No. 50843

Spain
and
Austria

Agreement between the Government of the Kingdom of Spain and the Federal Government of Austria concerning the exchange and mutual protection of classified information. Madrid, 14 November 2011

Entry into force: *1 January 2013, in accordance with article 16*

Authentic texts: *German and Spanish*

Registration with the Secretariat of the United Nations: *Spain, 1 May 2013*

Espagne
et
Autriche

Accord entre le Gouvernement du Royaume d'Espagne et le Gouvernement fédéral autrichien relatif à l'échange et à la protection réciproque des informations classifiées. Madrid, 14 novembre 2011

Entrée en vigueur : *1er janvier 2013, conformément à l'article 16*

Textes authentiques : *allemand et espagnol*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Espagne, 1er mai 2013*

[GERMAN TEXT – TEXTE ALLEMAND]

ABKOMMEN ZWISCHEN DER REGIERUNG DES KÖNIGREICHS SPANIEN UND DER ÖSTERREICHISCHEN BUNDESREGIERUNG ÜBER DEN AUSTAUSCH UND GEGENSEITIGEN SCHUTZ KLASSIFIZIERTER INFORMATIONEN

Die Regierung des Königreichs Spanien und die Österreichische Bundesregierung (im Weiteren "die Parteien" genannt),

In der Absicht, die Sicherheit aller klassifizierten Informationen zu gewährleisten, die gemäß dem jeweiligen innerstaatlichen Recht als solche eingestuft und der anderen Partei übermittelt werden,

Von dem Wunsch geleitet, eine Regelung über den gegenseitigen Schutz klassifizierter Informationen zu schaffen, die im Zuge der Zusammenarbeit zwischen den Parteien ausgetauscht werden oder entstehen,

Sind wie folgt übereingekommen:

ARTIKEL 1 BEGRIFFSBESTIMMUNGEN

Im Sinne dieses Abkommens:

(1) **"Klassifizierte Informatione"** sind jegliche Informationen oder Materialien, unabhängig von ihrer Form, die gemäß dem jeweiligen innerstaatlichen Recht als solche eingestuft und gekennzeichnet worden sind, um ihren Schutz vor unbefugter Preisgabe, missbräuchlicher Verwendung oder Verlust zu gewährleisten;

(2) **"Zuständige Sicherheitsbehörde"** bedeutet die gemäß Artikel 13 notifizierten Behörden oder Stellen;

(3) **"Sicherheitsunbedenklichkeitsbescheinigung für Personen"** ist die Entscheidung der zuständigen Sicherheitsbehörde, dass eine natürliche Person zum Zugang zu klassifizierten Informationen berechtigt ist;

(4) **"Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen"** ist die Entscheidung der zuständigen Sicherheitsbehörde, dass ein

Unternehmen und Einrichtungen, zum Umgang mit klassifizierten Informationen berechtigt sind;

(5) **"Herausgeber"** ist eine Partei sowie jede ihrer Hoheitsgewalt unterstehende Person des privaten oder öffentlichen Rechts, die klassifizierte Informationen herausgibt;

(6) **"Empfänger"** ist eine Partei sowie jede ihrer Hoheitsgewalt unterstehende Person des privaten oder öffentlichen Rechts, an die klassifizierte Informationen herausgegeben werden;

(7) **"Klassifizierter Vertrag"** ist ein Vertrag oder Untervertrag zwischen einer Behörde, einer Stelle oder einem Unternehmen vom Staat der einen Partei (Auftraggeber) und einer Behörde, einer Stelle oder einem Unternehmen vom Staat der anderen Partei (Auftragnehmer), dessen Erfüllung den Zugang zu klassifizierten Informationen oder deren Herstellung erfordert;

(8) **"Dritte"** sind jegliche Staaten oder internationale Organisationen, die nicht Partei dieses Abkommens sind.

ARTIKEL 2
GLEICHWERTIGKEIT DER KLASSIFIZIERUNGSSTUFEN

Die Parteien kommen über die Gleichwertigkeit der folgenden Klassifizierungsstufen überein:

Königreich Spanien	Republik Österreich
SECRETO	STRENG GEHEIM
RESERVADO	GEHEIM
CONFIDENCIAL	VERTRAULICH
DIFUSIÓN LIMITADA	EINGESCHRÄNKT

ARTIKEL 3
KENNZEICHNUNG

(1) Klassifizierte Informationen, die übermittelt werden sollen, werden vom Herausgeber gemäß der entsprechenden Klassifizierungsstufe in den Sprachen beider Parteien gekennzeichnet.

(2) Klassifizierte Informationen, die im Zuge der unter dieses Abkommen fallenden Zusammenarbeit hergestellt oder vervielfältigt werden, werden ebenso gekennzeichnet.

(3) Die Klassifizierungsstufe wird ausschließlich vom Herausgeber geändert oder aufgehoben. Der Empfänger wird über jegliche Änderung oder Aufhebung unverzüglich unterrichtet.

ARTIKEL 4
GRUNDSÄTZE DES SCHUTZES KLASSIFIZIERTER INFORMATIONEN

(1) Die Parteien treffen gemäß diesem Abkommen und dem innerstaatlichen Recht einer der Parteien alle geeigneten Maßnahmen, um den Schutz der übermittelten klassifizierten Informationen zu gewährleisten, und sorgen für die erforderliche Kontrolle dieses Schutzes.

(2) Die Parteien gewährleisten übermittelten klassifizierten Informationen mindestens den gleichen Schutzstandard, wie er eigenen klassifizierten Informationen der gleichwertigen Klassifizierungsstufe gewährleistet wird.

(3) Übermittelte klassifizierte Informationen werden nur zu dem Zweck, für den sie freigegeben wurden, verwendet und nur solchen Personen zugänglich gemacht, die gemäß dem jeweiligen innerstaatlichen Recht zum Zugang zu klassifizierten Informationen der gleichwertigen Klassifizierungsstufe ermächtigt sind und die diesen Zugang für die Erfüllung ihrer Aufgaben benötigen. Personen, die nicht Staatsangehörige einer der Staaten der Parteien sind, wird der Zugang zu solchen Informationen nur mit vorheriger schriftlicher Zustimmung des Herausgebers gewährt.

(4) Ein Empfänger gewährt Dritten oder einer Stelle, einem Unternehmen oder einer Person ohne schriftliche Zustimmung der zuständigen Sicherheitsbehörde des Herausgebers keinen Zugang zu klassifizierten Informationen.

(5) Klassifizierte Informationen, die im Zuge der unter dieses Abkommen fallenden Zusammenarbeit hergestellt werden, genießen den gleichen Schutz wie übermittelte klassifizierte Informationen.

ARTIKEL 5
SICHERHEITSUNBEDENKLICHKEITSBESCHEINIGUNGEN FÜR PERSONEN

(1) Zugang zu klassifizierten Informationen der Klassifizierungsstufen CONFIDENCIAL / VERTRAULICH und höher wird nur auf Grundlage einer Sicherheitsunbedenklichkeitsbescheinigung für Personen gemäß dem jeweiligen innerstaatlichen Recht gewährt.

(2) Bei im Zuge der Anwendung dieses Abkommens durchgeführten Sicherheitsüberprüfungen von Personen, die sich im anderen Staat aufhalten oder aufgehalten haben, unterstützen die zuständigen Sicherheitsbehörden einander gemäß dem jeweiligen innerstaatlichen Recht auf Ersuchen.

(3) Im Anwendungsbereich dieses Abkommens anerkennen die Parteien die von der anderen Partei ausgestellten Sicherheitsunbedenklichkeitsbescheinigungen für Personen.

(4) Im Anwendungsbereich dieses Abkommens informieren die zuständigen Sicherheitsbehörden einander unverzüglich über alle Änderungen von Sicherheitsunbedenklichkeitsbescheinigungen für Personen, insbesondere über einen Widerruf oder eine Änderung der Klassifizierungsstufe.

ARTIKEL 6
KLASSIFIZIERTE VERTRÄGE

(1) Ein klassifizierter Vertrag enthält Bestimmungen über die Sicherheitserfordernisse und über die Klassifizierung jeder seiner Aspekte oder Bestandteile.

(2) Im Zusammenhang mit klassifizierten Verträgen anerkennen die Parteien die von der anderen Partei ausgestellten Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen.

(3) Im Zusammenhang mit der Vorbereitung oder dem Abschluss klassifizierter Verträge informieren die zuständigen Sicherheitsbehörden einander auf Anfrage darüber, ob eine gültige Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen ausgestellt oder das entsprechende Verfahren eingeleitet wurde.

(4) Die zuständigen Sicherheitsbehörden informieren einander unverzüglich über jede Änderung von unter diesen Artikel fallenden Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen,

insbesondere über einen Widerruf oder eine Änderung der Klassifizierungsstufe.

(5) Der Auftraggeber übermittelt dem Auftragnehmer und der zuständigen Sicherheitsbehörde des Auftragnehmers die notwendigen Sicherheitserfordernisse des klassifizierten Vertrags, einschließlich einer Liste der klassifizierten Informationen, die übermittelt werden sollen.

ARTIKEL 7
ÜBERMITTLUNG

(1) Klassifizierte Informationen werden auf diplomatischem Wege oder auf andere zwischen den zuständigen Sicherheitsbehörden gemäß dem jeweiligen innerstaatlichen Recht vereinbarte Weise übermittelt. Werden Übermittlungen von Personen durchgeführt, besitzen diese eine Kurierbescheinigung.

(2) Klassifizierte Informationen können auf elektronischem Wege gemäß den zwischen den zuständigen Sicherheitsbehörden vereinbarten Sicherheitsverfahren übermittelt werden.

(3) Lieferungen großer Gegenstände oder Mengen klassifizierter Informationen werden zwischen den zuständigen Sicherheitsbehörden vereinbart und von ihnen auf den Einzelfall bezogen näher geregelt.

(4) Der Empfänger bestätigt den Empfang klassifizierter Informationen schriftlich.

ARTIKEL 8
VERVIELFÄLTIGUNG UND ÜBERSETZUNG

(1) Klassifizierte Informationen werden gemäß dem jeweiligen innerstaatlichen Recht vervielfältigt. Die Vervielfältigung klassifizierter Informationen durch den Empfänger kann von der zuständigen Sicherheitsbehörde des Herausgebers eingeschränkt oder ausgeschlossen werden.

(2) Klassifizierte Informationen der Klassifizierungsstufe SECRETO / STRENG GEHEIM werden nicht vervielfältigt und nur mit vorheriger schriftlicher Zustimmung der zuständigen Sicherheitsbehörde des Herausgebers übersetzt.

(3) Klassifizierte Informationen der Klassifizierungsstufen CONFIDENCIAL / VERTRAULICH und höher werden nur von Personen übersetzt, die die entsprechende Sicherheitsunbedenklichkeitsbescheinigung für Personen besitzen.

(4) Kopien und Übersetzungen werden wie Originale geschützt.

ARTIKEL 9
VERNICHTUNG

(1) Klassifizierte Informationen werden gemäß dem jeweiligen innerstaatlichen Recht nachweislich und auf eine Weise vernichtet, die eine vollständige oder teilweise Wiederherstellung nicht zulässt.

(2) Klassifizierte Informationen der Klassifizierungsstufe SECRETO / STRENG GEHEIM werden nicht vernichtet, sondern rückübermittelt.

(3) Klassifizierte Informationen der Klassifizierungsstufe RESERVADO / GEHEIM werden nur mit schriftlicher Zustimmung des Herausgebers vernichtet.

ARTIKEL 10
BESUCHE

(1) Besuchern wird nur im notwendigen Ausmaß und mit schriftlicher Genehmigung der zuständigen Sicherheitsbehörde der gastgebenden Partei Zugang zu klassifizierten Informationen sowie zu Einrichtungen, in denen klassifizierte Informationen bearbeitet oder aufbewahrt werden, gewährt. Die Erlaubnis wird nur solchen Personen erteilt, die gemäß dem jeweiligen innerstaatlichen Recht zum Zugang zu klassifizierten Informationen der entsprechenden Klassifizierungsstufe ermächtigt sind.

(2) Besuchsanträge werden mindestens zwanzig (20) Tage vor dem Besuch, in dringenden Fällen wenn möglich zehn (10) Tage vor dem Besuch, bei der zuständigen Sicherheitsbehörde gestellt. Die zuständigen Sicherheitsbehörden informieren einander über die Einzelheiten des Besuchs und gewährleisten den Schutz personenbezogener Daten.

(3) Besuchsanträge werden in englischer Sprache gestellt und enthalten insbesondere die folgenden Angaben:

a) Zweck und vorgesehenes Datum des Besuchs;

b) Vor- und Familienname, Geburtsdatum und –ort, Staatsangehörigkeit und Pass- oder Personalausweisnummer der Besucher;

c) Funktion der Besucher und Name der vertretenen Behörde oder Stelle oder des vertretenen Unternehmens;

d) Gültigkeit und Klassifizierungsstufe der Sicherheitsunbedenklichkeitsbescheinigung für Personen der Besucher;

e) Name, Adresse, Telefon- und Faxnummer, E-Mail-Adresse und Ansprechpartner der Behörden, Stellen oder Einrichtungen, die besucht werden sollen;

f) Datum des Antrags und Unterschrift der zuständigen Sicherheitsbehörde.

(4) Sobald der Besuch genehmigt wurde, übermittelt die zuständige Sicherheitsbehörde der gastgebenden Partei eine Kopie des Besuchsantrags an den Sicherheitsbeauftragten der Einrichtungen, die besucht werden sollen.

(5) Die Besuchsgenehmigungen sind höchstens über einen Zeitraum von zwölf (12) Monaten gültig.

(6) Hinsichtlich eines bestimmten klassifizierten Vertrags können die zuständigen Sicherheitsbehörden übereinkommen, eine Liste von Personen zu erstellen, die zu wiederkehrenden Besuchen berechtigt sind. Sobald solch eine Liste von den zuständigen Sicherheitsbehörden genehmigt wurde, ist diese anfänglich über einen Zeitraum von zwölf (12) Monaten gültig. Die Einzelheiten bestimmter Besuche auf Grundlage einer solchen Liste werden unmittelbar mit den Sicherheitsbeauftragten der Einrichtungen, die besucht werden sollen, geregelt.

ARTIKEL 11
SICHERHEITSVERLETZUNGEN

(1) Im Falle einer unbefugten Preisgabe, einer missbräuchlichen Verwendung oder eines Verlustes von unter dieses Abkommen fallenden klassifizierten Informationen oder eines entsprechenden Verdachts, wird die zuständige Sicherheitsbehörde des Herausgebers unverzüglich schriftlich informiert.

(2) Verletzungen der Bestimmungen über den Schutz unter dieses Abkommen fallender klassifizierter Informationen werden gemäß dem jeweiligen innerstaatlichen Recht untersucht und verfolgt. Die andere Partei leistet auf Ersuchen Unterstützung.

(3) Die Parteien informieren einander über das Ergebnis der Untersuchungen und die getroffenen Maßnahmen.

ARTIKEL 12
KOSTEN

Sollte die Durchführung dieses Abkommens Kosten verursachen, trägt jede Partei ihre eigenen Ausgaben.

ARTIKEL 13
ZUSTÄNDIGE SICHERHEITSBEHÖRDEN

Die Parteien teilen einander auf diplomatischem Wege die zuständigen Sicherheitsbehörden mit, die für die Durchführung dieses Abkommens verantwortlich sind.

ARTIKEL 14
KONSULTATIONEN

(1) Die zuständigen Sicherheitsbehörden informieren einander über das jeweilige innerstaatliche Recht über den Schutz klassifizierter Informationen und dessen Änderungen.

(2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die zuständigen Sicherheitsbehörden einander und ermöglichen die notwendigen gegenseitigen Besuche.

ARTIKEL 15
BEILEGUNG VON STREITIGKEITEN

Jegliche Streitigkeit über die Anwendung oder Auslegung dieses Abkommens wird im Wege direkter Gespräche zwischen den Parteien oder auf diplomatischem Wege beigelegt.

ARTIKEL 16
SCHLUSSBESTIMMUNGEN

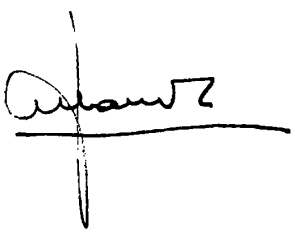
(1) Dieses Abkommen wird auf unbestimmte Zeit geschlossen und tritt am ersten Tag des zweiten Monats nach dem Tag in Kraft, an dem die Parteien einander den Abschluss der für das Inkrafttreten dieses Abkommens erforderlichen innerstaatlichen Verfahren mitgeteilt haben.

(2) Dieses Abkommen kann im gegenseitigen schriftlichen Einvernehmen beider Parteien geändert werden. Änderungen treten gemäß Absatz 1 in Kraft.

(3) Jede Partei kann dieses Abkommen jederzeit auf diplomatischem Wege kündigen. In einem solchen Fall tritt das Abkommen sechs (6) Monate nach Erhalt der Kündigungsnote durch die andere Partei außer Kraft. Wird das Abkommen gekündigt, so bleiben klassifizierte Informationen, die in Anwendung dieses Abkommens übermittelt oder hergestellt wurden, weiterhin nach den Bestimmungen dieses Abkommens geschützt.

Geschehen zu Madrid, am 14. November 2011 in zwei Urschriften jeweils in spanischer und deutscher Sprache, wobei beide Texte gleichermaßen authentisch sind.

Für die Regierung des Königreichs Spanien



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

Für die Österreichische Bundesregierung

RUDOLF LENNKH
Österreichischer Botschafter in Spanien

[SPANISH TEXT – TEXTE ESPAGNOL]

ACUERDO ENTRE EL GOBIERNO DEL REINO DE ESPAÑA Y EL GOBIERNO FEDERAL AUSTRIACO RELATIVO AL INTERCAMBIO Y PROTECCIÓN MUTUA DE LA INFORMACIÓN CLASIFICADA

El Gobierno del Reino de España y el Gobierno Federal de Austria (en lo sucesivo denominados "las Partes"),

Deseando garantizar la seguridad de toda la Información Clasificada designada como tal de conformidad con la normativa nacional de cada Parte y transmitida a la otra Parte,

Deseando ofrecer normas para la mutua protección de información clasificada intercambiada o generada en el curso de la cooperación entre las Partes,

Han convenido en lo siguiente:

ARTÍCULO 1 DEFINICIONES

Para los fines del presente Acuerdo:

(1) Por **"Información Clasificada"** se entenderá cualquier información o material, con independencia de su forma, denominada y marcada como tal de conformidad con la normativa nacional correspondiente de cada una de las Partes para garantizar su protección contra su divulgación no autorizada, su uso indebido o su pérdida;

(2) por **"Autoridad de Seguridad Competente"** se entenderán las autoridades o agencias que se hayan notificado de conformidad con el Artículo 13;

(3) por **"Habilitación Personal de Seguridad"** se entenderá la acreditación por la Autoridad de Seguridad Competente de que una persona física reúne los requisitos para tener acceso a Información Clasificada;

(4) por **"Habilitación de Seguridad para Establecimientos"** se entenderá la acreditación por la Autoridad de Seguridad Competente de que un

establecimiento o una institución tiene la capacidad para manejar Información Clasificada;

(5) por **"Parte de Origen"** se entenderá la Parte, así como cualquier otra entidad jurídica pública o privada bajo su jurisdicción, que proporcione la Información Clasificada;

(6) por **"Parte Receptora"** se entenderá la Parte, así como cualquier otra entidad jurídica pública o privada bajo su jurisdicción, a los que se transmita la Información Clasificada;

(7) por **"Contrato Clasificado"** se entenderá cualquier contrato o subcontrato entre cualquier autoridad, agencia o empresa del Estado de una Parte (Contratante) y cualquier autoridad, agencia o empresa del Estado de la otra Parte (Contratista) cuya ejecución suponga el acceso a Información Clasificada o la generación de la misma;

(8) por **"Tercero"** se entenderá todo Estado u organización internacional que no sea Parte en el presente Acuerdo.

ARTÍCULO 2
EQUIVALENCIA DE LOS NIVELES DE CLASIFICACIÓN DE SEGURIDAD

Las Partes acuerdan la siguiente equivalencia de los niveles de clasificación de seguridad:

Reino de España	República de Austria
SECRETO	STRENG GEHEIM
RESERVADO	GEHEIM
CONFIDENCIAL	VERTRAULICH
DIFUSIÓN LIMITADA	EINGESCHRÄNKT

ARTÍCULO 3
MARCADO

(1) La Información Clasificada que se transmita deberá estar marcada por la Parte de origen, de conformidad con el nivel de clasificación de seguridad pertinente, en los idiomas de ambas Partes.

(2) También debe marcarse la Información Clasificada que se genere o se reproduzca en el curso de la cooperación de conformidad con el presente Acuerdo.

(3) El nivel de clasificación de seguridad sólo podrá ser modificado o revocado por la Parte de origen. La Parte receptora deberá ser informada inmediatamente de toda modificación o revocación.

ARTÍCULO 4
PRINCIPIOS DE PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

(1) Las Partes adoptarán todas las medidas apropiadas, de conformidad con el presente Acuerdo y su normativa nacional propia, para garantizar la protección de la Información Clasificada que se transmita y ejercerá el necesario control de dicha protección.

(2) Las Partes otorgarán a la Información Clasificada que sea transmitida al menos el mismo nivel de protección que el que prestan a su propia Información Clasificada con un nivel de clasificación de seguridad equivalente.

(3) La Información Clasificada que se transmita se utilizará únicamente para el fin para el que se haya proporcionado y el acceso a la misma se limitará a las personas que hayan sido autorizadas de conformidad con la normativa nacional propia para tener acceso a Información Clasificada del nivel de clasificación de seguridad equivalente y tengan necesidad de conocerla para el ejercicio de sus obligaciones. El acceso a dicha información por personas que no sean ciudadanos de alguna de las Partes sólo tendrá lugar con el consentimiento previo y por escrito de la Parte de origen.

(4) La Parte Receptora no dará acceso a Información Clasificada a un Tercero ni a ninguna agencia, empresa o persona física sin el consentimiento por escrito de la Autoridad de Seguridad Competente de la Parte de origen.

(5) La Información Clasificada generada en el curso de la cooperación de conformidad con el presente Acuerdo disfrutará de la misma protección que la Información Clasificada que se transmita.

ARTÍCULO 5
HABILITACIÓN PERSONAL DE SEGURIDAD

(1) El acceso a la Información Clasificada de nivel de clasificación de seguridad CONFIDENCIAL / VERTRAULICH o superior se otorgará únicamente basándose en una Habilitación Personal de Seguridad conforme a la normativa nacional correspondiente a cada una de las Partes.

(2) Las Autoridades de Seguridad Competentes se asistirán mutuamente, previa petición y de conformidad con su normativa nacional propia cuando, en aplicación del presente Acuerdo, se lleven a cabo procedimientos de investigación de personas que residan o hayan residido en el otro Estado.

(3) En el ámbito del presente Acuerdo, las Partes reconocerán las Habilitaciones Personales de Seguridad expedidas por la otra Parte.

(4) En el ámbito del presente Acuerdo, las Autoridades de Seguridad Competentes se informarán mutuamente de forma inmediata acerca de cualquier modificación relacionada con Habilitaciones Personales de Seguridad, en especial acerca de una revocación o modificación del nivel de clasificación de seguridad.

ARTÍCULO 6
CONTRATOS CLASIFICADOS

(1) Un Contrato Clasificado deberá comprender disposiciones sobre los requisitos de seguridad y sobre la clasificación de cada uno de sus aspectos y elementos.

(2) En el contexto de los Contratos Clasificados las Partes deberán reconocer las Habilitaciones de Seguridad de Establecimiento expedidas por la otra Parte.

(3) En el contexto de la preparación o celebración de los Contratos Clasificados, las Autoridades de Seguridad Competentes se informarán mutuamente, previa petición, de si se ha expedido una Habilitación de Seguridad de Establecimiento válida o si se han iniciado los procedimientos oportunos para ello.

(4) Las Autoridades de Seguridad Competentes se informarán mutuamente y de forma inmediata sobre cualquier modificación respecto a Habilitaciones de Seguridad de Establecimiento comprendidas en el presente artículo, en especial respecto a la modificación o revocación del nivel de clasificación de seguridad.

(5) El Contratante deberá comunicar al Contratista y a la Autoridad de Seguridad Competente del Contratista los requisitos de seguridad necesarios del Contrato Clasificado, incluyendo una relación de la Información Clasificada que se transmita.

ARTÍCULO 7
TRANSMISIÓN

(1) La Información Clasificada se transmitirá por conducto diplomático, salvo que se acuerde otra cosa por las Autoridades de Seguridad Competentes de conformidad con las leyes y reglamentos nacionales de las Partes. Si las transmisiones son efectuadas en mano por personas físicas, éstas deben estar en posesión de un certificado que los acredite como mensajeros.

(2) La Información Clasificada podrá transmitirse electrónicamente de conformidad con los procedimientos de seguridad que hayan aprobado de mutuo acuerdo las Autoridades de Seguridad Competentes.

(3) El envío de objetos voluminosos o de grandes cantidades de Información Clasificada se acordará por ambas Autoridades de Seguridad Competentes y se regulará por ellas caso por caso.

(4) La Parte Receptora deberá confirmar por escrito la recepción de la Información Clasificada.

ARTÍCULO 8
REPRODUCCIÓN Y TRADUCCIÓN

(1) La reproducción de Información Clasificada se realizará de conformidad con la normativa nacional propia de las Partes. La Autoridad de Seguridad Competente de la Parte de Origen podrá restringir o excluir la reproducción de Información Clasificada por la Parte Receptora.

(2) La Información Clasificada de nivel de clasificación de seguridad SECRETO / STRENG GEHEIM no podrá reproducirse y sólo podrá traducirse si la Autoridad de Seguridad Competente de la Parte de Origen ha dado su consentimiento previo por escrito a tal efecto.

(3) La Información Clasificada de nivel de clasificación de seguridad CONFIDENCIAL / VERTRAULICH o superior sólo podrá traducirse por personas que ostenten la oportuna Habilitación Personal de Seguridad.

(4) Las copias y traducciones deberán protegerse de la misma forma que los originales.

ARTÍCULO 9
DESTRUCCIÓN

(1) La Información Clasificada deberá destruirse de conformidad con la normativa nacional propia de las Partes, de forma que pueda comprobarse y que no permita su reconstrucción total o parcial.

(2) La Información Clasificada de nivel de clasificación de seguridad SECRETO / STRENG GEHEIM no se destruirá sino que se devolverá.

(3) La Información Clasificada de nivel de clasificación de seguridad RESERVADO / GEHEIM sólo podrá destruirse con el consentimiento por escrito de la Parte de origen.

ARTÍCULO 10
VISITAS

(1) Los visitantes únicamente tendrán acceso a la Información Clasificada y a los establecimientos en los que se procesa o se conserva, en la medida necesaria y con la autorización por escrito de la Autoridad de Seguridad Competente de la Parte que reciba a los visitantes. El permiso sólo se concederá a personas autorizadas para tener acceso a la Información Clasificada del respectivo nivel de clasificación de seguridad de conformidad con la normativa nacional propia de cada Parte.

(2) Las solicitudes de visitas deberán presentarse a la Autoridad de Seguridad Competente de la Parte que reciba las visitas con una anterioridad de al menos veinte (20) días, y en casos urgentes de diez (10), de ser ello posible, a la fecha prevista para la visita. Las Autoridades de Seguridad Competentes deberán informarse mutuamente de los detalles de la visita y garantizar la protección de los datos personales.

(3) Las solicitudes de visitas se formularán en inglés y deberán establecer en especial lo siguiente:

a) finalidad y fecha prevista de la visita;

b) nombre y apellidos, lugar y fecha de nacimiento, nacionalidad y número de pasaporte o de carnet de identidad del visitante;

c) cargo de los visitantes y nombre de la autoridad, agencia o empresa que representan;

d) la validez y nivel de Habilitación Personal de Seguridad de los visitantes;

e) nombre, dirección, número de fax y teléfono, dirección de correo electrónico y punto de contacto de las autoridades, agencias o establecimientos que deseen visitar;

f) fecha de la solicitud y firma de la Autoridad de Seguridad Competente.

(4) Una vez que la visita haya sido aprobada, la Autoridad de Seguridad Competente de la Parte receptora de la visita deberá proporcionar una copia de la solicitud de visita a los oficiales de seguridad de los establecimientos que se deseen visitar.

(5) La validez de las autorizaciones de visita no deberá exceder de doce (12) meses.

(6) Las Autoridades de Seguridad Competentes podrán acordar establecer una lista de personas autorizadas para efectuar visitas periódicas en relación con un Contrato Clasificado determinado. Una vez que las Autoridades de Seguridad Competentes hayan aprobado una lista de estas características, tendrá validez por un período inicial de doce (12) meses. Los términos de las visitas concretas basadas en dicha lista se establecerán directamente con los oficiales de seguridad de los establecimientos que deban visitarse.

ARTÍCULO 11
INFRACCIÓN DE LA SEGURIDAD

(1) En caso de sospecha o descubrimiento de una revelación no autorizada, un uso indebido o pérdida de Información Clasificada comprendida en el ámbito del presente Acuerdo, la Autoridad de Seguridad Competente de la Parte de Origen deberá ser informada por escrito de forma inmediata.

(2) La infracción de las disposiciones sobre protección de la Información Clasificada comprendida en el ámbito del presente Acuerdo deberá ser investigada y perseguida de conformidad con la normativa nacional propia de las Partes. La otra Parte proporcionará su asistencia previa petición.

(3) Las Partes se informarán recíprocamente sobre el resultado de las investigaciones y las medidas adoptadas.

ARTÍCULO 12
GASTOS

En caso de que la aplicación del presente Acuerdo lleve aparejado algún coste, cada Parte sufragará sus propios gastos.

ARTÍCULO 13
AUTORIDADES DE SEGURIDAD COMPETENTES

Las Partes se notificarán mutuamente por conducto diplomático cuáles son las Autoridades de Seguridad Competentes responsables de la aplicación del presente Acuerdo.

ARTÍCULO 14
CONSULTAS

(1) Las Autoridades de Seguridad Competentes se informarán mutuamente de la respectiva normativa nacional sobre protección de Información Clasificada y de cualquier enmienda a la misma.

(2) Con la finalidad de garantizar una estrecha cooperación en la aplicación del presente Acuerdo, las Autoridades de Seguridad Competentes se consultarán recíprocamente y facilitarán las visitas mutuas necesarias.

ARTÍCULO 15
SOLUCIÓN DE CONTROVERSIAS

Toda controversia entre las Partes sobre la interpretación o aplicación del presente Acuerdo se resolverá mediante conversaciones directas entre las Partes o por conducto diplomático.

ARTÍCULO 16
DISPOSICIONES FINALES

(1) El presente Acuerdo se concluye por un periodo indefinido y entrará en vigor el primer día del segundo mes siguiente al día en que las Partes se hayan notificado recíprocamente que se han concluido los trámites legales internos para su entrada en vigor.

(2) El presente Acuerdo podrá modificarse mediante consentimiento mutuo por escrito de las Partes. Las enmiendas entrarán en vigor de conformidad con el párrafo 1.

(3) Cada Parte podrá denunciar el presente Acuerdo en cualquier momento por conducto diplomático. En tal caso, el Acuerdo expirará seis (6) meses después de la recepción de la notificación de denuncia por la otra Parte. En caso de denuncia, la Información Clasificada transmitida o generada al amparo del presente Acuerdo seguirá siendo protegida de conformidad con lo dispuesto en el mismo.

Hecho en Madrid el 11 de noviembre de 2011, en dos originales, en español y alemán, siendo ambos textos igualmente auténticos.

Por el Gobierno de España

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

Por el Gobierno Federal Austriaco

Dr. Rudolf Lennkh
Embajador de la República de
Austria en España

[TRANSLATION – TRADUCTION]

AGREEMENT BETWEEN THE GOVERNMENT OF THE KINGDOM OF SPAIN AND THE FEDERAL GOVERNMENT OF AUSTRIA CONCERNING THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Kingdom of Spain and the Federal Government of Austria (hereinafter referred to as "the Parties"),

Aiming to guarantee the security of all Classified Information designated as such in accordance with each Party's domestic legislation and transmitted to the other Party,

Aiming to propose rules for the mutual protection of Classified Information exchanged or produced within the framework of cooperation between the Parties,

Have agreed as follows:

Article 1. Definitions

For the purposes of this Agreement:

(1) "Classified Information" means any information or material, regardless of its form, which is designated and marked as such in accordance with each Party's domestic legislation to ensure its protection against unauthorized disclosure, misappropriation or loss;

(2) "Competent Security Authority" means the authorities or agencies notified in accordance with article 13;

(3) "Personal Security Clearance" means the authorization issued by a Competent Security Authority confirming that an individual fulfills the necessary requirements enabling him or her to have access to Classified Information;

(4) "Facility Security Clearance" means the authorization issued by the Competent Security Authority confirming that a facility or institution has the ability to handle Classified Information;

(5) "Originating Party" means the Party, as well as any other public or private legal entity under its jurisdiction, which provided Classified Information;

(6) "Receiving Party" means the Party, as well as any other public or private legal entity under its jurisdiction, to which Classified Information is transmitted;

(7) "Classified Contract" means any contract or subcontract between any authority, agency or company of the State of a (Contracting) Party and any authority, agency or company of the other (Contractor) Party, the implementation of which requires access to Classified Information or the production of such Information;

(8) "Third party" means any State or international organization that is not a party to this Agreement.

Article 2. Equivalence of Security Classification Levels

The Parties agree on the following equivalence of security classification levels:

Kingdom of Spain	Republic of Austria	Translation
SECRETO	STRENG GEHEIM	Top secret
RESERVADO	GEHEIM	Secret
CONFIDENCIAL	VERTRAULICH	Confidential
DIFUSION LIMITADA	EINGESCHRÄNKT	Protected

Article 3. Marking

(1) Classified Information that is to be transmitted shall be marked by the originating Party in accordance with the appropriate security classification level, in the languages of both Parties.

(2) Classified Information generated or reproduced within the framework of cooperation under this Agreement shall also be marked.

(3) The security classification level can only be changed or revoked by the originating Party. The receiving Party must be notified at once of any change or revocation thereto.

Article 4. Principles of Protection of Classified Information

(1) The Parties shall take all appropriate measures, in accordance with this Agreement and their respective domestic legislation, to guarantee the protection of the transmitted Classified Information and shall provide for the necessary oversight of this protection.

(2) The Parties shall afford the transmitted Classified Information at least the same degree of protection as that which is afforded to their own Classified Information at the equivalent security classification level.

(3) The transmitted Classified Information shall be used only for the purpose for which it was provided and shall only be made available to persons who have been authorized to access it in accordance with domestic legislation at the equivalent security classification level on a need-to-know basis in order to fulfil their obligations. Access to such information by persons who are not nationals of either of the Parties shall only be permitted with the prior written consent of the originating Party.

(4) The receiving Party shall not provide access to Classified Information to a third party nor to any agency, company or individual without the written consent of the Competent Security Authority of the originating Party.

(5) Classified Information produced within the framework of cooperation under this Agreement shall enjoy the same protection as transmitted Classified Information.

Article 5. Personal Security Clearance

(1) Access to Classified Information ranked as "CONFIDENCIAL / VERTRAULICH" in terms of its security classification level or higher shall only be granted on the basis of a Personal Security Clearance in accordance with each Party's applicable domestic legislation.

(2) Upon request, the Competent Security Authorities shall, in accordance with their respective domestic legislation, provide mutual assistance to one another when, pursuant to this Agreement, investigations are conducted in connection with persons who reside or resided in the other State.

(3) Within the framework of this Agreement, each Party shall recognize the Personal Security Clearances issued by the other Party.

(4) Within the framework of this Agreement, the Competent Security Authorities shall inform one another at once about any changes concerning the Personal Security Clearances, particularly concerning any revocation or change of the security classification level.

Article 6. Classified Contracts

(1) A Classified Contract shall contain provisions relating to the security requirements and the security classification level of each of its aspects and elements.

(2) In the context of Classified Contracts, the Parties shall recognize the Facility Security Clearances issued by the other Party.

(3) In the context of the preparation or implementation of the Classified Contracts, the Competent Security Authority shall inform one another, upon request, as to whether a valid Facility Security Clearance has been issued or whether the relevant proceedings have been initiated.

(4) The Competent Security Authorities shall inform one another at once about any changes regarding the Facility Security Clearances referred to in this article, particularly regarding any change or revocation of the security classification level.

(5) The Contractor must provide the Supplier and the latter's Competent Security Authority with the security requirements needed for the Classified Contract, including a list of the Classified Information to be transmitted.

Article 7. Transmission

(1) Classified Information shall be transmitted through the diplomatic channel, unless the Competent Security Authorities decide otherwise, in accordance with the Parties' domestic legislation. If the transmissions are carried out manually by individuals, the latter must be issued a courier certificate.

(2) The Parties may transmit Classified Information by electronic means in accordance with security procedures agreed upon by the Competent Security Authorities.

(3) The shipment of bulky objects or large quantities of Classified Information shall be agreed upon by both Competent Security Authorities and shall be regulated by them on a case-by-case basis.

(4) The receiving Party must confirm receipt of the Classified Information in writing.

Article 8. Reproduction and Translation

(1) The reproduction of Classified Information shall be carried out in accordance with each Party's domestic legislation. The Competent Security Authority of the originating Party may restrict or exclude the reproduction of Classified Information by the receiving Party.

(2) Classified Information ranked as "SECRETO / STRENG GEHEIM" in terms of its security classification level may not be reproduced and may only be translated if the Competent Security Authority of the originating Party has granted its prior consent in writing to that end.

(3) Classified Information ranked as "CONFIDENCIAL / VERTRAULICH" in terms of its security classification level or higher may only be translated by persons holding the appropriate Personal Security Clearance.

(4) Copies and translations shall be safeguarded in the same way as originals.

Article 9. Destruction

(1) Classified Information must be destroyed in accordance with each Party's domestic legislation, in a verifiable manner that makes its full or partial reconstruction impossible.

(2) Classified Information ranked as "SECRETO / STRENG GEHEIM" in terms of its security classification level shall not be destroyed but shall instead be returned.

(3) Classified Information ranked as "RESERVADO / GEHEIM" in terms of its security classification level may only be destroyed with the written consent of the originating Party.

Article 10. Visits

(1) Visitors shall have access to Classified Information and to the facilities in which it is processed or stored only to the extent necessary and with the written authorization of the Competent Security Authority of the host Party. Permission shall be granted only to persons authorized to be given access to Classified Information at the corresponding classification level in accordance with domestic legislation.

(2) Requests for visits shall be submitted to the Competent Security Authority of the host Party at least 20 days prior to the visit. In urgent cases, they should be submitted, whenever possible, ten days prior to the visit. The Competent Security Authorities shall inform one another about the details of the visit and guarantee the protection of personal data.

(3) Requests for visits must be made in English and state the following, in particular:

(a) The purpose and expected date of the visit;

(b) The visitor's first and last names, date and place of birth, citizenship and passport or ID card number;

(c) The visitor's function and the name of the authority, agency or company represented;

(d) The validity and level of the visitor's Personal Security Clearance;

(e) The name, address, fax and phone numbers, e-mail address and contact points of the authorities, agencies or facilities to be visited;

(f) The date of the Competent Security Authority's request and signature.

(4) Once the visit has been approved, the Competent Security Authority of the Party hosting the visit shall provide a copy of the request for the visit to the security officers of the facilities to be visited.

(5) The maximum period of validity of the authorizations to visit shall not exceed 12 months.

(6) The Competent Security Authorities may agree to draw up a list of persons authorized to make periodic visits in connection with a specific Classified Contract. Once approved by the Competent Security Authorities, such a list shall remain valid for an initial period of 12 months. The conditions for the specific visits made on the basis of that list shall be agreed upon directly with the security officers of the facilities to be visited.

Article 11. Breaches of Security

(1) In cases where unauthorized disclosure, misuse or loss of Classified Information covered under this Agreement is suspected or confirmed, the Competent Security Authority of the receiving Party shall be notified thereof at once.

(2) Any breach of the provisions regarding the protection of Classified Information covered under this Agreement must be investigated and prosecuted in accordance with each Party's domestic legislation. The other Party shall provide assistance upon request.

(3) The Parties shall inform one another of the outcome of the investigations and of the measures adopted.

Article 12. Expenses

Each Party shall bear any expenses it may incur in the implementation of this Agreement.

Article 13. Competent Security Authorities

The Parties shall communicate to one another through the diplomatic channel the names of the Competent Security Authorities responsible for the implementation of this Agreement.

Article 14. Consultations

(1) The Competent Security Authorities shall inform one another of their respective domestic legislation and regulations concerning the protection of Classified Information and any changes thereto.

(2) In order to ensure close cooperation in the implementation of this Agreement, the Competent Security Authorities shall consult one another and facilitate the necessary mutual visits.

Article 15. Settlement of Disputes

Any dispute concerning the interpretation or application of this Agreement shall be settled through direct negotiations between the Parties or through the diplomatic channel.

Article 16. Final Provisions

(1) This Agreement is concluded for a period of indefinite duration and shall enter into force on the first day of the second month following the day on which the Parties have notified one another of the completion of the domestic legal procedures necessary for its entry into force.

(2) This Agreement may be amended by written mutual consent of the Parties. Amendments shall enter into force in accordance with paragraph 1.

(3) Each Party may terminate this Agreement through the diplomatic channel at any time. In such a case, the Agreement shall cease to have effect six months after the receipt of the termination notice by the other Party. In case of termination, Classified Information transmitted or produced pursuant to this Agreement shall continue to be protected in accordance with these provisions.

DONE at Madrid on 11 November 2011, in two originals, in Spanish and German, both texts being equally authentic.

For the Government of Spain:

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

For the Federal Government of Austria:

RUDOLF LENNKH
Ambassador of the Republic of Austria in Spain

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DU ROYAUME D'ESPAGNE ET LE GOUVERNEMENT FÉDÉRAL AUTRICHIEN RELATIF À L'ÉCHANGE ET À LA PROTECTION RÉCIPROQUE DES INFORMATIONS CLASSIFIÉES

Le Gouvernement du Royaume d'Espagne et le Gouvernement fédéral autrichien (ci-après dénommés « les Parties »),

Désirant garantir la sécurité des informations classifiées désignées comme telles conformément à la législation nationale de chacune des Parties,

Désirant proposer des règles pour la protection mutuelle des informations classifiées, échangées ou produites dans le cadre de la coopération entre les Parties,

Sont convenus de ce qui suit :

Article premier. Définitions

Aux fins du présent Accord :

1) L'expression « information classifiée » désigne toute information ou tout matériel, sous quelque forme que ce soit, qui est, conformément à la législation nationale de chacune des Parties, désigné et marqué comme tel pour assurer sa protection contre toute divulgation non autorisée, utilisation illicite ou perte;

2) L'expression « autorité de sécurité compétente » désigne les autorités ou organismes notifiés conformément à l'article 13;

3) L'expression « habilitation personnelle de sécurité » désigne l'habilitation délivrée par l'autorité de sécurité compétente indiquant qu'une personne physique remplit les conditions nécessaires pour avoir accès aux informations classifiées;

4) L'expression « habilitation de sécurité d'établissement » désigne l'habilitation délivrée par l'autorité de sécurité compétente indiquant qu'un établissement ou une institution possède la capacité nécessaire pour gérer les informations classifiées;

5) L'expression « Partie d'origine » désigne la Partie, ainsi que toute autre entité juridique publique ou privée relevant de sa compétence, qui fournit les informations classifiées;

6) L'expression « Partie destinataire » désigne la Partie, ainsi que toute autre entité juridique publique ou privée relevant de sa compétence, à laquelle les informations classifiées sont transmises;

7) L'expression « contrat classifié » désigne un contrat ou un contrat de sous-traitance conclu entre une autorité, un organisme ou une entreprise de l'État d'une Partie (contractant) et une autorité, un organisme ou une entreprise de l'État de l'autre Partie (fournisseur) dont l'exécution requiert l'accès à des informations classifiées ou la production de telles informations;

8) L'expression « tierce partie » désigne tout État ou organisation internationale qui n'est pas partie au présent Accord.

Article 2. Équivalence des niveaux de classification de sécurité

Les Parties conviennent de l'équivalence des niveaux de classification de sécurité ci-après:

Royaume d'Espagne	République d'Autriche	Traduction
SECRETO	STRENG GEHEIM	Très secret
RESERVADO	GEHEIM	Secret
CONFIDENCIAL	VERTRAULICH	Confidentiel
DIFUSION LIMITADA	EINGESCHRÄNKT	Restreint

Article 3. Marquage

1) Les informations classifiées qui sont transmises sont marquées par la Partie d'origine conformément au niveau de classification de sécurité pertinent, dans les langues des deux Parties.

2) Les informations classifiées qui sont produites ou reproduites dans le cadre de la coopération effectuée au titre du présent Accord sont également marquées.

3) Le niveau de classification de sécurité ne peut être modifié ou révoqué que par la Partie d'origine. La Partie destinataire est informée sans délai de toute modification ou révocation.

Article 4. Principes de protection des informations classifiées

1) Les Parties prennent toutes les mesures appropriées, conformément au présent Accord et à leur législation nationale, pour garantir la protection des informations classifiées transmises et veillent au contrôle de ladite protection.

2) Les Parties accordent aux informations classifiées transmises un degré de protection au moins identique à celui qu'elles accordent à leurs propres informations classifiées dont le niveau de classification de sécurité est équivalent.

3) Les informations classifiées transmises ne sont utilisées qu'aux fins pour lesquelles elles sont fournies et leur accès est limité aux personnes autorisées, conformément à la législation nationale, à avoir accès à des informations classifiées d'un niveau de classification de sécurité équivalent et qui en ont besoin pour s'acquitter de leurs obligations. L'accès à des informations classifiées par des personnes qui ne sont des ressortissants d'aucune des Parties n'est autorisé qu'avec le consentement écrit préalable de la Partie d'origine.

4) La Partie destinataire ne donne pas accès à des informations classifiées à une tierce partie ni à un organisme, une entreprise ou personne physique quelconque sans le consentement écrit de l'autorité de sécurité compétente de la Partie d'origine.

5) Les informations classifiées produites dans le cadre de la coopération menée au titre du présent Accord jouissent de la même protection que les informations classifiées qui sont transmises.

Article 5. Habilitation personnelle de sécurité

1) L'accès à des informations classifiées de niveau CONFIDENCIAL / VERTRAULICH ou supérieur n'est accordé que sur la base d'une habilitation personnelle de sécurité conforme à la législation nationale applicable de chacune des Parties.

2) Sur demande préalable, les autorités de sécurité compétentes se prêtent mutuellement assistance, conformément à leur législation nationale et en application du présent Accord, lorsque des enquêtes sont menées sur des personnes qui résident ou qui ont résidé dans l'autre État.

3) Dans le cadre du présent Accord, les Parties reconnaissent les habilitations personnelles de sécurité délivrées par l'autre Partie.

4) Dans le cadre du présent Accord, les autorités de sécurité compétentes s'informent mutuellement sans délai de toute modification relative aux habilitations personnelles de sécurité, en particulier pour ce qui est de la révocation ou de la modification du niveau de classification de sécurité.

Article 6. Contrats classifiés

1) Tout contrat classifié doit contenir des dispositions relatives aux exigences de sécurité et à la classification de chaque aspect et de chaque élément.

2) Dans le cadre des contrats classifiés, les Parties reconnaissent les habilitations de sécurité d'établissement délivrées par l'autre Partie.

3) Dans le cadre la préparation ou de la conclusion des contrats classifiés, les autorités de sécurité compétentes s'informent mutuellement, sur demande, si une habilitation de sécurité d'établissement en cours de validité a été délivrée ou si les procédures requises à cet effet ont été engagées.

4) Les autorités de sécurité compétentes s'informent mutuellement sans délai de toute modification des habilitations de sécurité d'établissement visées dans le présent article, en particulier s'agissant de toute modification ou révocation du niveau de classification de sécurité.

5) Le contractant doit communiquer au fournisseur et à l'autorité de sécurité compétente du fournisseur les exigences de sécurité relatives au contrat classifié, y compris une liste des informations classifiées transmises.

Article 7. Transmission

1) Les informations classifiées sont transmises par la voie diplomatique, à moins que les autorités de sécurité compétentes n'en décident autrement, en conformité avec les lois et règlements internes des Parties. Si les transmissions sont effectuées manuellement par des personnes physiques, celles-ci doivent être munies d'un certificat les accréditant comme messagers.

2) Les informations classifiées peuvent être transmises par voie électronique conformément aux procédures de sécurité approuvées d'un commun accord par les autorités de sécurité compétentes.

3) L'envoi d'objets volumineux ou de grandes quantités d'informations classifiées fait l'objet d'accords entre les deux autorités de sécurité compétentes et est réglé par elles au cas par cas.

4) La Partie destinataire doit confirmer par écrit la réception des informations classifiées.

Article 8. Reproduction et traduction

1) La reproduction des informations classifiées se fait conformément à la législation nationale des Parties. L'autorité de sécurité compétente de la Partie d'origine peut restreindre ou exclure la reproduction d'informations classifiées par la Partie destinataire.

2) Les informations classifiées du niveau de classification de sécurité SECRETO / STRENG GEHEIM ne peuvent être reproduites; elles ne sont traduites qu'avec le consentement écrit préalable de l'autorité de sécurité compétente de la Partie d'origine.

3) Les informations classifiées du niveau de classification de sécurité CONFIDENCIAL / VERTRAULICH ou d'un niveau de classification supérieur ne peuvent être traduites que par des personnes qui disposent de l'habilitation personnelle de sécurité appropriée.

4) Les copies et traductions doivent être protégées de la même manière que les originaux.

Article 9. Destruction

1) Les informations classifiées sont détruites conformément à la législation nationale des Parties, d'une manière vérifiable ne permettant pas leur reconstitution totale ou partielle.

2) Les informations classifiées du niveau de classification de sécurité SECRETO / STRENG GEHEIM ou d'un niveau de classification supérieur ne seront pas détruites mais restituées.

3) Les informations classifiées du niveau de classification de sécurité RÉSERVADO / GEHEIM ne seront détruites qu'avec le consentement écrit de la Partie d'origine.

Article 10. Visites

1) Les visiteurs n'ont accès aux informations classifiées et aux établissements où elles sont traitées ou conservées que dans la mesure nécessaire et avec l'autorisation écrite de l'autorité de sécurité compétente de la Partie qui reçoit les visiteurs. L'autorisation n'est accordée qu'aux personnes autorisées à avoir accès aux informations classifiées du niveau de classification correspondant, conformément à la législation nationale de chaque Partie.

2) Les demandes de visite doivent être présentées à l'autorité de sécurité compétente de la Partie qui reçoit les visites au moins 20 jours à l'avance et, dans les cas urgents et dans la mesure du possible, 10 jours avant la visite. Les autorités de sécurité compétentes doivent s'informer mutuellement des détails de la visite et garantir la protection des données à caractère personnel.

3) Les demandes de visite doivent être formulées en langue anglaise et indiquer, en particulier :

a) L'objet et la date prévue de la visite;

b) Les nom et prénom, les lieu et date de naissance, la nationalité et le numéro de passeport ou de document d'identité du visiteur;

c) La fonction du visiteur ainsi que le nom de l'autorité, organisme ou entreprise qu'il représente;

d) La validité et le niveau de l'habilitation personnelle de sécurité du visiteur;

e) Les nom, adresse, numéro de télécopieur et de téléphone, adresse électronique et point de contact des autorités, organismes ou établissements qui souhaitent effectuer une visite;

f) La date de la demande et la signature de l'autorité de sécurité compétente.

4) Une fois la visite approuvée, l'autorité de sécurité compétente de la Partie destinataire de la visite doit fournir une copie de la demande de visite aux responsables de la sécurité des établissements que le visiteur désire visiter.

5) La période de validité maximale des autorisations de visite est de 12 mois.

6) Les autorités de sécurité compétentes peuvent convenir de dresser une liste des personnes autorisées à effectuer des visites périodiques dans le cadre d'un contrat classifié spécifique. Une fois approuvée par les autorités compétentes de sécurité, une telle liste demeure valide pour une période initiale de 12 mois. Les conditions des visites effectuées sur la base de ladite liste sont convenues directement avec les responsables de la sécurité des établissements concernés.

Article 11. Infractions à la sécurité

1) En cas de divulgation non autorisée, d'utilisation illicite ou de perte d'informations classifiées relevant du présent Accord, suspectée ou avérée, les autorités de sécurité compétentes de la Partie destinataire en sont immédiatement informées.

2) Toute infraction aux dispositions du présent Accord relatives à la protection des informations classifiées fait l'objet d'enquêtes et de poursuites conformément à la législation nationale des Parties. L'autre Partie coopère sur demande préalable.

3) Les Parties s'informent réciproquement des conclusions des enquêtes et des mesures qui sont prises à cet effet.

Article 12. Frais

Les Parties prennent en charge les frais éventuels qu'elles exposent dans le cadre de l'application du présent Accord.

Article 13. Autorités de sécurité compétentes

Les Parties se communiquent par la voie diplomatique l'identité des autorités de sécurité compétentes chargées de l'application du présent Accord.

Article 14. Consultations

1) Les autorités de sécurité compétentes s'informent mutuellement des dispositions de leurs législations nationales respectives concernant la protection des informations classifiées et de toute modification y relative.

2) Dans le but d'assurer une coopération étroite dans l'application du présent Accord, les autorités de sécurité compétentes se consultent et facilitent les visites mutuelles nécessaires.

Article 15. Règlement des différends

Tout différend entre les Parties à propos de l'interprétation ou de l'application du présent Accord est réglé par voie de négociations directes ou par la voie diplomatique.

Article 16. Dispositions finales

1) Le présent Accord est conclu pour une durée indéterminée; il entre en vigueur le premier jour du deuxième mois suivant la date à laquelle les Parties se seront notifié réciproquement l'accomplissement des formalités juridiques internes nécessaires à cette fin.

2) Le présent Accord peut être modifié par consentement mutuel écrit des Parties. Les modifications entrent en vigueur conformément aux dispositions du paragraphe 1.

3) Chacune des Parties peut dénoncer le présent Accord à tout moment par la voie diplomatique. Dans ce cas, le présent Accord expire six mois après la réception de la notification de dénonciation par l'autre Partie. En cas de dénonciation, les informations classifiées transmises ou produites en application du présent Accord continuent d'être protégées conformément aux présentes dispositions.

FAIT à Madrid, le 11 novembre 2011, en deux exemplaires originaux, en espagnol et en allemand, les deux textes faisant également foi.

Pour le Gouvernement d'Espagne :

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

Pour le Gouvernement de la République fédérale autrichienne :

RUDOLF LENNKH
Ambassadeur de la République d'Autriche en Espagne