SPORAZUM

MED

REPUBLIKO SLOVENIJO

IN

KRALJEVINO ŠPANIJO

O

IZMENJAVI IN MEDSEBOJNEM VAROVANJU

TAJNIH PODATKOV

Republika Slovenija

in

Kraljevina Španija,

v nadaljevanju "pogodbenici",

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

dogovorili:

1. ČLEN
CILJ

Pogodbenici v skladu s svojo notranjo zakonodajo ter ob upoštevanju državnih interesov in nacionalne varnosti sprejmeta vse ustrezne ukrepe, da bi zagotovili varovanje tajnih podatkov, ki se prenesejo ali nastanejo po tem sporazumu.

2. ČLEN
PODROČJE UPORABE

(1) Ta sporazum določa postopke za varovanje tajnih podatkov, ki jih izmenjujeta pogodbenici.

(2) Pogodbenica se ne more sklicevati na ta sporazum, da bi pridobila tajne podatke, ki jih je druga pogodbenica prejela od tretje strani.

3. ČLEN
POMEN IZRAZOV

V tem sporazumu izrazi pomenijo:

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

tajni podatek: podatek, ki se ne glede na obliko prenese ali nastane med pogodbenicama po notranji zakonodaji pogodbenice in ga je treba v interesu nacionalne varnosti varovati pred nepooblaščenim razkritjem ali drugim ogrožanjem ter ga je pogodbenica določila za takega in ustrezno označila;

izvajalec: pravna oseba s pravno sposobnostjo za sklepanje pogodb;

varnostno dovoljenje organizacije: pozitivna odločitev pristojnega varnostnega organa, da z varnostnega vidika izvajalec lahko ravna s tajnimi podatki v skladu z notranjo zakonodajo;

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

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

dovoljenje za dostop do tajnih podatkov: pozitivna odločitev po varnostnem preverjanju, opravljenem v skladu z notranjo zakonodajo, na podlagi katere ima posameznik pravico do dostopa do tajnih podatkov do stopnje tajnosti, ki je navedena na dovoljenju, in za ravnanje z njimi;

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

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

4. ČLEN

PRISTOJNI VARNOSTNI ORGANI

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

v Republiki Sloveniji:

Urad Vlade Republike Slovenije za varovanje tajnih podatkov;

v Kraljevini Španiji:

Secretario de Estado Director del Centro Nacional de Inteligencia,
Oficina Nacional de Seguridad.

(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.

5. ČLEN

STOPNJE TAJNOSTI

(1) Tajni podatki, dani na podlagi tega sporazuma, so označeni z ustreznimi stopnjami tajnosti v skladu z notranjo zakonodajo.

(2) Enakovredne oznake stopnje tajnosti so:

Republika Slovenija	Kraljevina Španija
STROGO TAJNO	SECRETO
TAJNO	RESERVADO
ZAUPNO	CONFIDENCIAL
INTERNO	DIFUSIÓN LIMITADA

(3) Stopnja tajnosti podatkov, ki nastanejo pri medsebojnem sodelovanju pogodbenic, se določi, spremeni ali zniža samo z medsebojnim soglasjem. Če med pogodbenicama ni soglasja glede stopnje tajnosti, ki naj bi se določila za take podatke, sprejmeta predlagano višjo stopnjo tajnosti.

6. 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 5. člena.

7. ČLEN

VAROVANJE 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 njeno notranjo zakonodajo, in
b) obvesti pogodbenico prejemnico o vseh pogojih za dajanje tajnih podatkov ali omejitvah njihove uporabe ter 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 5. člena, in
b) zagotovi, da se stopnja tajnosti ne spremeni, razen s pisnim dovoljenjem pogodbenice izvora.

(4) Pogodbenica zagotovi, da se izvajajo 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.

8. ČLEN

OMEJITEV UPORABE TAJNIH PODATKOV IN DOSTOPA DO NJIH

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

(2) Pogodbenica prejemnica tretji strani ali njenim državljanom ne da tajnih podatkov ali dovoli dostopa do njih brez predhodnega pisnega soglasja pogodbenice izvora.

9. 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 podatkov stopnje INTERNO/DIFUSIÓN LIMITADA lahko poteka tudi po pošti ali prek druge dostavne službe v skladu z notranjo zakonodajo.

(3) Pogodbenici lahko prenašata tajne podatke po odobrenih in zaščitenih informacijsko-komunikacijskih poteh v skladu z varnostnimi postopki, o katerih se dogovorita nacionalna varnostna organa.

10. 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) Posamezniki, ki prevajajo ali razmnožujejo tajne podatke, morajo imeti ustrezno dovoljenje za dostop do tajnih podatkov, kadar je to potrebno.

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

(5) Tajni podatki z oznako STROGO TAJNO/SECRETO se ne smejo uničiti. Ko jih pogodbenica prejemnica ne potrebuje več, se vrnejo pogodbenici izvora.

(6) Tajne podatke stopnje TAJNO/RESERVADO pogodbenica prejemnica, ko jih ne potrebuje več, uniči v skladu z notranjo zakonodajo in o tem uradno obvesti pogodbenico izvora.

(7) Tajne podatke stopnje ZAUPNO/CONFIDENCIAL ali nižje stopnje pogodbenica prejemnica, ko jih ne potrebuje več, uniči v skladu z notranjo zakonodajo.

11. ČLEN

POGODBE S TAJNIMI PODATKI

(1) Preden se tajni podatki v zvezi s pogodbo s tajnimi podatki dajo izvajalcem, podizvajalcem ali morebitnim izvajalcem, pogodbenica prejemnica obvesti pogodbenico izvora, ali:

a) njihove organizacije lahko ustrezno varujejo tajne podatke;

b) imajo varnostno dovoljenje organizacije za ravnanje s tajnimi podatki ustrezne stopnje;

c) ima njihovo osebje dovoljenje za dostop do tajnih podatkov ustrezne stopnje za opravljanje dolžnosti, pri katerih je potreben dostop do tajnih podatkov;

d) so vse osebe, ki imajo dostop do tajnih podatkov, obveščene o svoji odgovornosti in obveznostih pri varovanju tajnih podatkov v skladu z ustrezno zakonodajo pogodbenice prejemnice.

(2) Nacionalni varnostni organ lahko zahteva inšpekcijski pregled v organizaciji, da se zagotovi stalno izpolnjevanje varnostnih standardov v skladu z notranjo zakonodajo.

(3) Pogodba s tajnimi podatki vsebuje določbe o varnostnih zahtevah in stopnji tajnosti vsakega njenega vidika ali dela. Izvod takega dokumenta se predloži pristojnim varnostnim organom pogodbenic.

12. 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 prek nacionalnega varnostnega organa organizacije pošiljateljice predloži nacionalnemu varnostnemu organu organizacije gostiteljice vsaj 20 dni pred začetkom obiska. 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) Dovoljenje za obisk velja največ eno leto.

(5) Nacionalna varnostna organa se lahko dogovorita o seznamu obiskovalcev, ki imajo pravico do večkratnih obiskov. Ko je seznam potrjen, se lahko sodelujoče organizacije o obiskih dogovarjajo neposredno v skladu z dogovorjenimi pogoji.

(6) Pogodbenica zagotavlja varstvo osebnih podatkov obiskovalcev v skladu z notranjo zakonodajo.

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

13. ČLEN

SODELOVANJE PRI VAROVANJU TAJNOSTI

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

(2) Pristojna varnostna organa se obveščata o izjemnih varnostnih tveganjih, ki lahko ogrozijo dane tajne podatke.

(3) Nacionalna varnostna organa si na zaprosilo pomagata pri izvajanju postopkov varnostnega preverjanja.

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

14. 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) Pristojna pogodbenica takoj uvede preiskavo in sprejme vse mogoče ustrezne ukrepe v skladu z notranjo zakonodajo, da omeji posledice kršitve iz prvega odstavka tega člena in prepreči 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.

15. ČLEN

STROŠKI

(1) Sporazum ne predvideva nastanka katerih koli stroškov.

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

16. ČLEN

REŠEVANJE SPOROV

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

17. 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 veljavnosti tega sporazuma.

(2) Sporazum se lahko na zahtevo pogodbenice kadar koli spremeni, vendar le na podlagi obojestranskega pisnega soglasja 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, 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, preneseni na podlagi tega sporazuma, še naprej varujejo v skladu z njegovimi določbami, dokler pogodbenica prejemnica ni pisno razrešena te obveznosti ali ni od nje zahtevano, da jih vrne pogodbenici izvora.

(5) Za izvajanje sporazuma se lahko sklenejo dogovori o izvajanju.

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

Sklenjeno v Madridu, 21. oktobra 2014 v dveh izvirnikih v slovenskem, španskem in angleškem jeziku, pri čemer so vsa besedila enako verodostojna. Pri različni razlagi se sklicuje na angleško besedilo.

Za Republiko Slovenijo

Za Kraljevino Španijo

ACUERDO

ENTRE

LA REPÚBLICA DE ESLOVENIA

Y

EL REINO DE ESPAÑA

PARA

EL INTERCAMBIO Y PROTECCIÓN RECÍPROCA DE INFORMACIÓN CLASIFICADA

La República de Eslovenia

Y

El Reino de España

en lo sucesivo denominados las "Partes",

deseosos de garantizar la protección de la Información Clasificada intercambiada entre las Partes o entre entidades públicas y privadas bajo su jurisdicción,

han convenido en lo siguiente:

ARTÍCULO 1

OBJETO

De conformidad con sus leyes y reglamentos nacionales, y respetando sus intereses y seguridad nacionales, ambas Partes adoptarán las medidas necesarias para garantizar la protección de la Información Clasificada que se transmita o se genere conforme al presente Acuerdo.

ARTÍCULO 2

ÁMBITO DE APLICACIÓN

(1) El presente Acuerdo establece procedimientos para la protección de la Información Clasificada intercambiada entre las Partes.

(2) Ninguna de las Partes podrá alegar lo dispuesto en el presente Acuerdo para obtener Información Clasificada que la otra Parte haya recibido de un Tercero.

ARTÍCULO 3

DEFINICIONES

A los efectos del presente Acuerdo, serán de aplicación las siguientes definiciones:

Contrato Clasificado: Un contrato o subcontrato, incluidas las negociaciones precontractuales, que contenga Información Clasificada o suponga acceder a la misma.

Información Clasificada: Cualquier Información, con independencia de su forma, transmitida o generada entre las Partes conforme a las leyes y reglamentos de cualquiera de ellas y que requiera, en interés de la seguridad nacional, una

protección contra la divulgación no autorizada o cualquier otro comprometimiento, y que sea designada como tal y marcada de la forma pertinente por alguna de las Partes.

Contratista: Una persona jurídica con capacidad jurídica para celebrar contratos.

Habilitación de Seguridad de Establecimiento: La determinación efectiva por la Autoridad de Seguridad Competente de que un Contratista posee, desde el punto de vista de la seguridad, la capacidad para manejar Información Clasificada, de conformidad con las leyes y reglamentos nacionales.

Necesidad de conocer: Principio conforme al cual sólo se permitirá acceder a Información Clasificada a una persona para las cuestiones relacionadas con sus tareas o funciones oficiales.

Parte de Origen: La Parte, incluidas las entidades públicas y privadas bajo su jurisdicción, que facilite Información Clasificada a la Parte Receptora.

Habilitación Personal de Seguridad: Determinación positiva, a raíz de un procedimiento de investigación conforme a las leyes y reglamentos nacionales, según la cual se concluye que una persona puede acceder a la Información Clasificada y manejarla hasta el grado definido en la autorización.

Parte Receptora: La Parte, incluidas las entidades públicas y privadas bajo su jurisdicción, que reciba Información Clasificada de la Parte de Origen.

Tercero: Todo Estado, incluidas las entidades públicas o privadas bajo su jurisdicción, u organización internacional que no sea Parte en el presente Acuerdo.

ARTÍCULO 4

AUTORIDADES DE SEGURIDAD COMPETENTES

(1) Las Autoridades Nacionales de Seguridad designadas por las Partes como responsables de la aplicación general y de los controles correspondientes a todos los pormenores del presente Acuerdo son:

En la República de Eslovenia:

República de Eslovenia; Oficina del Gobierno para la Protección de la Información Clasificada

En el Reino de España:

Secretario de Estado, Director del Centro Nacional de Inteligencia
Oficina Nacional de Seguridad

(2) Las Autoridades Nacionales de Seguridad se comunicarán entre sí la existencia de otras Autoridades de Seguridad Competentes responsables de la ejecución del presente Acuerdo.

(3) Las Partes se informarán mutuamente por conducto diplomático cualquier modificación que afecte a sus Autoridades Nacionales de Seguridad.

ARTÍCULO 5

CLASIFICACIONES DE SEGURIDAD

(1) La Información Clasificada que se divulgue conforme al presente Acuerdo se marcará con la clasificación de seguridad pertinente de acuerdo con las leyes y reglamentos nacionales.

(2) Las siguientes marcas de clasificación de seguridad nacional se consideran equivalentes:

República de Eslovenia	**Reino de España**
STROGO TAJNO	SECRETO
TAJNO	RESERVADO
ZAUPNO	CONFIDENCIAL
INTERNO	DIFUSIÓN LIMITADA

(3) El grado de clasificación de seguridad que se atribuya a la información generada en el curso de la cooperación recíproca entre las Partes sólo podrá establecerse, modificarse o desclasificarse de mutuo acuerdo. En caso de desacuerdo sobre el grado de clasificación de seguridad que deba atribuirse a dicha información, las Partes adoptarán el grado más alto propuesto por cualquiera de ellas.

ARTÍCULO 6

ACCESO A LA INFORMACIÓN CLASIFICADA

(1) El acceso a la Información Clasificada sólo se permitirá a aquellas personas con Necesidad de Conocer a las que se haya informado sobre su tratamiento y protección y que hayan recibido la debida autorización de conformidad con las leyes y reglamentos nacionales.

(2) Las Partes se reconocerán mutuamente sus Habilitaciones Personales de Seguridad y Habilitaciones de Seguridad de Establecimiento. El apartado 2 del artículo 5 se aplicará según proceda.

ARTÍCULO 7

PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

(1) Las Partes otorgarán a la Información Clasificada mencionada en el presente Acuerdo al menos el mismo nivel de protección que otorguen a su propia Información Clasificada de grado de clasificación de seguridad equivalente.

(2) La Autoridad de Seguridad Competente de la Parte de Origen:

a) garantizará que en la Información Clasificada aparezca la marca de clasificación de seguridad pertinente de conformidad con sus leyes y reglamentos nacionales, e
b) informará a la Parte Receptora de cualesquiera condiciones impuestas a la divulgación, o limitaciones al uso, de la Información Clasificada y de cualquier ulterior cambio de la clasificación de seguridad.

(3) La Autoridad de Seguridad Competente de la Parte Receptora:

a) garantizará que en la Información Clasificada aparezca la marca de clasificación de seguridad equivalente de conformidad con el apartado 2 del artículo 5, y
b) se asegurará de que el grado de clasificación de seguridad no se modifica a menos que lo autorice por escrito la Parte de Origen.

(4) Cada Parte se cerciorará de que se aplican las medidas pertinentes para proteger la Información Clasificada tratada, almacenada o transmitida a través de los sistemas de información y comunicaciones. Dichas medidas garantizarán la confidencialidad, integridad, disponibilidad y, si procede, el no repudio y la autenticidad de la Información Clasificada, así como un nivel idóneo de responsabilidad y trazabilidad de cualquier actuación relativa a dicha Información.

ARTÍCULO 8

LIMITACIÓN AL USO Y ACCESO A LA INFORMACIÓN CLASIFICADA

(1) La Parte Receptora sólo hará uso de la Información Clasificada para los fines que dieron lugar a su divulgación y con sujeción a las limitaciones establecidas por la Parte de Origen.

(2) La Parte Receptora no divulgará ni permitirá el acceso de terceros o sus nacionales a la Información Clasificada sin el previo consentimiento por escrito de la Parte de Origen.

ARTÍCULO 9

TRANSMISIÓN DE LA INFORMACIÓN CLASIFICADA

(1) La Información Clasificada se transmitirá entre las Partes por conducto diplomático o cualquier otro cauce seguro mutuamente aprobado por sus Autoridades Nacionales de Seguridad, de conformidad con las leyes y reglamentos nacionales.

(2) La Información Clasificada como INTERNO/DIFUSIÓN LIMITADA/ podrá transmitirse por correo o cualquier otro servicio de entrega de conformidad con las leyes y reglamentos nacionales.

(3) Las Partes podrán transmitir la Información Clasificada a través de medios electrónicos autorizados y seguros de acuerdo con los procedimientos de seguridad acordados entre las Autoridades Nacionales de Seguridad.

ARTÍCULO 10

REPRODUCCIÓN, TRADUCCIÓN Y DESTRUCCIÓN DE LA INFORMACIÓN CLASIFICADA

(1) Toda reproducción y traducción llevará las marcas pertinentes de clasificación de seguridad y será objeto de la misma protección que la Información Clasificada original. Las traducciones y la cantidad de reproducciones se limitarán al número mínimo requerido para fines oficiales.

(2) Todas las traducciones llevarán la marca de la clasificación de seguridad original y en ellas figurará una anotación, en la lengua de traducción, en la que se haga constar que contienen Información Clasificada de la Parte de Origen.

(3) Las personas que traduzcan o reproduzcan Información Clasificada deberán contar con la pertinente Habilitación Personal de Seguridad, cuando ésta sea necesaria.

(4) La Información Clasificada marcada STROGO TAJNO/SECRETO, tanto en su original como en su traducción, sólo podrá reproducirse con el consentimiento escrito de la Parte de Origen.

(5) La Información Clasificada marcada STROGO TAJNO/ SECRETO no podrá destruirse; se devolverá a la Parte de Origen cuando la Parte Receptora ya no la considere necesaria.

(6) La Información Clasificada TAJNO/RESERVADO será destruida por la Parte Receptora de conformidad con sus leyes y reglamentos cuando ya no la considere necesaria y notificándolo a la Parte de Origen.

(7) La Información Clasificada ZAUPNO/CONFIDENCIAL, o de grado inferior, será destruida por la Parte Receptora de conformidad con sus leyes y reglamentos cuando ya no la considere necesaria.

ARTÍCULO 11

CONTRATOS CLASIFICADOS

(1) Antes de facilitar Información Clasificada relativa a un Contrato Clasificado a un contratista, subcontratista o posible contratista, la Parte Receptora informará a la Parte de Origen de lo siguiente:

a) si los establecimientos de aquéllos cuentan con capacidad para proteger adecuadamente la Información Clasificada;

b) si cuentan con la Habilitación de Seguridad de Establecimiento para el tratamiento de la Información Clasificada al grado correspondiente;

c) si el personal cuenta con el grado adecuado de Habilitación Personal de Seguridad para desempeñar funciones que exigen acceder a la Información Clasificada;

d) si se ha informado a todos aquellos con acceso a la Información Clasificada de las responsabilidades y obligaciones que les incumben en materia de protección de la misma de conformidad con las leyes y reglamentos de la Parte Receptora.

(2) Cada Autoridad Nacional de Seguridad podrá solicitar que se lleve a cabo una inspección de seguridad en un establecimiento para garantizar el cumplimiento de las normas de seguridad de conformidad con las leyes y reglamentos nacionales.

(3) Un Contrato Clasificado deberá comprender disposiciones sobre los requisitos de seguridad y sobre la clasificación de cada uno de sus pormenores y elementos. Se remitirá una copia de dicho documento a las Autoridades de Seguridad Competentes de las Partes.

ARTÍCULO 12

VISITAS

(1) Las visitas que impliquen acceder a Información Clasificada estarán sujetas a la autorización previa de la Autoridad Nacional de Seguridad de la Parte anfitriona.

(2) Al menos 20 días antes del comienzo de la visita, se enviará una solicitud de autorización de la misma a través de la Autoridad Nacional de Seguridad de la Parte remitente dirigida a la Autoridad Nacional de Seguridad del establecimiento que desea visitarse. La solicitud de visita incluirá los siguientes datos, que se utilizarán tan sólo para los fines de la misma:

a) el nombre del visitante, la fecha y el lugar de nacimiento, su nacionalidad y número de documento de identidad/pasaporte;

b) el cargo del visitante, especificándose la entidad a la que representa;

c) el proyecto en el que participa el visitante;

d) la validez y el grado de Habilitación Personal de Seguridad del visitante, si procede;

e) el nombre, dirección, número de fax / teléfono, dirección de correo electrónico y punto de contacto del establecimiento a visitar;

f) el objeto de la visita, incluido el grado máximo de clasificación de seguridad de la Información Clasificada que vaya a manejarse;

g) la fecha prevista y duración de la visita. En caso de visitas recurrentes deberá indicarse el periodo total cubierto por las mismas;

h) la fecha y firma de la Autoridad Nacional de Seguridad remitente.

(3) En casos urgentes, las Autoridades Nacionales de Seguridad podrán acordar plazos más cortos para la presentación de la solicitud de visita.

(4) La validez de las autorizaciones de visita no excederá de un año.

(5) Las Autoridades Nacionales de Seguridad podrán elaborar un listado de visitantes con derecho a efectuar visitas recurrentes. Una vez aprobado el listado, las visitas podrán organizarse directamente entre los establecimientos interesados, de conformidad con las condiciones estipuladas.

(6) Cada Parte garantizará la protección de los datos personales de los visitantes, de conformidad con las leyes y reglamentos nacionales.

(7) La Información Clasificada que llegue a conocimiento de un visitante se considerará comprendida en lo previsto en el presente Acuerdo.

ARTÍCULO 13

COOPERACIÓN EN MATERIA DE SEGURIDAD

(1) Con objeto de establecer y mantener normas de seguridad comparables, las Autoridades de Seguridad Competentes se facilitarán mutuamente, previa petición, información sobre sus normas, procedimientos y prácticas de seguridad para la protección de la Información Clasificada A tal fin, las Autoridades Nacionales de Seguridad podrán organizar visitas recíprocas.

(2) Las Autoridades de Seguridad Competentes se informarán mutuamente de los riesgos excepcionales de seguridad que puedan poner en peligro la Información Clasificada cedida.

(3) Cuando se solicite, las Autoridades Nacionales de Seguridad se asistirán mutuamente en el cumplimiento de los procedimientos de habilitación de seguridad.

(4) Las Autoridades Nacionales de Seguridad se informarán a la mayor brevedad de cualquier modificación de las Habilitaciones Personales de Seguridad y de las Habilitaciones de Seguridad de Establecimiento mutuamente reconocidas.

ARTÍCULO 14

INFRACCIÓN DE LA SEGURIDAD

(1) Si se produce una infracción de la seguridad que derive en una divulgación no autorizada, apropiación indebida o pérdida de la Información Clasificada, o se sospecha que se ha producido dicha infracción, la Autoridad Nacional de Seguridad de la Parte Receptora informará inmediatamente por escrito a la Autoridad Nacional de Seguridad de la Parte de Origen.

(2) La Parte competente iniciará de inmediato una investigación y adoptará todas las medidas que resulten apropiadas, de conformidad con las leyes y reglamentos nacionales, a fin de limitar las consecuencias de la infracción mencionada en el apartado 1 del presente artículo e impedir futuras infracciones. Si así se le solicita, la otra Parte prestará la asistencia pertinente; se informará a ésta del resultado de las actuaciones y de las medidas adoptadas a raíz de la infracción.

(3) Cuando la infracción de seguridad se haya producido por un Tercero, la Autoridad Nacional de Seguridad de la Parte remitente adoptará sin dilación las medidas mencionadas en el apartado 2.

ARTÍCULO 15
GASTOS

(1) El presente Acuerdo no prevé la generación de gasto alguno.

(2) Si durante la aplicación del presente Acuerdo se producen gastos imprevistos para alguna de las Partes, cada una de ellas los sufragará por su cuenta.

ARTÍCULO 16
SOLUCIÓN DE CONTROVERSIAS

Cualquier controversia relativa a la interpretación o aplicación del presente Acuerdo se resolverá mediante consultas y negociaciones entre las Partes y no se someterá a ningún tribunal internacional ni a ningún Tercero para su resolución.

ARTÍCULO 17
DISPOSICIONES FINALES

(1) El presente Acuerdo entrará en vigor el primer día del segundo mes a contar desde la fecha de recepción de la última notificación escrita por la que las Partes se informen recíprocamente, por conducto diplomático, de que se han completado sus trámites jurídicos internos necesarios para la entrada en vigor.

(2) El presente Acuerdo podrá ser enmendado en cualquier momento, a petición de cualquiera de las Partes, pero siempre con el consentimiento mutuo por escrito de ambas. Las enmiendas entrarán en vigor de conformidad con el apartado 1.

(3) El presente Acuerdo se celebra por un periodo indefinido. Cada Parte podrá denunciarlo mediante notificación previa por escrito a la otra Parte por conducto diplomático. En tal caso, el presente Acuerdo expirará seis meses después de la fecha en la que la otra Parte haya recibido la denuncia.

(4) En caso de terminación del presente Acuerdo, la Información Clasificada facilitada conforme al mismo continuará protegida de conformidad con las

disposiciones del mismo hasta que se exima por escrito a la Parte Receptora de dicha obligación o se le solicite que la devuelva a la Parte de Origen.

(5) Podrán celebrarse acuerdos de carácter administrativo para la aplicación del presente Acuerdo.

En testimonio de lo cual, los abajo firmantes, debidamente autorizados al efecto, han firmado el presente Acuerdo.

Hecho por duplicado, en Madrid, el 21 de octubre de 2014 en dos originales en esloveno, español e inglés, siendo todos los textos igualmente auténticos. En caso de divergencia en la interpretación, el texto inglés servirá de referencia.

Por la República de Eslovenia

Por el Reino de España

AGREEMENT

BETWEEN

THE REPUBLIC OF SLOVENIA

AND

THE KINGDOM OF SPAIN

ON

THE EXCHANGE AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

The Republic of Slovenia

and

the Kingdom of Spain

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

have agreed on the following:

ARTICLE 1
OBJECTIVE

In accordance with their national laws and regulations and in respect of national interests and security, both Parties shall take all appropriate measures to ensure the protection of Classified Information, which is transmitted or generated according to this Agreement.

ARTICLE 2
SCOPE OF APPLICATION

(1) This Agreement sets out procedures for the protection of Classified Information exchanged between the Parties.

(2) Neither Party shall invoke this Agreement in order to obtain Classified Information that the other Party has received from a Third Party.

ARTICLE 3
DEFINITIONS

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

Classified Contract: A contract or a subcontract, including pre-contractual negotiations, that contains Classified Information or involves access to it.

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

Contractor: A legal entity possessing the legal capacity to conclude contracts.

Facility Security Clearance: A positive determination by the Competent Security Authority that, from a security point of view, a Contractor has the capability to handle Classified Information, in accordance with national laws and regulations.

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.

Originating Party: The Party, including any public or private entities under its jurisdiction, that releases Classified Information to the Recipient Party.

Personnel Security Clearance: A positive determination following an accomplished vetting procedure in accordance with national laws and regulations, on the basis of which an individual is eligible to have access to and to handle Classified Information up to the level defined in the clearance.

Recipient Party: The Party, including any public or private entities under its jurisdiction, that receives Classified Information from the Originating Party.

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

ARTICLE 4
COMPETENT SECURITY AUTHORITIES

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

In the Republic of Slovenia:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov;

In the Kingdom of Spain:
Secretario de Estado, Director del Centro Nacional de Inteligencia
Oficina Nacional de Seguridad

(2) The National Security Authorities shall notify each other of any other Competent Security Authorities that are responsible for the implementation of this Agreement.

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

ARTICLE 5
SECURITY CLASSIFICATIONS

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

(2) The following national security classification markings are equivalent:

Republic of Slovenia	Kingdom of Spain
STROGO TAJNO	SECRETO
TAJNO	RESERVADO
ZAUPNO	CONFIDENCIAL
INTERNO	DIFUSIÓN LIMITADA

(3) The level of security classification to be given to the information generated in the process of the mutual cooperation of the Parties shall only be determined, modified or declassified by mutual consent. In the case of disagreement on the level of security classification to be given to such information, the Parties shall adopt the higher level proposed by any of them.

ARTICLE 6
ACCESS TO CLASSIFIED INFORMATION

(1) Access to Classified Information shall be allowed only to those individuals with a Need-to-Know, who have been briefed on the handling and protection of Classified Information, and who have been duly authorised in accordance with national laws and regulations.

(2) The Parties shall mutually recognise their Personnel and Facility Security Clearances. Paragraph 2 of Article 5 shall apply accordingly.

ARTICLE 7
PROTECTION OF CLASSIFIED INFORMATION

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

(2) The Competent Security Authority of the Originating Party shall:

a) ensure that the Classified Information is marked with an appropriate security classification marking 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 the Classified Information and of any subsequent changes in the security classification.

(3) The Competent Security Authority of the Recipient Party shall:

a) ensure that the Classified Information is marked with an equivalent security classification marking in accordance with Paragraph 2 of Article 5, and

b) ensure that the security classification level is not changed unless authorised in writing by the Originating Party.

(4) Each Party shall ensure that appropriate measures are implemented for the protection of the 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 the Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

ARTICLE 8
RESTRICTION ON THE USE AND ACCESS TO CLASSIFIED INFORMATION

(1) The Recipient Party shall use Classified Information only 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 or allow access to Classified Information to a Third Party or its nationals without prior written consent of the Originating Party.

ARTICLE 9
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) Information classified as INTERNO / DIFUSIÓN LIMITADA may also be transmitted by post or another delivery service in accordance with national laws and regulations.

(3) The Parties may transmit Classified Information through approved and secured electronic means in line with security procedures agreed between the National Security Authorities.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) All reproductions and translations shall bear appropriate security classification markings and they shall be protected as the original Classified Information. Translations and the number of reproductions shall be limited to the minimum required for an official purpose.

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

(3) The individuals translating or reproducing Classified Information shall hold the appropriate Personnel Security Clearance, where necessary.

(4) Classified Information marked STROGO TAJNO / SECRETO, both in the original and in the translation, shall be reproduced only upon the written permission of the Originating Party.

(5) Classified Information marked STROGO TAJNO / SECRETO shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the recipient Party.

(6) Information classified TAJNO / RESERVADO shall be destroyed by the Recipient Party in accordance with its national laws and regulations after it is no longer considered necessary with a notification to the Originating Party.

(7) Information classified ZAUPNO / CONFIDENCIAL or below shall be destroyed by the Recipient Party in accordance with its national laws and regulations, after it is no longer considered necessary.

ARTICLE 11
CLASSIFIED CONTRACTS

(1) Before providing Classified Information related to a Classified Contract to Contractors, sub-contractors or prospective contractors, the Recipient Party shall inform the Originating Party whether:

a) their facilities have the capability to adequately protect Classified Information;

b) they possess the Facility Security Clearance for handling Classified Information to the appropriate level;

c) its personnel has the appropriate level of Personnel Security Clearance to perform functions that require access to the Classified Information;

d) all persons having access to the Classified Information are informed of their responsibilities and obligations to protect the Classified Information in accordance with the appropriate laws and regulations of the Recipient Party.

(2) Each National Security Authority may request that a security inspection be carried out at a facility to ensure continuing compliance with security standards in accordance with national laws and regulations.

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

ARTICLE 12
VISITS

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

(2) A request for a visit shall be submitted through the National Security Authority of the sending facility to the National Security Authority of the hosting facility at least 20 days prior to the commencement of the visit. The request for the visit shall include the following data, which shall be used for the purpose of the visit only:

a) the visitor's name, date and place of birth, citizenship and identification card/passport number;

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

c) a specification of the project in which the visitor participates;

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

e) the name, address, phone/fax number, e-mail 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 case of recurring visits, the total period covered by the visits shall be stated;

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

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

(4) The validity of the visit authorisation shall not exceed one year.

(5) The National Security Authorities may agree on a list of visitors entitled to recurring visits. Once the list has been approved, visits may be arranged directly between the facilities involved, in accordance with the terms and conditions agreed upon.

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

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

ARTICLE 13
SECURITY CO-OPERATION

(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. To this end, the National Security Authorities may visit each other.

(2) The Competent Security Authorities shall inform each other of exceptional security risks that may endanger the released Classified Information.

(3) When requested, the National Security Authorities shall assist each other in carrying out security clearance procedures.

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

ARTICLE 14
BREACH OF SECURITY

(1) In case of a security breach resulting in unauthorised disclosure, misappropriation or loss of Classified Information or the 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 Party shall immediately initiate an investigation and undertake all possible appropriate measures in accordance with national laws and regulations so as to limit the consequences of the breach referred to in Paragraph 1 of this Article and to prevent further breaches. When requested, the other Party shall provide appropriate assistance; it shall be informed of the outcome of the proceedings and the measures undertaken due to the breach.

(3) When the breach of security has occurred in a Third Party, the National Security Authority of the sending Party shall take the actions referred to in paragraph 2 of this Article without delay.

ARTICLE 15
EXPENSES

(1) This Agreement does not include the generation of any costs.

(2) In case that, in the course of the implementation of this Agreement, there are unexpected costs for any of the Parties, each Party shall bear its own expenses.

ARTICLE 16
SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties and shall not be referred to any international tribunal or Third Party for settlement.

ARTICLE 17
FINAL PROVISIONS

(1) This Agreement shall enter into force on the first day of the second month from the date of receipt of the latest written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.

(2) This Agreement may be amended, at any moment, at the request of either Party, but on the basis of the mutual written consent of the Parties. Amendments shall enter into force in accordance with paragraph 1 of this Article.

(3) This Agreement is concluded for an indefinite period of time. Either Party may cancel this Agreement by giving the other Party notice in writing through diplomatic

channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the notice of cancellation.

(4) 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 until the Recipient Party is released from this obligation in writing or is requested to return it to the Originating Party.

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

In witness whereof the undersigned, being duly authorised thereto, have signed this Agreement.

Done in Madrid on 21 October 2014 in two originals in the Slovenian, Spanish and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall be used as a reference.

For the Republic of Slovenia

For the Kingdom of Spain