quando ritenute non più necessarie dalle Parti.

5) Le Informazioni Classificate di livello SEGRETO/TAJNO o inferiore devono essere distrutte dalla Parte Ricevente in conformità con le leggi ed i regolamenti nazionali quando ritenute non più necessarie.

6) In caso di emergenza le Informazioni Classificate trasmesse o originate ai sensi di quest'Accordo, che risulta impossibile proteggere o riconsegnare, devono essere distrutte immediatamente. La Parte Ricevente deve notificare appena possibile l'avvenuta distruzione all'Autorità Nazionale per la Sicurezza della Parte Originatrice.

Articolo 10
Contratti classificati e Abilitazioni di Sicurezza Industriali

1) Prima di trasmettere Informazioni Classificate attinenti ad un Contratto Classificato a Contraenti, Sub contraenti o potenziali contraenti, la Parte Ricevente assicura che:

   a) Tali Contraenti, Subcontraenti o potenziali contraenti e le relative sedi sono in grado di proteggere adeguatamente le informazioni.

   b) Le sedi siano in possesso di un'adeguata Abilitazione di Sicurezza Industriale.

c) Tutte le persone che svolgono funzioni che implicano l'accesso ad Informazioni Classificate sono in possesso di una specifica Abilitazione di Sicurezza Personale.

d) Tutte le persone che hanno accesso ad Informazioni Classificate sono informati delle loro responsabilità ed obblighi di proteggere le informazioni in conformità con le pertinenti leggi e regolamenti della Parte Ricevente.

2) Ciascuna Autorità Nazionale per la Sicurezza può richiedere un'ispezione di sicurezza presso una struttura al fine di assicurare una permanente conformità agli standard di sicurezza in accordo con le leggi ed i regolamenti nazionali.

3) Il Contratto Classificato deve contenere specifiche disposizioni concernenti le misure di sicurezza, le classificazioni di ciascun aspetto o elemento del Contratto Classificato e specifici riferimenti a questo Accordo. Una copia di tale documento deve essere sottoposta alle Autorità Nazionali per la Sicurezza delle Parti.

4) Le Parti devono reciprocamente riconoscere le Abilitazioni di Sicurezza Industriali. A tal fine si applica il paragrafo 2 dell'art. 4.

5) Le Autorità Nazionali per la Sicurezza si informano tempestivamente in merito ad ogni cambiamento relativo alle Abilitazioni di Sicurezza Industriale reciprocamente riconosciute.

Articolo 11
Visite

1) Le visite che prevedono l'accesso ad Informazioni Classificate devono essere subordinate ad una preventiva autorizzazione dell'Autorità Nazionale per la Sicurezza della Parte dove la visita ha luogo.

2) La richiesta per visita deve essere inviata alla competente Autorità Nazionale per la Sicurezza con un anticipo di almeno 30 giorni rispetto alla data di inizio della visita. Essa deve contenere i seguenti dati e può essere utilizzata solo per la visita in parola:

a) il nome del visitatore, la data e il luogo di nascita, la nazionalità e il numero del passaporto o di un'altro documento di identificazione del visitatore;

b) la funzione del visitatore e l'indicazione del datore di lavoro che il visitatore rappresenta;

c) la specificazione del progetto cui il visitatore prende parte;

d) la validità e l'indicazione del livello di Abilitazione di Sicurezza Personale del visitatore, qualora richiesto;

e) l'indicazione della denominazione, indirizzo, numero telefonico/fax, indirizzo di posta elettronica e punto di contatto della struttura oggetto della visita;

f) lo scopo della visita, ivi incluso il più elevato livello di classifica delle Informazioni interessate;

g) la data e durata della visita. In caso di visite ricorrenti il periodo totale di durata delle stesse;

h) la data e firma dell'Autorità Nazionale per la Sicurezza inviante.

3) In casi urgenti, le Autorità Nazionali per la Sicurezza possono concordare un periodo più breve per la presentazione della richiesta di visita.

4) Le Autorità Nazionali per la Sicurezza possono accordarsi su una lista di visitatori in caso di visite ricorrenti. Tale lista è valida per un periodo iniziale non superiore a 12 mesi e la cui validità può essere estesa per un periodo non superiore ad ulteriori 12 mesi. La richiesta di visite ricorrenti può essere presentata in conformità con quanto previsto al paragrafo 2 di quest'articolo. Una volta che lista viene approvata le visite potranno essere organizzate direttamente tra i siti interessati.

5) Le Parti devono assicurare la protezione dei dati personali dei visitatori in conformità con le leggi ed i regolamenti nazionali.

Articolo 12
Violazioni alla Sicurezza

1) In caso di infrazione alla sicurezza, che comporti un accesso non autorizzato, un'appropriazione indebita, o perdita di Informazioni Classificate o il sospetto di tale violazione, l'Autorità Nazionale per la Sicurezza della Parte Ricevente deve immediatamente informare l'Autorità Nazionale per la Sicurezza della Parte Originatrice per iscritto.

2) In conformità con le proprie leggi e regolamenti nazionali, la Parte competente deve avviare tutte le misure necessarie per limitare le conseguenze della violazione come da paragrafo 1 di questo articolo e prevenire il verificarsi di nuove violazioni. Su richiesta, l'altra Parte fornisce adeguata assistenza; viene informata delle risultanze del procedimento e delle misure intraprese in seguito alla violazione.

3) Nel caso in cui la violazione alla sicurezza sia avvenuta in una Parte Terza, l'Autorità Nazionale per la Sicurezza della Parte che ha inviato l'Informazione Classificata, deve adottare, senza ritardo, le azioni previste al paragrafo 2 di questo articolo.

4) Le competenti Autorità Nazionali per la Sicurezza si scambiano informazioni circa rischi eccezionali che possano mettere in pericolo l'Informazione Classificata ceduta.

Articolo 13
Costi

1) L'attuazione di questo Accordo non prevede alcun costo.

2) Nell'eventualità che una Parte debba sostenere dei costi inattesi nel corso dell'attuazione dell'Accordo, ciascuna Parte sostiene le proprie spese.

Articolo 14
Risoluzione delle controversie

I) Ogni controversia concernente l'interpretazione o l'attuazione di questo Accordo è definita attraverso consultazioni e negoziazioni tra le Parti. Nel frattempo, le Parti continuano ad adempiere alle disposizioni non controverse previste in questo Accordo.

Articolo 15
Disposizioni finali

1) Questo Accordo entra in vigore il primo giorno del secondo mese dalla data di ricezione dell'ultima notifica scritta con la quale le Parti si sono informate, reciprocamente, attraverso canali diplomatici, che le loro procedure legali necessarie per l'entrata in vigore sono state completate.

2) Questo Accordo può essere emendato attraverso il reciproco consenso scritto tra le Parti. Gli emendamenti entrano in vigore in conformità con le disposizioni del paragrafo 1 di questo articolo.

3) Questo Accordo rimane in vigore per un periodo di tempo indeterminato. Ciascuna delle Parti può denunciare questo Accordo informando l'altra per iscritto, tramite canali diplomatici. In tal caso, questo Accordo cessa di essere in vigore sei mesi dopo la data in cui l'altra Parte ha ricevuto la notizia di denuncia.

4) In caso di conclusione della validità del presente Accordo, tutte le Informazioni Classificate trasferite sulla base di questo Accordo devono continuare ad essere protette in conformità con le disposizioni qui stabilite e, su richiesta, restituite alla Parte Originatrice.

5) Ulteriori intese possono essere concluse per l'attuazione di questo Accordo.

In fede, i sottoscritti Rappresentanti, debitamente autorizzati dai rispettivi Governi, firmano il presente Accordo.

Fatto a Lubiana il 17.12.2015 in due originali, in lingua italiana e slovena, entrambi i testi ugualmente autentici.

PER IL GOVERNO DELLA REPUBBLICA ITALIANA

Rosella Tarantini

PER IL GOVERNO DELLA REPUBBLICA DI SLOVENIA

SPORAZUM
MED
VLADO ITALIJANSKE REPUBLIKE
IN
VLADO REPUBLIKE SLOVENIJE
O IZMENJAVI IN MEDSEBOJNEM VAROVANJU
TAJNIH PODATKOV

Vlada Italijanske republike in Vlada Republike Slovenije, v nadaljevanju "pogodbenici", sta se

v želji, da bi v skladu s svojimi notranjimi zakoni in drugimi predpisi zagotovili varovanje tajnih podatkov, izmenjanih med njima ali med javnimi in zasebnimi subjekti pod njuno jurisdikcijo,

ob priznavanju potrebe po vzpostavitvi skupnih varnostnih predpisov za varovanje tajnih podatkov tudi v zvezi z morebitnim izvajanjem sporazumov o tehničnem sodelovanju in razvijanjem pogodbenih dejavnosti med pogodbenicama

dogovorili:

1. člen
Cilj

Pogodbenici v skladu s svojimi notranjimi zakoni in drugimi predpisi ter ob upoštevanju interesov in varnosti države sprejmeta vse ustrezne ukrepe, da bi zagotovili varovanje tajnih podatkov, ki se prenesejo ali nastanejo po tem sporazumu.

2. člen
Pomen izrazov

V tem sporazumu izrazi pomenijo:

a) **tajni podatek:** podatek, ki se ne glede na obliko prenese ali nastane med pogodbenicama in mu je bila v skladu z notranjimi zakoni in drugimi predpisi pogodbenic določena stopnja tajnosti;

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

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

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

e) **dovoljenje za dostop do tajnih podatkov:** pozitivna odločitev po varnostnem preverjanju v skladu z notranjimi zakoni in drugimi predpisi, na podlagi katere je posameznik pooblaščen za dostop do tajnih podatkov do stopnje tajnosti, navedene na dovoljenju, in ravnanje z njimi;

f) **varnostno dovoljenje organizacije**: pozitivna odločitev po varnostnem preverjanju, da izvajalec, ki je pravna oseba, izpolnjuje pogoje za ravnanje s tajnimi podatki v skladu z notranjimi zakoni in drugimi predpisi pogodbenice;

g) **izvajalec:** javni ali zasebni subjekt s pravno sposobnostjo za sklepanje pogodb;

h) **pogodba s tajnimi podatki:** pogodba z izvajalcem ali podizvajalcem, ki vsebuje tajne podatke ali vključuje njihovo poznavanje;

i) **tretja stran:** država, vključno z javnimi ali zasebnimi subjekti pod njeno jurisdikcijo, ali mednarodna organizacija, ki ni pogodbenica tega sporazuma;

j) **obisk:** dostop do javnih ali zasebnih subjektov za namene tega sporazuma, ki vključuje ravnanje s tajnimi podatki.

3. člen
Pristojni varnostni organi

(1) Nacionalna varnostna organa, ki sta ju pogodbenici imenovali za pristojna za splošno izvajanje tega sporazuma in ustrezen nadzor nad vsemi njegovimi vidiki, sta:

v Italijanski republiki:
Predsedstvo Sveta ministrov – nacionalni varnostni organ, Oddelek za varnost podatkov (DIS), UCSe.

v Republiki Sloveniji:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov – nacionalni varnostni organ;

(2) Nacionalna varnostna organa se uradno obveščata o drugih pristojnih varnostnih organih, odgovornih za izvajanje tega sporazuma.

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

(4) 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. V ta namen se lahko nacionalna varnostna organa obiskujeta.

(5) Pristojna varnostna organa v skladu z notranjimi zakoni in drugimi predpisi pogodbenic zagotovita, da njuni javni in zasebni subjekti dosledno in zavezujoče upoštevajo ta sporazum.

4. člen
Stopnje tajnosti

(1) Tajni podatki, dani na podlagi tega sporazuma, so označeni z ustrezno stopnjo tajnosti v skladu z notranjimi zakoni in drugimi predpisi pogodbenic.

(2) Enakovredne nacionalne oznake stopnje tajnosti so:

Italijanska republika	**Republika Slovenija**
SEGRETISSIMO	STROGO TAJNO
SEGRETO	TAJNO
RISERVATISSIMO	ZAUPNO
RISERVATO	INTERNO

5. člen
Načela varovanja tajnih podatkov

(1) Pogodbenici zagotavljata tajnim podatkom iz tega sporazuma enako varovanje kot svojim tajnim podatkom enakovredne stopnje tajnosti.

(2) Pristojni varnostni organ pogodbenice izvora:
a) zagotovi, da so tajni podatki označeni z ustrezno oznako stopnje tajnosti v skladu z njenimi notranjimi zakoni in drugimi predpisi, 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 oznakami stopnje tajnosti v skladu z drugim odstavkom 4. člena, in
b) zagotovi, da se stopnja tajnosti ne spremeni, razen s pisnim dovoljenjem pogodbenice izvora;
c) uporabi tajne podatke le za namen, za katerega so bili dani, in z omejitvami, ki jih je navedla pogodbenica izvora;
d) tajnih podatkov ne da tretji strani brez pisnega soglasja pogodbenice izvora.

6. člen
Dostop do tajnih podatkov in dovoljenja za dostop do tajnih podatkov

(1) Dostop do tajnih podatkov stopnje RISERVATISSIMO/ZAUPNO in višje stopnje je dovoljen le tistim osebam, ki imajo potrebo po seznanitvi in ustrezno dovoljenje za dostop do tajnih podatkov.

(2) Dostop do tajnih podatkov stopnje RISERVATO/INTERNO je omejen na osebe, ki imajo potrebo po seznanitvi in so bile ustrezno poučene.

(3) Pogodbenici si priznavata dovoljenja za dostop do tajnih podatkov. Pri tem se uporablja drugi odstavek 4. člena.

(4) Na podlagi zaprosila si nacionalna varnostna organa v skladu z notranjimi zakoni in drugimi predpisi pomagata z izmenjavo ustreznih podatkov o postopkih varnostnega preverjanja za izdajo dovoljenja za dostop do tajnih podatkov in varnostnega dovoljenja organizacij.

(5) Nacionalna varnostna organa se takoj obvestita o vsaki spremembi v medsebojno priznanih dovoljenjih za dostop do tajnih podatkov.

7. člen
Varovanje tajnih podatkov v komunikacijsko-informacijskih sistemih

(1) Pogodbenica zagotovi, da se izvajajo ustrezni ukrepi za varovanje tajnih podatkov, ki se obdelujejo, hranijo ali prenašajo v komunikacijsko-informacijskih 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.

(2) Pogodbenici zato zagotovita, da se s tako izmenjanimi tajnimi podatki ravna v skladu z njunimi notranjimi zakoni in drugimi predpisi ter se tako tudi hranijo in varujejo.

(3) Pogodbenici medsebojno priznavata vsak uradni dokument odobritve v zvezi z opremo in mehanizmi komunikacijsko-informacijskih sistemov, ki ga izda ustrezni nacionalni varnostni organ.

8. člen
Prenos tajnih podatkov

(1) Prenos tajnih podatkov med pogodbenicama poteka po diplomatski poti ali po drugih varnih poteh, ki jih odobrita nacionalna varnostna organa v skladu z notranjimi zakoni in drugimi predpisi.

(2) Tajni podatki stopnje SEGRETISSIMO/STROGO TAJNO se pošiljajo samo po diplomatski poti.

(3) Tajni podatki stopnje RISERVATO/INTERNO se lahko pošiljajo tudi po pošti ali z drugo dostavno službo v skladu z notranjimi zakoni in drugimi predpisi.

(4) Ob prenosu večje pošiljke s tajnimi podatki se o postopkih prevoza dogovorijo in jih odobrijo pristojni varnostni organi pogodbenic za vsak primer posebej.

9. člen
Razmnoževanje, prevajanje in uničevanje tajnih podatkov

(1) Vsi izvodi in prevodi imajo ustrezno oznako stopnje tajnosti ter se varujejo kot tajni podatki izvirnika. Prevodi in število izvodov so omejeni na najmanjšo količino, ki je potrebna za uradne namene.

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

(3) Tajni podatki izvirnika in prevoda z oznako SEGRETISSIMO/STROGO TAJNO se razmnožujejo izključno s pisnim dovoljenjem pogodbenice izvora.

(4) Tajni podatki z oznako SEGRETISSIMO/STROGO TAJNO se ne smejo uničiti. Ko jih pogodbenici ne potrebujeta več, se vrnejo pogodbenici izvora.

(5) Pogodbenica prejemnica tajne podatke stopnje SEGRETO/TAJNO ali nižje stopnje uniči v skladu s svojimi notranjimi zakoni in drugimi predpisi, ko jih ne potrebuje več.

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

10. člen
Pogodbe s tajnimi podatki in varnostna dovoljenja organizacij

(1) Preden se tajni podatki iz pogodbe s tajnimi podatki dajo izvajalcem, podizvajalcem ali morebitnemu izvajalcu, pogodbenica prejemnica zagotovi, da:

a) so izvajalec, podizvajalec ali morebitni izvajalec in njihove organizacije zmožni podatke ustrezno varovati;

b) ima organizacija ustrezno varnostno dovoljenje;

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

d) so vse osebe, ki imajo dostop do tajnih podatkov, obveščene o svoji odgovornosti in obveznosti varovanja podatkov v skladu z zakoni in drugimi predpisi pogodbenice prejemnice.

(2) Nacionalni varnostni organ lahko zahteva inšpekcijski pregled organizacije, da se zagotovi stalno izpolnjevanje varnostnih standardov v skladu z notranjimi zakoni in drugimi predpisi.

(3) Pogodba s tajnimi podatki vsebuje določbe o varnostnih zahtevah, stopnji tajnosti vsakega njenega vidika ali dela in sklicevanju na ta sporazum. Izvod takega dokumenta se predloži nacionalnima varnostnima organoma pogodbenic.

(4) Pogodbenici si priznavata varnostna dovoljenja organizacij. Pri tem se uporablja drugi odstavek 4. člena.

(5) Nacionalna varnostna organa se takoj obvestita o vsaki spremembi v medsebojno priznanih varnostnih dovoljenjih organizacij.

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 ustreznemu nacionalnemu varnostnemu organu vsaj 30 dni pred začetkom obiska. Zaprosilo za obisk vsebuje te 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) položaj 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, elektronski naslov organizacije, v kateri bo obisk, in osebo 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 lahko nacionalna varnostna organa 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 največ 12 mesecev. Zaprosilo za večkratne obiske se predloži v skladu z drugim odstavkom tega člena. Ko je seznam potrjen, se lahko sodelujoče organizacije o obiskih dogovarjajo neposredno.

(5) Pogodbenica zagotavlja varstvo osebnih podatkov obiskovalcev v skladu z notranjimi zakoni in drugimi predpisi.

12. 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 sprejmejo vse ukrepe v skladu z notranjimi zakoni in drugimi predpisi, da omejijo posledice kršitve iz prvega odstavka tega člena in preprečijo nadaljnje kršitve. Na podlagi zaprosila druga pogodbenica zagotovi ustrezno pomoč; obvesti se o izidu postopkov in ukrepih, sprejetih zaradi kršitve.

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

(4) Pristojni varnostni organi se obveščajo o izjemnih varnostnih tveganjih, ki lahko ogrozijo dane tajne podatke.

13. člen
Stroški

(1) Izvajanje tega sporazuma ne vključuje nobenih stroškov.

(2) Če pri izvajanju tega sporazuma nastanejo pri pogodbenici nepričakovani stroški, vsaka pogodbenica krije svoje izdatke.

14. člen
Reševanje sporov

Spore zaradi razlage ali uporabe tega sporazuma pogodbenici rešujeta s posvetovanji in pogajanji. Medtem pa pogodbenici še naprej izpolnjujeta nesporne določbe tega sporazuma.

15. člen
Končne določbe

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

(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 obvestilom, ki ga po diplomatski poti pošlje 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, preneseni v skladu s tem sporazumom, še naprej varujejo v skladu z njegovimi določbami in se na podlagi zaprosila vmejo pogodbenici izvora.

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

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

Sklenjeno v Ljubljani 17. 12. 2015 v dveh izvirnikih v italijanskem in slovenskem jeziku, pri čemer sta besedili enako verodostojni.

ZA VLADO
ITALIJANSKE REPUBLIKE

Rosella Franchini

ZA VLADO
REPUBLIKE SLOVENIJE