No. 52388

Spain
and
Serbia

Agreement between the Kingdom of Spain and the Republic of Serbia on the exchange and mutual protection of classified information. Madrid, 13 March 2014

Entry into force: *6 November 2014 by notification, in accordance with article 17*

Authentic texts: *Serbian and Spanish*

Registration with the Secretariat of the United Nations: *Spain, 29 January 2015*

Espagne
et
Serbie

Accord entre le Royaume d'Espagne et la République de Serbie relatif à l'échange et la protection réciproque des informations classifiées. Madrid, 13 mars 2014

Entrée en vigueur : *6 novembre 2014 par notification, conformément à l'article 17*

Textes authentiques : *serbe et espagnol*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Espagne, 29 janvier 2015*

[SERBIAN TEXT – TEXTE SERBE]

Споразум

између

Краљевине Шпаније

и

Републике Србије

о размени и узајамној заштити тајних података

Краљевина Шпанија

и

Република Србија

(у даљем тексту: „стране"),

у жељи да осигурају заштиту тајних података који се размењују или стварају између страна или између јавних и приватних субјеката у њиховој надлежности,

споразумеле су се о следећем:

Члан 1.
Циљ

Овим споразумом стране се обавезују да предузимају све одговарајуће мере да, у складу са својим законодавствима и поштујући националне интересе и безбедност, осигурају заштиту тајних података који се размењују или стварају у складу са овим споразумом.

Члан 2.
Област примене

1. Овим споразумом одређују се процедуре за заштиту тајних података који се размењују или стварају између страна или између јавних и приватних субјеката у њиховој надлежности.

2. Ниједна од страна неће се позивати на овај споразум како би прибавила тајне податке које је друга страна примила од треће стране.

Члан 3.
Дефиниције

Ради примене овог споразума наведени појмови имају следеће значење:

1. **уговор с тајним подацима** јесте уговор или подуговор, укључујући и преговоре пре њиховог закључивања, који садржи тајне податке или подразумева приступ тим подацима;

2. **тајни подаци** јесу подаци или материјали за које је утврђено да захтевају заштиту од неовлашћеног откривања и који су као такви обележени одређеном ознаком тајности у складу с националним законодавством;

3. **надлежни орган** јесте орган којег је једна страна одредила да је надлежан за примену овог споразума и надзор над том применом;

4. **уговарач** јесте правно лице које поседује пословну способност за закључивање уговора у складу са одредбама овог споразума;

5. **безбедносни цертификат за правно лице** јесте позитивно решење које је издао надлежни орган и којим се са становишта безбедности потврђује да правно лице поседује физичке и организационе капацитете за руковање тајним подацима и њихово чување у складу с националним законодавством;

6. **принцип „потребно је да зна"** означава да постоји потреба да се приступи тајним подацима у оквиру делокруга одређеног службеног положаја и ради извршења посебног задатка;

7. **страна давалац** јесте страна која ствара тајне податке или их преноси другој страни;

8. **безбедносни цертификат за физичка лица** јесте позитивно решење које је издао надлежни орган и којим се потврђује да физичко лице испуњава услове да приступи тајним подацима у складу с националним законодавством;

9. **страна прималац** јесте страна која прима тајне податке које је створила страна давалац или их је њој пренела;

10. **трећа страна** јесте свака држава или међународна организација која није страна у овом споразуму.

Члан 4.
Надлежни органи

1. Надлежни органи одговорни за примену овог споразума су:

за Краљевину Шпанију:

државни секретар, директор Националног обавештајног центра, Национална канцеларија за безбедност;

за Републику Србију:

Канцеларија Савета за националну безбедност и заштиту тајних података.

2. Стране ће једна другу дипломатским путем обавештавати о свакој измени њиховог законодавства која се односи на надлежности надлежних органа.

Члан 5.
Ознаке тајности и еквиваленти

1. Тајним подацима који се преносе или стварају у оквиру области примене овог споразума стране обезбеђују исти степен заштите који је предвиђен за њихове тајне податке еквивалентног степена тајности.

2. Страна давалац одређује, мења или скида ознаку тајности која је додељена тајним подацима. Страна давалац без одлагања, писаним путем, обавештава страну примаоца о донетим одлукама како би се примениле одговарајуће безбедносне мере.

3. Стране су сагласне да су следећи степени тајности еквивалентни и подударни са степенима тајности који се наводе у следећој табели:

За Краљевину Шпанију	За Републику Србију
SECRETO	ДРЖАВНА ТАЈНА
RESERVADO	СТРОГО ПОВЕРЉИВО
CONFIDENCIAL	ПОВЕРЉИВО
DIFUSIÓN LIMITADA	ИНТЕРНО

Члан 6.
Принципи безбедности

1. Приступ тајним подацима степена тајности CONFIDENCIAL / ПОВЕРЉИВО или већег степена тајности ограничава се на физичка

лица која у извршавању својих задатака поступају у складу с принципом „потребно је да зна", која је надлежни орган за то овластио и која имају безбедносни цертификат за физичка лица одговарајућег степена тајности. Приступ тајним подацима степена тајности DIFUSIÓN LIMITADA / ИНТЕРНО ограничава се на физичка лица која поступају у складу с принципом „потребно је да зна" и прописно су за то овлашћена и обучена.

2. Страна прималац не преноси тајне податке трећој страни нити било којем физичком лицу или јавном и приватном субјекту које има држављанство треће стране без писаног одобрења стране даваоца.

3. Тајни подаци користе се само у ону сврху за коју су пренети на основу сваког споразума који су стране потписале, као и на основу уговора с тајним подацима.

4. Надлежни органи страна, на захтев, обавештавају један другог о својим безбедносним стандардима, процедурама и праксама у вези са заштитом тајних података како би остварили и применили сличне безбедносне стандарде.

5. Надлежни органи страна обавештавају један другог о мерама примењеним за заштиту тајних података који се преносе или стварају на основу овог споразума.

Члан 7.
Безбедносни цертификати

1. Надлежни органи страна, на захтев, пружају један другом помоћ за време обављања поступка провере својих држављана или правних лица која су стално настањена или бораве на територији једне или друге стране, у складу с националним законодавством.

2. Стране признају безбедносне цертификате за физичка и правна лица издате у складу са законодавством друге стране. Еквивалентност безбедносних цертификата у складу је са чланом 5. овог споразума.

3. Надлежни органи страна обавештавају један другог о свакој евентуалној промени у вези са одређеним безбедносним цертификатом за физичко или правно лице, посебно у случају његовог опозива или снижавања степена тајности.

Члан 8.
Превођење и умножавање тајних података

1. Тајни подаци означени степеном тајности SECRETO / ДРЖАВНА ТАЈНА преводе се и умножавају само уз претходно писано одобрење стране даваоца.

2. Превођење и умножавање тајних података врши се у складу са следећим процедурама:

   а) физичка лица одговорна за превођење или умножавање тајних података, према потреби, поседују одговарајући безбедносни цертификат за физичка лица;

   б) преводи и умножени примерци обележавају се оригиналним ознакама тајности и добијају исту заштиту као и оригинали;

   ц) број преведених и умножених примерака ограничен је на број који је потребан у службене сврхе;

   д) преводи садрже одговарајућу напомену на језику превода у којој се наводи да садрже тајне податке добијене од стране даваоца.

Члан 9.
Уништавање тајних података

1. Тајни подаци степена тајности CONFIDENCIAL / ПОВЕРЉИВО и нижег степена тајности уништавају се тако да се онемогући њихова реконструкција у складу с националним законодавством.

2. Тајни подаци степена тајности RESERVADO / СТРОГО ПОВЕРЉИВО уништавају се тако да се онемогући њихова реконструкција у складу с националним законодавством и уз претходно прибављено писано одобрење стране даваоца.

3. Тајни подаци степена тајности SECRETO / ДРЖАВНА ТАЈНА не уништавају се, него се враћају страни даваоцу.

4. У ванредним ситуацијама, када није могуће заштитити тајне податке или их вратити страни даваоцу, страна прималац их без одлагања уништава и о томе, писаним путем, обавештава страну даваоца.

Члан 10.
Пренос тајног податка између страна

1. Пренос тајних података између страна обавља се дипломатским путем или другим безбедним путем које одобре њихови надлежни органи у складу с националним законодавством.

2. Ако пренос тајних података обавља курир, он мора имати одговарајући безбедносни цертификат и бити упознат са својим дужностима, као и поседовати курирски цертификат који му је издао надлежни орган стране која преноси тајне податке.

3. Стране могу преносити тајне податке степена тајности DIFUSIÓN LIMITADA / ИПТЕРНО електронским путем, у складу с безбедносним процедурама које одобре надлежни органи страна.

4. Безбедносне и обавештајне службе страна могу непосредно размењивати тајне податке у оквиру свог делокруга, у складу са одредбама овог споразума и националним законодавством.

Члан 11.
Област индустријске безбедности

1. Пре достављања тајних података у вези са уговором с тајним подацима у погледу уговарача, подуговарача или потенцијалних уговарача, надлежни орган стране примаоца обавестиће надлежни орган стране даваоца о следећем:

   а) да ли њихова правна лица имају капацитет да адекватно заштите тајне податке и да ли имају безбедносни цертификат за правна лица за поступање с тајним подацима одговарајућег степена тајности;

   б) да ли њихово особље има безбедносни цертификат за физичка лица одговарајућег степена тајности за обављање задатака који захтевају приступ тајним подацима;

   ц) да ли су сва лица која имају приступ тајним подацима упозната са својим дужностима и обавезама везаним за заштиту тајних података у складу са законодавством стране примаоца.

2. Надлежни органи могу захтевати да се у објекту правног лица изврши безбедносна инспекција, како би се осигурало континуирано

испуњавање безбедносних стандарда у складу с националним законодавством.

3. Уговор с тајним подацима садржи одредбе о безбедносним захтевима и о тајности сваког дела уговора с тајним подацима или објекта који је предмет уговора с тајним подацима. Примерак безбедносних захтева за сваки уговор с тајним подацима прослеђује се надлежном органу стране на чијој територији се изводе радови, како би се омогућио адекватан надзор и контрола безбедносних стандарда, процедура и пракси које су уговарачи утврдили ради заштите тајних података.

4. У току преговора ради закључивања уговора с тајним подацима између организација страна, надлежни орган обавештава другу страну о степену тајности додељеном тајним подацима на које се односе преговори.

Члан 12.
Посете

1. Посете под којима се подразумева приступ тајним подацима одобрава писаним путем надлежни орган стране домаћина.

2. Посетиоце мора адекватно проверити надлежни безбедносни орган стране која реализује посету у складу с националним законодавством.

3. Надлежни орган стране која реализује посету обавештава надлежни орган стране домаћина о планираној посети достављањем захтева за посету.

4. Захтев за посету обавезно садржи следеће:

   а) име и презиме посетиоца, функцију, место и датум рођења, држављанство, број путне исправе или личне карте;

   б) назив, адресу, број телефона и факса, имејл адресу и информацију о лицу за контакт у органима, агенцијама или објектима који ће бити посећени;

   ц) по потреби, потврду о безбедносном цертификату посетиоца и његово важење;

   д) разлог и сврху посете;

е) очекивани датум и трајање посете која се захтева. У случају чешћих посета, навести укупно трајање тих посета;

ф) датум, потпис, као и печат надлежног органа.

5. Када се посета одобри, надлежни орган стране домаћина доставља примерак захтева за посету лицу надлежном за безбедност у органу, установи или агенцији чији ће објекти бити посећени.

6. Одобрење посете не може важити дуже од једне године.

7. Надлежни органи могу усагласити списак посетилаца који су овлашћени да реализују чешће посете. Када надлежни органи одобре тај списак, правна лица могу непосредно организовати посете својим објектима у складу с напред договореним условима и одредбама.

Члан 13.
Повреда безбедности

1. У случају да се сумња или да се утврди да је дошло до неовлашћеног откривања, противправног присвајања или губитка тајних података који се односе на област примене овог споразума, надлежни орган стране даваоца се писаним путем без одлагања о томе обавештава.

2. Надлежни орган без одлагања покреће истрагу и предузима све одговарајуће мере, у складу с националним законодавством, како би отклонио последице такве повреде безбедности. Друга страна ће, на захтев, пружити одговарајућу помоћ и бити обавештена о резултатима истраге и мерама предузетим ради спречавања даљих повреда безбедности.

3. Ако до повреде безбедности дође у трећој страни, надлежни орган стране која шаље тајне податке, без одлагања, предузима радње предвиђене у ставу 1. овог члана.

Члан 14.
Трошкови

1. Примена овог споразума не захтева трошкове.

2. У случају било каквих трошкова, свака страна сноси своје трошкове који настану у вези с применом и праћењем примене овог споразума.

Члан 15.
Решавање спорова

Сви спорови у вези са тумачењем или применом одредаба овог споразума решавају се путем консултација и преговорима између страна.

Члан 16.
Административни уговори

Надлежни органи страна могу ради примене овог споразума закључити административне уговоре.

Члан 17.
Завршне одредбе

1. Споразум се закључује на неодређено време и ступа на снагу даном пријема последњег писаног обавештења којим се стране дипломатским путем обавештавају да су испуњене њихове унутрашње законске процедуре неопходне за ступање на снагу Споразума.

2. На захтев једне од страна, овај споразум се може у сваком тренутку изменити на основу писане сагласности обе стране. Измене ступају на снагу у складу са ставом 1. овог члана.

3. Свака страна може отказати овај споразум упућивањем другој страни, дипломатским путем, писаног обавештења о отказивању. У том случају, овај споразум биће раскинут након истека шест месеци од дана када друга страна прими обавештење о отказивању.

4. У случају отказивања овог споразума, сви тајни подаци који су пренети или створени у складу са овим споразумом биће заштићени у складу са одредбама овог споразума, осим ако страна давалац писаним путем не ослободи страну примаоца такве обавезе.

Сачињено у Мадриду дана 13. марта 2014. године у два оригинална примерка, сваки на шпанском, српском и енглеском језику, при чему су сви текстови подједнако веродостојни.

за Краљевину Шпанију

Феликс Сапз Ролдан

државни секретар
директор Националног обавештајног центра

за Републику Србију

др Горан Матић

директор Канцеларије Савета за националну безбедност и заштиту тајних података

[SPANISH TEXT – TEXTE ESPAGNOL]

ACUERDO

ENTRE

EL REINO DE ESPAÑA

Y

LA REPÚBLICA DE SERBIA

PARA

EL INTERCAMBIO Y PROTECCIÓN RECÍPROCA

DE INFORMACIÓN CLASIFICADA

El Reino de España

Y

la República de Serbia,

en lo sucesivo denominados las "Partes",

Deseosos de garantizar la protección de la Información Clasificada que se genere o se intercambie entre las Parte, o entre entidades públicas o privadas bajo su jurisdicción,

Han convenido en lo siguiente:

ARTÍCULO 1
OBJETO

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

ARTÍCULO 2
ÁMBITO DE APLICACIÓN

1. En el presente Acuerdo se establecen los procedimientos para la protección de la Información Clasificada que se genere o se intercambie entre las Partes, o entre entidades públicas o privadas bajo su jurisdicción.

2. Ninguna de las Partes podrá invocar 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:

1. Por **"Contrato Clasificado"** se entenderá todo contrato o subcontrato, incluidas las negociaciones precontractuales, que contenga Información Clasificada o suponga el acceso a la misma;

2. Por **"Información Clasificada"** se entenderá cualquier Información o material en relación con los cuales se determine la necesidad de protegerlos contra su divulgación no autorizada y que hayan sido así designados mediante una clasificación de seguridad de conformidad con las leyes y reglamentos nacionales;

3. Por **"Autoridad Competente"** se entenderá la autoridad designada por cada Parte como responsable de la aplicación y supervisión del presente Acuerdo;

4. Por **"Contratista"** se entenderá toda persona jurídica con capacidad jurídica para celebrar contratos al amparo de lo dispuesto en el presente Acuerdo;

5. Por **"Habilitación de Seguridad de Establecimiento"** se entenderá la determinación positiva, emitida por la Autoridad Competente según la cual un establecimiento posee, desde el punto de vista de la seguridad, capacidad material y organizativa para manejar o almacenar Información Clasificada, de conformidad con sus respectivas leyes y reglamentos nacionales;

6. Por **"Necesidad de conocer"** se entenderá la necesidad de acceder a Información Clasificada por el desempeño de un cargo oficial determinado y para la realización de una tarea específica;

7. Por **"Parte de Origen"** se entenderá la Parte en la que se genere la Información Clasificada o que la transmita a la otra Parte;

8. Por **"Habilitación Personal de Seguridad"** se entenderá una determinación positiva, emitida por la Autoridad Competente conforme a las leyes y reglamentos nacionales, según la cual se concluye que una persona puede tener acceso a Información Clasificada;

9. Por **"Parte Receptora"** se entenderá la Parte que reciba Información Clasificada generada o transmitida por la otra Parte;

10. Por **"Tercero"** se entenderá todo Estado u organización internacional que no sea Parte en el presente Acuerdo.

ARTÍCULO 4
AUTORIDADES COMPETENTES

1. Las Autoridades Competentes para la aplicación del presente Acuerdo son:

   Para el Reino de España:

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

   Para la República de Serbia:

   Oficina del Consejo Nacional de Seguridad y Protección de Información Clasificada

2. Las Partes se informarán mutuamente, por conducto diplomático, sobre cualquier modificación que se produzca en sus leyes y reglamentos nacionales en relación con las responsabilidades de sus Autoridades Competentes.

ARTÍCULO 5
CLASIFICACIONES DE SEGURIDAD Y EQUIVALENCIAS

1. Las Partes asignarán a toda la Información Clasificada que se transmita o se genere en el marco del presente Acuerdo el mismo grado de protección de seguridad previsto para su propia Información Clasificada de grado equivalente.

2. El grado de clasificación de seguridad que se asigne a la Información Clasificada podrá determinarse, modificarse o desclasificarse únicamente por la Parte de Origen, que comunicará sin demora dichas decisiones por escrito a la Parte Receptora, con el fin de que se adopten las medidas oportunas relativas a la seguridad.

3. Las Partes convienen en que los siguientes grados de clasificación de seguridad son equivalentes y corresponden a los grados de clasificación de seguridad especificados en la siguiente tabla:

ESPAÑA	SERBIA
SECRETO	ДРЖАВНА ТАЈНА
RESERVADO	СТРОГО ПОВЕРЉИВО
CONFIDENCIAL	ПОВЕРЉИВО
DIFUSIÓN LIMITADA	ИНТЕРНО

ARTÍCULO 6
DISPOSICIONES RELATIVOS A LA SEGURIDAD

1. El acceso a la Información Clasificada de grado CONFIDENCIAL / ПОВЕРЉИВО o superior estará limitado a las personas que tengan "necesidad de conocer" para el desempeño de sus funciones, hayan sido autorizadas por las autoridades pertinentes y estén en posesión de una Habilitación Personal de Seguridad del grado correspondiente. El acceso a la Información Clasificada de grado DIFUSIÓN LIMITADA / ИНТЕРНО estará limitado a las personas que tengan "necesidad de conocer" y hayan sido debidamente autorizadas e instruidas para ello.

2. La Parte Receptora no transmitirá Información Clasificada a Terceros o a cualesquiera personas o entidades públicas o privadas que sean nacionales de un Tercero sin la autorización previa por escrito de la Parte de Origen.

3. La Información Clasificada no podrá utilizarse para fines distintos de aquellos para los que fue transmitida, sobre la base de acuerdos firmados entre las Partes, incluidos los Contratos Clasificados.

4. Con el fin de alcanzar y mantener niveles de seguridad similares, las respectivas Autoridades Competentes se facilitarán mutuamente, si así se les solicita, información sobre sus normas de seguridad, procedimientos y prácticas para la protección de la Información Clasificada.

5. Las Autoridades Competentes se informarán recíprocamente de las medidas existentes para la protección de la Información Clasificada que se transmita o se genere al amparo del presente Acuerdo.

ARTÍCULO 7
HABILITACIONES DE SEGURIDAD

1. Previa solicitud, las Autoridades Competentes de las Partes, teniendo en cuenta sus leyes y reglamentos nacionales, se prestarán asistencia mutua durante los procedimientos de habilitación de sus nacionales que residan en el territorio de la otra Parte o de sus establecimientos que estén localizados en él.

2. Las Habilitaciones Personales de Seguridad y las Habilitaciones de Seguridad de Establecimiento expedidas con arreglo a las leyes y reglamentos de una Parte se reconocerán por la otra Parte. La equivalencia de las habilitaciones de seguridad se ajustará a lo dispuesto en el artículo 5 del presente Acuerdo.

3. Las Autoridades Competentes se informarán mutuamente sobre cualquier modificación que se produzca en relación con una Habilitación Personal de Seguridad o una Habilitación de Seguridad de Establecimiento, en particular, en caso de retirada o rebaja del grado de clasificación.

ARTÍCULO 8
TRADUCCIÓN Y REPRODUCCIÓN

1. La Información clasificada con el grado SECRETO / ДРЖАВНА ТАЈНА solo podrá traducirse o reproducirse previo consentimiento escrito de la Parte de Origen.

2. Las traducciones y reproducciones de Información Clasificada se realizarán con arreglo a los siguientes procedimientos:

   a) Las personas responsables de la traducción o reproducción de la Información Clasificada deberán contar con la Habilitación Personal de Seguridad pertinente, cuando sea necesaria;

   b) Toda reproducción y traducción de Información Clasificada llevará la marca de clasificación original y será objeto de la misma protección que los originales;

   c) El número de reproducciones se limitará al requerido para fines oficiales;

   d) En las traducciones figurará una anotación, en la lengua de traducción, en la que se haga constar que contiene Información Clasificada de la Parte de Origen.

ARTÍCULO 9
DESTRUCCIÓN DE INFORMACIÓN CLASIFICADA

1. La Información Clasificada de grado CONFIDENCIAL / ПОВЕРЉИВО e inferior se destruirá de modo que se impida su reconstrucción, conforme a las respectivas leyes y reglamentos nacionales.

2. La Información Clasificada marcada como RESERVADO / СТРОГО ПОВЕРЉИВО se destruirá de modo que se impida su reconstrucción, de conformidad con las respectivas leyes y reglamentos nacionales, y previa aprobación por escrito de la Parte de Origen.

3. La Información Clasificada marcada SECRETO / ДРЖАВНА ТАЈНА no podrá destruirse. Deberá devolverse a la Parte de Origen.

4. En caso de producirse una situación de crisis, la Información Clasificada que resulte imposible proteger o devolver a la Parte de Origen se destruirá inmediatamente. La Parte Receptora notificará por escrito a la Parte de Origen la destrucción de la Información Clasificada.

ARTÍCULO 10
TRANSMISIÓN ENTRE LAS PARTES

1. Las Partes se transmitirán la Información Clasificada por conducto diplomático o por cualquier otro cauce seguro mutuamente aprobado por sus Autoridades Competentes, conforme a las respectivas leyes y reglamentos nacionales.

2. Cuando la transmisión se realice mediante un correo, éste debe contar con la Habilitación de Seguridad correspondiente, conocer sus responsabilidades y estar en posesión de un certificado de correo expedido por la Autoridad Competente de la Parte que transmita la Información Clasificada.

3. Las partes podrán transmitir Información Clasificada de grado DIFUSIÓN LIMITADA / ИНТЕРНО por medios electrónicos con arreglo a los procedimientos de seguridad mutuamente aprobados por las Autoridades Competentes de las Partes.

4. Los servicios de seguridad e inteligencia de las Partes podrán intercambiar directamente Información Clasificada en el marco de sus actividades, de conformidad con lo dispuesto en el presente Acuerdo y en las leyes y reglamentos nacionales aplicables.

ARTÍCULO 11
DISPOSICIONES DE SEGURIDAD EN EL ÁMBITO INDUSTRIAL

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

   a) si los establecimientos de aquéllos cuentan con capacidad para proteger adecuadamente la Información Clasificada y con la Habilitación de Seguridad de Establecimiento para manejar la Información Clasificada del grado correspondiente;

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

   c) 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 aplicables de la Parte Receptora.

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

3. Todo Contrato Clasificado deberá contener disposiciones sobre los requisitos de seguridad y sobre la clasificación de cada uno de sus pormenores y elementos. Se remitirá una copia de los requisitos de seguridad de todos los Contratos Clasificados a la Autoridad Competente de la Parte en que vaya a realizarse el trabajo, para permitir la supervisión y el control adecuados de las normas, los procedimientos y las prácticas de seguridad establecidos por los Contratistas para la protección de la Información Clasificada.

4. En caso de celebrarse negociaciones precontractuales, la Autoridad Competente correspondiente informará a la Autoridad Competente de la otra Parte sobre la clasificación de seguridad asignada a la Información Clasificada relativa a las negociaciones precontractuales.

ARTÍCULO 12
VISITAS

1. Las visitas que impliquen acceder a Información Clasificada estarán sujetas a la autorización previa de la Autoridad Competente de la Parte anfitriona.

2. Los visitantes deberán haber sido adecuadamente habilitados por la Autoridad Competente de la Parte visitante de conformidad con las leyes y reglamentos nacionales.

3. La Autoridad Competente de la Parte visitante informará sobre la visita programada a la Autoridad Competente de la Parte anfitriona mediante un Modelo de Solicitud de Visita.

4. La solicitud de visita incluirá los siguientes datos, como mínimo:

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

   b) el nombre, dirección, número de teléfono y fax, dirección de correo electrónico y punto de contacto de las autoridades, agencias o establecimientos que vayan a visitarse;

   c) un certificado de la Habilitación Personal de Seguridad y su validez, si procede;

   d) el objeto y finalidad de la visita;

   e) la fecha prevista y duración de la visita solicitada. En caso de visitas recurrentes deberá indicarse el periodo total que abarcarían las mismas;

   f) fecha, firma y sello oficial de la Autoridad Competente.

5. Una vez aprobada la visita, la Autoridad Competente de la Parte anfitriona facilitará una copia del Formulario de Solicitud de Visita al responsable de seguridad de la autoridad, establecimiento o agencia cuyas instalaciones vayan a visitarse.

6. La validez de las autorizaciones de visita no excederá de un ano.

7. Las Autoridades Competentes podrán acordar un listado de visitantes con derecho a efectuar visitas recurrentes. Una vez aprobado el listado por las respectivas Autoridades Competentes, las visitas podrán organizarse directamente entre los establecimientos interesados, de conformidad con las condiciones estipuladas.

ARTÍCULO 13
INFRACCIÓN DE SEGURIDAD

1. Si se produce una divulgación no autorizada, apropiación indebida o pérdida de la Información Clasificada en el marco del presente Acuerdo, o se sospecha que se ha producido dicha infracción, se informará inmediatamente por escrito a la Autoridad Competente de la Parte de Origen.

2. La Autoridad 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. Si así se le solicita, la otra Parte prestará la asistencia pertinente y se informará a ésta del resultado de las actuaciones y de las medidas adoptadas para evitar futuras infracciones de seguridad.

3. Cuando la infracción de seguridad se haya producido en un Tercero, la Autoridad Competente de la Parte que envía la Información Clasificada adoptará sin dilación las medidas mencionadas en el apartado 1 de este artículo.

ARTÍCULO 14
GASTOS

1. Como norma general, la aplicación del presente Acuerdo no generará gasto alguno.

2. En caso de producirse, cada una de las Partes sufragará sus propios gastos ocasionados durante la aplicación del presente Acuerdo y su supervisión.

ARTÍCULO 15
SOLUCIÓN DE CONTROVERSIAS

Cualquier controversia relativa a la interpretación o aplicación de las disposiciones del presente Acuerdo se resolverá mediante consultas y negociaciones entre las Partes.

ARTÍCULO 16
ACUERDOS DE IMPLEMENTACIÓN

Podrán celebrarse Acuerdos de Implementación para la aplicación del presente Acuerdo entre las Autoridades Competentes.

ARTÍCULO 17
DISPOSICIONES FINALES

1. El presente Acuerdo se celebra por un periodo indefinido y entrará en vigor en 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 requisitos jurídicos internos necesarios para su entrada en vigor.

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

3. Cada Parte podrá denunciar el presente acuerdo mediante notificación previa por escrito a la otra Parte por conducto diplomático. En tal caso, el presente Acuerdo terminará seis (6) meses después de la fecha en la que la otra Parte haya recibido la notificación de denuncia.

4. En caso de terminación del presente Acuerdo, toda la Información Clasificada cedida o generada conforme al mismo continuará protegida de conformidad con las disposiciones del mismo hasta que la Parte de Origen exima por escrito a la Parte Receptora de dicha obligación.

Hecho en Madrid, el 13 de marzo de 2014 en dos originales en español y serbio, siendo todos los textos igualmente auténticos.

Por el Reino de España

FÉLIX SANZ ROLDÁN
Secretario de Estado Director del Centro Nacional de Inteligencia

Por la República de Serbia

Goran Matic PhD
Director de la Oficina del Consejo Nacional de Seguridad y Protección de Información Clasificada

[TRANSLATION – TRADUCTION]

AGREEMENT BETWEEN THE KINGDOM OF SPAIN AND THE REPUBLIC OF SERBIA ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Kingdom of Spain and the Republic of Serbia, hereinafter referred to as the "Parties",

Desirous to guarantee the protection of classified information generated or exchanged between the Parties, or between public or private entities under their jurisdiction,

Have agreed as follows:

Article 1. Purpose

This Agreement establishes that both Parties shall adopt the measures necessary to guarantee the protection of classified information exchanged or generated under this Agreement, in accordance with their domestic laws and regulations, and observing their national interests and security.

Article 2. Scope of application

1. This Agreement sets out procedures for the protection of classified information generated or exchanged between the Parties, or between public or private entities under their jurisdiction.

2. Neither Party shall invoke this Agreement to obtain classified information which the other Party has received from a third party.

Article 3. Definitions

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

1. "Classified contract" shall mean any contract or sub-contract, including pre-contractual negotiations, which contains classified information or involves access to such information;

2. "Classified information" shall mean any information or material, for which the need has been identified to protect it from unauthorized disclosure and which has been designated as such by means of a security classification in accordance with domestic laws and regulations;

3. "Competent authority" shall mean the authority designated by each Party as being responsible for the application and monitoring of this Agreement;

4. "Contractor" shall mean any legal person endowed with the legal capacity to conclude contracts within the scope of the provisions of this Agreement;

5. "Facility security clearance" shall mean the positive decision, issued by the competent authority, pursuant to which a facility possesses, from a security point of view, the material and organizational capacity to handle or store classified information, in accordance with its respective domestic laws and regulations;

6. "Need-to-know" shall mean the need to access classified information for the purpose of performing a particular official role and to conduct a specific task;

7. “Originating Party” shall mean the Party in which the classified information is generated or which transmits it to the other Party;

8. “Personnel security clearance” shall mean a positive decision, issued by the competent authority in accordance with domestic laws and regulations, by which it is concluded that a person may have access to classified information;

9. “Receiving Party” shall mean the Party that receives the classified information generated or transmitted by the other Party;

10. “Third party” shall mean any State or international organization that is not a party in this Agreement.

Article 4. Competent authorities

1. For the purpose of applying this Agreement, the competent authorities shall be:

For the Kingdom of Spain:

Secretary of State,

Director of the National Intelligence Centre, National Security Office

For the Republic of Serbia:

Office of the National Security Council and Protection of Classified Information

2. The Parties shall inform one another, via the diplomatic channel, of any changes to their domestic laws and regulations with regard to the responsibilities of their competent authorities.

Article 5. Security classifications and equivalences

1. The Parties shall assign to all classified information which is transmitted or generated within the framework of this Agreement the same level of security protection foreseen for their own classified information of equivalent level.

2. The level of security classification assigned to classified information may be determined, modified or declassified only by the originating Party, which shall communicate such decisions in writing and without delay to the receiving Party, in order for the appropriate measures concerning security to be adopted.

3. The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the following table:

Spain	Translation	Serbia	Translation
SECRETO	Secret	ДРЖАВНА ТАЈНА	State Secret
RESERVADO	Restricted	СТРОГО ПОВЕРЉИВО	Top Secret
CONFIDENCIAL	Confidential	ПОВЕРЉИВО	Secret
DIFUSIÓN LIMITADA	Restricted Distribution	ИНТЕРНО	Internal

Article 6. Provisions relating to security

1. Access to classified information graded CONFIDENCIAL/ПОВЕРЉИВО or above shall be restricted to persons who have the "need-to-know" for the purpose of performing their duties, who have been authorized by the pertinent authorities and who hold a personnel security clearance of the corresponding grade. Access to classified information graded DIFUSIÓN LIMITADA/ИНТЕРНО shall be restricted to persons who have the "need-to-know" and who have been duly authorized and instructed to that end.

2. The receiving Party shall not transmit classified information to third parties or any public or private persons or entities that are nationals of a third party without prior written authorization by the originating Party.

3. Classified information may not be used for purposes other than those for which it was transmitted on the basis of agreements signed between Parties, including classified contracts.

4. For the purpose of achieving and maintaining similar security levels, the respective competent authorities shall provide one another, if requested of them, information about their security standards, procedures and practices for protecting classified information.

5. The competent authorities shall inform one another about the existing measures for the protection of the classified information transmitted or generated within the scope of this Agreement.

Article 7. Security clearances

1. Upon request, the competent authorities of the Parties, having taken into account their domestic laws and regulations, shall assist one another during the vetting procedures of their nationals living, or of their facilities located, in the territory of the other Party.

2. The personnel security clearances and the facility security clearances issued under the laws and regulations of one Party shall be recognized by the other Party. The equivalence of the security clearances shall be adjusted to the provisions of article 5 of this Agreement.

3. The competent authorities shall inform one another of any change concerning a personnel security clearance or a facility security clearance, particularly where the classification level is withdrawn or downgraded.

Article 8. Translation and reproduction

1. Classified information graded SECRETO/ДРЖАВНА ТАЈНА may only be translated or reproduced with the prior written consent of the originating Party.

2. Translations and reproductions of classified information shall be carried out in accordance with the following procedures:

(a) The persons responsible for the translation or reproduction of the classified information must hold the appropriate personnel security clearance, where necessary;

(b) All reproductions and translations of classified information shall carry the original classification marking and shall be subject to the same protection as the originals;

(c) The number of reproductions shall be limited to that required for official purposes;

(d) Translations shall carry a note, in the language of translation, stating that it contains classified information belonging to the originating Party.

Article 9. Destruction of classified information

1. Classified information graded CONFIDENCIAL/ПОВЕРЉИВО or below shall be destroyed in such a manner as to prevent its reconstruction, in accordance with the respective domestic laws and regulations.

2. Classified information graded RESERVADO/СТРОГО ПОВЕРЉИВО shall be destroyed in such a manner as to prevent its reconstruction, in accordance with the respective domestic laws and regulations, and subject to the prior written consent of the originating Party.

3. Classified information graded SECRETO/ДРЖАВНА ТАЈНА may not be destroyed. It must be returned to the originating Party.

4. In the event of a crisis situation, classified information which cannot be protected or returned to the originating Party shall be destroyed immediately. The receiving Party shall notify the originating Party in writing of the destruction of the classified information.

Article 10. Transmission between the Parties

1. The Parties shall transmit classified information to one another through the diplomatic channel or through any other secure channel mutually approved by the competent authorities, in accordance with the respective domestic laws and regulations.

2. Where transmission is via a courier, the latter must hold the appropriate personnel security clearance, know his or her responsibilities and possess a courier certificate issued by the competent authority of the Party that is transmitting the classified information.

3. The Parties may transmit classified information graded DIFUSIÓN LIMITADA/ИНТЕРНО by electronic means in accordance with security procedures mutually agreed upon by the competent authorities of the Parties.

4. The security and intelligence services of the Parties may exchange classified information directly within the course of their activities, in accordance with the provisions of this Agreement and of the applicable domestic laws and regulations.

Article 11. Security provisions in the area of industry

1. Prior to providing classified information concerning a classified contract to a contractor, sub-contractor or possible contractor, the competent authority of the receiving Party shall inform the competent authority of the originating Party about the following:

(a) Whether their facilities have the capacity to adequately protect the classified information and the facility security clearance to handle classified information of the corresponding level;

(b) Whether their personnel hold the appropriate level of personnel security clearance to perform duties which require access to the classified information;

(c) Whether all those with access to the classified information have been informed about the responsibilities and obligations which apply to them with regard to protecting the classified information in accordance with the applicable laws and regulations of the receiving Party.

2. Each competent authority may request that a security inspection be carried out at a facility to ensure permanent compliance with security standards in accordance with domestic laws and regulations.

3. Every classified contract shall contain provisions concerning the security requirements and classification of each of its details and elements. A copy of the security requirements of all the classified contracts shall be sent to the competent authority of the Party in which the work is to be carried out to allow suitable supervision and control of the security standards, procedures and practices established by the contractors for the protection of the classified information.

4. In the event of pre-contractual negotiations being held, the corresponding competent authority shall inform the competent authority of the other Party about the security classification assigned to the classified information relating to the pre-contractual negotiations.

Article 12. Visits

1. Visits which imply access to classified information shall be subject to the prior authorization of the competent authority of the host Party.

2. The visitors must have been adequately vetted by the competent authority of the visiting Party in accordance with the domestic laws and regulations.

3. The competent authority of the visiting Party shall inform the competent authority of the host Party about the planned visit by means of a visit request form.

4. The request shall include the following data as a minimum:

(a) First name and surname of the visitor, official position, date and place of birth, nationality and identity card or passport number;

(b) Name, address, telephone and fax numbers, email address and point of contact of the authorities, agencies or facilities to be visited;

(c) A personnel security clearance certificate and its period of validity, if appropriate;

(d) The aim and purpose of the visit;

(e) The planned date and duration of the visit. In the cases of recurring visits, the total period covered by the visits must be stated;

(f) Date, signature and seal of the competent authority.

5. Once the visit has been approved, the competent authority of the host Party shall provide a copy of the visit request form to the person responsible for security at the authority, facility or agency whose installations are to be visited.

6. Visitors' permits shall be valid for no more than one year.

7. The competent authorities may agree on a list of visitors authorized to make recurring visits. Once the list has been approved by the respective competent authorities, the visits can be organized directly with the facilities in question, in accordance with the conditions stipulated.

Article 13. Breach of security

1. If an unauthorized disclosure, improper appropriation or loss of classified information occurs within the framework of this Agreement, or such a breach is suspected, the competent authority of the originating Party shall be informed in writing immediately.

2. The competent authority shall immediately launch an investigation and shall adopt all measures deemed appropriate, in accordance with domestic laws and regulations, with the aim of limiting the consequences of the aforementioned breach. If requested of it, the other Party shall provide relevant assistance and this Party shall be informed about the result of the actions and measures adopted to prevent future security breaches.

3. Where the security breach has taken place in a third party, the competent authority of the Party that transmitted the classified information shall adopt without delay the measures mentioned in paragraph 1 of this article.

Article 14. Costs

1. As a general rule, the application of this Agreement shall not generate any costs.

2. Should costs be incurred, each Party shall bear its own costs arising from the application of this Agreement and the monitoring thereof.

Article 15. Settlement of disputes

Any dispute arising from the interpretation or application of the provisions of this Agreement shall be settled by means of consultations and negotiations between the Parties.

Article 16. Implementation agreements

Implementation agreements may be concluded between the competent authorities for the purpose of applying this Agreement.

Article 17. Final provisions

1. This Agreement shall be valid for a period of indefinite duration and shall enter into force on the date of receipt of the last written notification by means of which the Parties inform one another, via the diplomatic channel, that their domestic legal requirements for its entry into force have been completed.

2. This Agreement may be amended at any time, at the request of either Party, with the mutual written consent of both Parties. The amendments shall enter into force in accordance with the provisions of paragraph 1 of this article.

3. Either Party may terminate this Agreement by means of a prior written notice to the other Party, sent through the diplomatic channel. In that case, this Agreement shall end six months after the date on which the other Party received the notice of termination.

4. In the event of this Agreement being terminated, all classified information provided or generated in accordance with the Agreement shall continue to be protected under the provisions of the Agreement until the originating Party releases, in writing, the receiving Party of such obligation.

DONE at Madrid, on 13 March 2014, in two originals in Spanish and Serbian, each text being equally authentic.

For the Kingdom of Spain:

FÉLIX SANZ ROLDÁN
Secretary of State
Director of the National Intelligence Centre

For the Republic of Serbia:

GORAN MATIC
Director of the Office of the National Security Council
and Protection of Classified Information

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE ROYAUME D'ESPAGNE ET LA RÉPUBLIQUE DE SERBIE RELATIF À L'ÉCHANGE ET LA PROTECTION RÉCIPROQUE DES INFORMATIONS CLASSIFIÉES

Le Royaume d'Espagne et la République de Serbie, ci-après dénommés les « Parties »,

Désireux de garantir la protection de l'information classifiée générée ou échangée entre les Parties, ou entre des entités publiques ou privées relevant de leur compétence,

Sont convenus de ce qui suit :

Article premier. Objet

Aux termes du présent Accord, les deux Parties adoptent les mesures nécessaires pour garantir la protection de l'information classifiée qui est échangée ou générée en vertu du présent Accord, conformément à leurs lois et règlements nationaux et dans le respect de leurs intérêts et sécurité nationaux.

Article 2. Champ d'application

1. Le présent Accord établit les procédures à appliquer pour la protection de l'information classifiée qui est générée ou échangée entre les Parties, ou entre des entités publiques ou privées relevant de leur compétence.

2. Ni l'une ni l'autre des Parties ne peut invoquer le présent Accord pour obtenir une information classifiée que l'autre Partie a reçue d'un tiers.

Article 3. Définitions

Aux fins du présent Accord :

1. L'expression « contrat classifié » désigne tout contrat ou sous-contrat, y compris les négociations précontractuelles, qui contient une information classifiée ou implique l'accès à celle-ci;

2. L'expression « information classifiée » désigne toute information ou tout matériel qu'il a été jugé nécessaire de protéger contre la divulgation non autorisée et qui a été ainsi désigné au moyen d'une classification de sécurité, conformément aux lois et règlements nationaux;

3. L'expression « autorité compétente » désigne l'autorité désignée par chaque Partie comme responsable de l'application et du suivi du présent Accord;

4. Le terme « contractant » désigne toute personne morale ayant la capacité juridique de conclure des contrats en vertu des dispositions du présent Accord;

5. L'expression « habilitation de sécurité d'établissement » désigne la détermination positive, émise par l'autorité compétente, selon laquelle un établissement possède, sur le plan de la sécurité, la capacité matérielle et organisationnelle de gérer ou de stocker des informations classifiées, conformément à ses lois et règlements nationaux;

6. L'expression « besoin d'en connaître » désigne le besoin d'accéder à une information classifiée pour l'exercice d'une charge officielle déterminée et pour la réalisation d'une tâche spécifique;

7. L'expression « Partie d'origine » désigne la Partie dans laquelle l'information classifiée est générée ou qui la transmet à l'autre Partie;

8. L'expression « habilitation personnelle de sécurité » désigne une détermination positive, émise par l'autorité compétente conformément aux lois et règlements nationaux, selon laquelle une personne peut avoir accès à une information classifiée;

9. L'expression « Partie réceptrice » désigne la Partie qui reçoit une information classifiée générée ou transmise par l'autre Partie;

10. Le terme « tiers » désigne tout État ou toute organisation internationale qui n'est pas Partie au présent Accord.

Article 4. Autorités compétentes

1. Les autorités compétentes pour l'application du présent Accord sont :

Pour le Royaume d'Espagne :
Le Secrétariat d'État,
Directeur du Centre national du renseignement
Bureau national de sécurité

Pour la République de Serbie :
Le Bureau du Conseil national de la sécurité et de la protection de l'information classifiée

2. Les Parties s'informent mutuellement, par la voie diplomatique, de toute modification qui se produirait dans leurs lois et règlements nationaux en rapport avec les responsabilités de leurs autorités compétentes.

Article 5. Classifications de sécurité et équivalences

1. Les Parties accordent à toute information classifiée qui est transmise ou générée dans le cadre du présent Accord le même niveau de protection qu'elles accordent à leur propre information classifiée ayant un niveau équivalent.

2. Le niveau de classification de sécurité accordé à l'information classifiée ne peut être déterminé, modifié ou déclassifié que par la Partie d'origine, laquelle communique les décisions correspondantes, sans délai, à la Partie réceptrice, afin que soient adoptées les mesures opportunes concernant la sécurité.

3. Les Parties conviennent que les niveaux de classification de sécurité suivants sont équivalents et correspondent aux niveaux de classification de sécurité spécifiés dans le tableau ci-après :

Espagne	Traduction	Serbie	Traduction
SECRETO	Secret	ДРЖАВНА ТАЈНА	Secret d'État
RESERVADO	Restreint	СТРОГО ПОВЕРЉБИВО	Très secret
CONFIDENCIAL	Confidentiel	ПОВЕРЉИВО	Secret
DIFUSIÓN LIMITADA	Diffusion limitée	ИНТЕРНО	Interne

Article 6. Dispositions relatives à la sécurité

1. L'accès à l'information classifiée de niveau CONFIDENCIAL/ПОВЕРЉИВО ou supérieur est limité aux personnes qui ont « besoin d'en connaître » pour l'exercice de leurs fonctions, y ont été autorisées par les autorités pertinentes et détiennent une habilitation personnelle de sécurité du niveau correspondant. L'accès à l'information classifiée de niveau DIFUSIÓN LIMITADA/ИНТЕРНО est limité aux personnes qui ont « besoin d'en connaître », y ont été dûment autorisées et ont reçu des instructions à cet effet.

2. La Partie réceptrice ne transmet aucune information classifiée à de tierces parties ou à des personnes ou entités publiques ou privées, quelles qu'elles soient, qui sont des ressortissants d'une tierce partie, sans l'autorisation écrite préalable de la Partie d'origine.

3. L'information classifiée ne peut être utilisée à des fins différentes de celles pour lesquelles elle a été transmise, sur la base d'accords signés entre les Parties, y compris les contrats classifiés.

4. Dans le but d'atteindre et de maintenir des niveaux de sécurité similaires, les autorités compétentes respectives se fournissent mutuellement, si elles en reçoivent la demande, des informations au sujet de leurs règles de sécurité, procédures et pratiques en vue de la protection de l'information classifiée.

5. Les autorités compétentes s'informent réciproquement des mesures existantes en vue de la protection de l'information classifiée qui est transmise ou générée en vertu du présent Accord.

Article 7. Habilitations de sécurité

1. Sur demande préalable, les autorités compétentes des Parties se fournissent, compte tenu de leurs lois et règlements nationaux, une assistance mutuelle au cours des procédures d'habilitation de leurs ressortissants qui résident sur le territoire de l'autre Partie ou de leurs établissements s'y trouvant.

2. Les habilitations personnelles de sécurité et les habilitations de sécurité d'établissement délivrées conformément aux lois et règlements d'une Partie sont reconnues par l'autre Partie. L'équivalence des habilitations de sécurité s'ajuste aux dispositions de l'article 5 du présent Accord.

3. Les autorités compétentes s'informent mutuellement de toute modification ayant lieu en ce qui concerne une habilitation personnelle de sécurité ou une habilitation de sécurité d'établissement, particulièrement en cas de retrait ou de baisse du niveau de classification.

Article 8. Traduction et reproduction

1. L'information classifiée de niveau SECRETO/ДРЖАВНА ТАЈНА ne peut être traduite ou reproduite qu'avec le consentement écrit préalable de la Partie d'origine.

2. Les traductions et reproductions d'information classifiée s'effectuent conformément aux procédures suivantes :

a) Les personnes responsables de la traduction ou de la reproduction de l'information classifiée doivent disposer de l'habilitation personnelle de sécurité correspondante, lorsqu'elle est nécessaire;

b) Toute reproduction et traduction de l'information classifiée porte la marque de classification originelle et fait l'objet de la même protection que les originaux;

c) Le nombre des reproductions est limité à celui qui est requis à des fins officielles;

d) Dans toute traduction doit figurer une annotation, dans la langue de traduction, indiquant qu'elle contient une information classifiée de la Partie d'origine.

Article 9. Destruction d'information classifiée

1. L'information classifiée de niveau CONFIDENCIAL/ПОВЕРЉИВО et d'un niveau inférieur est détruite de manière à empêcher sa reconstitution, conformément aux lois et règlements nationaux correspondants.

2. L'information classifiée marquée RESERVADO/СТРОГО ПОВЕРЈБИВО est détruite de manière à empêcher sa reconstitution, conformément aux lois et règlements nationaux correspondants, avec l'approbation écrite préalable de la Partie d'origine.

3. L'information classifiée marquée SECRETO/ДРЖАВНА ТАЈНА ne peut être détruite. Elle doit être rendue à la Partie d'origine.

4. En situation de crise, l'information classifiée qu'il est impossible de protéger ou de rendre à la Partie d'origine est immédiatement détruite. La Partie réceptrice notifie à la Partie d'origine, par écrit, la destruction de l'information classifiée.

Article 10. Transmission entre les Parties

1. Les Parties se transmettent l'information classifiée par la voie diplomatique ou par toute autre voie sûre approuvée mutuellement par leurs autorités compétentes, conformément aux lois et règlements nationaux correspondants.

2. Lorsque la transmission s'effectue par un messager, celui-ci doit être muni de l'habilitation de sécurité correspondante, connaître ses responsabilités et être en possession d'un certificat délivré par l'autorité compétente de la Partie qui transmet l'information classifiée.

3. Les Parties peuvent transmettre une information classifiée de niveau DIFUSIÓN LIMITADA/ИНТЕРНО par des moyens électroniques, conformément aux procédures de sécurité approuvées d'un commun accord par les autorités compétentes des Parties.

4. Les services de sécurité et de renseignements des Parties peuvent échanger directement des informations classifiées dans le cadre de leurs activités, conformément aux dispositions du présent Accord et aux lois et règlements nationaux applicables.

Article 11. Dispositions de sécurité dans le domaine industriel

1. Avant de fournir une information classifiée relative à un contrat classifié à un contractant, à un sous-traitant ou à un contractant éventuel, l'autorité compétente de la Partie réceptrice informe l'autorité compétente de la Partie d'origine de ce qui suit :

a) Si les établissements de ces personnes jouissent de la capacité de protéger adéquatement l'information classifiée et de l'habilitation de sécurité d'établissement permettant de gérer l'information classifiée du niveau correspondant;

b) Si son personnel jouit du niveau d'habilitation personnelle de sécurité nécessaire pour exercer des fonctions qui requièrent l'accès à l'information classifiée;

c) Si tous ceux qui ont accès à l'information classifiée ont été informés des responsabilités et obligations qui leur incombent en rapport avec la protection de cette information, conformément aux lois et règlements applicables de la Partie réceptrice.

2. Chaque autorité compétente peut demander qu'une inspection de sécurité soit effectuée dans un établissement pour garantir l'observation permanente des règles de sécurité conformément aux lois et règlements nationaux.

3. Tout contrat classifié doit contenir des dispositions sur les règles de sécurité et sur la classification de chacun de ses points particuliers et éléments. Une copie des règles de sécurité de tous les contrats classifiés est remise à l'autorité compétente de la Partie dans laquelle le travail est à réaliser, afin de permettre la supervision et le contrôle adéquats des règles, procédures et pratiques de sécurité établies par les contractants pour la protection de l'information classifiée.

4. Au cas où des négociations précontractuelles sont menées, l'autorité compétente correspondante informe l'autorité compétente de l'autre Partie de la classification de sécurité accordée à l'information classifiée relative aux négociations précontractuelles.

Article 12. Visites

1. Les visites qui impliquent l'accès à une information classifiée sont assujetties à l'autorisation préalable de l'autorité compétente de la Partie hôte.

2. Les visiteurs doivent avoir été adéquatement habilités par l'autorité compétente de la Partie effectuant la visite, conformément aux lois et règlements nationaux.

3. L'autorité compétente de la Partie désirant effectuer une visite informe l'autorité compétente de la Partie hôte de la visite prévue en utilisant à cet effet un formulaire de demande de visite.

4. La demande de visite inclut au moins les données suivantes :

a) Les nom et prénom du visiteur, sa fonction, la date et le lieu de sa naissance, sa nationalité et le numéro de son document d'identité ou de son passeport;

b) Le nom, l'adresse, les numéros de téléphone et de télécopieur, l'adresse de courrier électronique et le point de contact des autorités, organismes ou établissements à visiter;

c) Un certificat de l'habilitation personnelle de sécurité et sa validité, le cas échéant;

d) L'objet et le but de la visite;

e) La date prévue et la durée de la visite demandée. En cas de visites récurrentes, la durée totale des visites est à indiquer;

f) La date, la signature et le sceau officiel de l'autorité compétente.

5. Une fois la visite approuvée, l'autorité compétente de la Partie hôte fournit une copie du formulaire de demande de visite au responsable de la sécurité de l'autorité, de l'établissement ou de l'organisme dont les installations sont à visiter.

6. La validité des autorisations de visite ne doit pas dépasser un an.

7. Les autorités compétentes peuvent convenir d'une liste de visiteurs ayant le droit d'effectuer des visites récurrentes. Une fois la liste approuvée par les autorités compétentes respectives, les visites peuvent être organisées directement entre les établissements intéressés, conformément aux conditions convenues.

Article 13. Infraction à la sécurité

1. La divulgation non autorisée, l'appropriation indue ou la perte d'une information classifiée dans le cadre du présent Accord, ou une telle infraction présumée, est immédiatement portée par écrit à la connaissance de l'autorité compétente de la Partie d'origine.

2. L'autorité compétente ouvre immédiatement une enquête et adopte toutes les mesures qui paraissent appropriées, conformément aux lois et règlements nationaux, afin de limiter les conséquences de l'infraction visée. L'autre Partie fournit, sur demande, l'assistance appropriée et est informée du résultat des actions et mesures adoptées afin d'éviter des infractions à la sécurité à l'avenir.

3. Lorsque l'infraction à la sécurité se produit chez un tiers, l'autorité compétente de la Partie qui envoie l'information classifiée adopte sans délai les mesures visées au paragraphe 1 du présent article.

Article 14. Frais

1. En règle générale, l'application du présent Accord n'entraîne aucun frais.

2. Au cas où des frais seraient entraînés, chacune des Parties se charge de ses propres frais survenus pendant l'application du présent Accord et sa supervision.

Article 15. Règlement des différends

Tout différend relatif à l'interprétation ou à l'application des dispositions du présent Accord est réglé par voie de consultations et de négociations entre les Parties.

Article 16. Accords de mise en œuvre

Des accords de mise en œuvre peuvent être conclus entre les autorités compétentes aux fins de l'application du présent Accord.

Article 17. Dispositions finales

1. Le présent Accord est conclu pour une période indéterminée et entre en vigueur à la date de la réception de la dernière des notifications écrites par lesquelles les Parties s'informent, par la voie diplomatique, de l'accomplissement des conditions juridiques internes requises à cette fin.

2. Le présent Accord peut être modifié à tout moment, à la demande de l'une ou l'autre des Parties, avec le consentement mutuel écrit des deux Parties. Les modifications entrent en vigueur conformément aux dispositions du paragraphe 1 du présent article.

3. L'une ou l'autre des Parties peut dénoncer le présent Accord, moyennant une notification écrite préalable transmise à l'autre Partie par la voie diplomatique. Dans ce cas, le présent Accord expire six mois après la date de réception de la notification par l'autre Partie.

4. En cas de dénonciation du présent Accord, toute information classifiée cédée ou générée selon ses termes continue d'être protégée conformément aux dispositions du présent Accord, tant que la Partie d'origine n'a pas dispensé la Partie réceptrice de cette obligation par écrit.

FAIT à Madrid, le 13 mars 2014, en deux exemplaires originaux, en langues espagnole et serbe, les deux textes faisant également foi.

Pour le Royaume d'Espagne :

FÉLIX SANZ ROLDÁN
Secrétaire d'État
Directeur du Centre national du renseignement

Pour la République de Serbie :

GORAN MATIC
Directeur du Bureau du Conseil national de la sécurité
et de la protection de l'information classifiée