

No. 55172*

**Romania
and
Germany**

**Agreement between the Government of Romania and the Government of the Federal Republic of Germany concerning mutual protection of classified information.
Bucharest, 14 December 2016**

Entry into force: *27 October 2017 by notification, in accordance with article 15*

Authentic texts: *German and Romanian*

Registration with the Secretariat of the United Nations: *Romania, 15 May 2018*

**No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

**Roumanie
et
Allemagne**

**Accord entre le Gouvernement de la Roumanie et le Gouvernement de la République fédérale d'Allemagne relatif à la protection mutuelle d'informations classifiées.
Bucarest, 14 décembre 2016**

Entrée en vigueur : *27 octobre 2017 par notification, conformément à l'article 15*

Textes authentiques : *allemand et roumain*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Roumanie,
15 mai 2018*

**Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.*

[GERMAN TEXT – TEXTE ALLEMAND]

**ABKOMMEN
ZWISCHEN
DER REGIERUNG VON RUMÄNIEN
UND
DER REGIERUNG DER BUNDESREPUBLIK DEUTSCHLAND
ÜBER
DEN GEGENSEITIGEN SCHUTZ VON VERSCHLUSSSACHEN**

Die Regierung von Rumänien
und
die Regierung der Bundesrepublik Deutschland
(im Folgenden als Vertragsparteien bezeichnet) –

zum Schutz der Verschlussachen, die auf direktem Wege oder über andere öffentliche Stellen oder juristische Personen des öffentlichen oder privaten Rechts, die mit von der jeweils anderen Vertragspartei übermittelten Verschlussachen befasst sind, ausgetauscht werden, und im Rahmen der Tätigkeiten, die in den Verantwortungsbereich der zuständigen Sicherheitsbehörden der Vertragsparteien fallen –

sind wie folgt übereingekommen:

Artikel 1
Anwendungsbereich

(1) Dieses Abkommen bildet die Grundlage jeder Tätigkeit, in deren Rahmen zwischen den Vertragsparteien in Übereinstimmung mit innerstaatlichen Vorschriften Verschlussachen über die zuständigen Sicherheitsbehörden oder über andere öffentliche Stellen oder juristische Personen des öffentlichen oder privaten Rechts ausgetauscht werden.

Dies betrifft folgende Fälle:

- a) die Zusammenarbeit zwischen den Vertragsparteien betreffend die Landesverteidigung und alle anderen Angelegenheiten, die mit der nationalen Sicherheit zusammenhängen;
- b) gemeinsame Projekte, Verträge oder andere Formen der bilateralen Zusammenarbeit zwischen öffentlichen Stellen oder juristischen Personen des öffentlichen oder privaten Rechts im Bereich der Landesverteidigung und in allen anderen Angelegenheiten, die mit der nationalen Sicherheit zusammenhängen;
- c) Veräußerung von Ausrüstung, Produkten und Fachkenntnissen.

(2) Dieses Abkommen berührt nicht die jeweiligen Verpflichtungen beider Vertragsparteien aus anderen internationalen Übereinkünften und darf nicht gegen die Interessen, die Sicherheit oder die territoriale Unversehrtheit anderer Staaten verwendet werden.

Artikel 2 **Begriffsbestimmungen**

Im Sinne dieses Abkommens

- a) bedeutet „Verschlussache“
alle Informationen, Dokumente oder Materialien, unabhängig von ihrer Erscheinungsform, denen in Übereinstimmung mit innerstaatlichen Vorschriften ein bestimmter Geheimhaltungsgrad zugewiesen wurde und die entsprechend zu schützen sind;
- b) bedeutet „Verschlussachenauftrag“
eine Vereinbarung zwischen Auftraggeber und Auftragnehmer, in der deren Rechte und Pflichten begründet und näher bestimmt werden und die Verschlussachen beinhaltet oder den Zugang zu Verschlussachen einbezieht;
- c) bedeutet „Auftraggeber“
eine öffentliche Stelle oder juristische Person des öffentlichen oder privaten Rechts, die einen Verschlussachenauftrag vergibt;
- d) bedeutet „Auftragnehmer“
eine juristische Person des öffentlichen oder privaten Rechts, die an einem Vergabeverfahren teilnimmt, das Zugang zu Verschlussachen erfordert, oder einen Verschlussachenauftrag erhält und abwickelt;
- e) bedeutet „Preisgabe von Verschlussachen“
eine Situation, in der aufgrund einer Verletzung der Sicherheit Verschlussachen ihre Vertraulichkeit, Unversehrtheit oder Verfügbarkeit eingebüßt haben;
- f) bedeutet „Nachweis der Verschlussachenermächtigung“
ein Dokument, das in Übereinstimmung mit den innerstaatlichen Vorschriften ausgestellt wird und bestätigt, dass seinem Inhaber unter Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ bei der Ausübung seiner Aufgaben Zugang zu Verschlussachen eines bestimmten Geheimhaltungsgrads gewährt werden darf;

- g) bedeutet „Sicherheitsbescheid“
ein Dokument, das in Übereinstimmung mit den innerstaatlichen Vorschriften ausgestellt wird und bestätigt, dass ein Auftragnehmer unter den Aspekten der Sicherheit die jeweiligen Mindestvoraussetzungen für den Umgang mit Verschlusssachen zum Zweck der Teilnahme am Vergabeverfahren erfüllt oder zur Ausübung von Tätigkeiten in Verbindung mit Verschlusssachenaufträgen ermächtigt ist;
- h) bedeutet „Kenntnis nur, wenn nötig“
den Grundsatz, durch dessen Anwendung Zugang zu Verschlusssachen individuell gewährt werden kann, und zwar nur solchen Personen, die bei der Ausübung ihrer Aufgaben mit Verschlusssachen arbeiten oder Zugang zu diesen erhalten müssen;
- i) bedeutet „Zuständige Sicherheitsbehörde“
eine auf innerstaatlicher Ebene ermächtigte Einrichtung, die unter Einhaltung der innerstaatlichen Vorschriften die einheitliche Durchführung der Schutzmaßnahmen für Verschlusssachen gewährleistet. Solche Behörden sind in Artikel 3 aufgeführt;
- j) bedeutet „Beauftragte Sicherheitsbehörde“
die Einrichtung, die unter Einhaltung der innerstaatlichen Vorschriften ermächtigt ist, innerhalb ihres Tätigkeits- und Zuständigkeitsbereichs ihre eigenen Strukturen und Maßnahmen betreffend die Abstimmung und Kontrolle der Tätigkeiten, die mit dem Schutz von Verschlusssachen in Verbindung stehen, ein- und durchzuführen.

Artikel 3 **Zuständige Sicherheitsbehörden**

(1) Zuständige Sicherheitsbehörden auf innerstaatlicher Ebene für die Durchführung und die Kontrolle der im Rahmen der Durchführung dieses Abkommens ergriffenen Maßnahmen sind:

In Rumänien	In der Bundesrepublik Deutschland
Regierung von Rumänien Amt des Nationalen Registers für geheimhaltungsbedürftige Informationen des Staates Str. Mures n. 4 sect. 1 RO – Bukarest	1. Nationale Sicherheitsbehörde (Hauptansprechpartner): Bundesministerium des Innern Alt-Moabit 140 D - 10557 Berlin 2. Beauftragte Sicherheitsbehörde für den Geheimschutz in der Wirtschaft: Bundesministerium für Wirtschaft und Energie D - 53107 Bonn 3. Beauftragte Sicherheitsbehörde für den Geheimschutz im militärischen Bereich: Bundesministerium der Verteidigung D - 53003 Bonn

(2) Die Vertragsparteien unterrichten einander schriftlich über Änderungen der Zuständigkeit oder der Anschrift der in Absatz 1 aufgeführten zuständigen Sicherheitsbehörden, soweit sie für die Zusammenarbeit im Rahmen dieses Abkommens von Bedeutung sind.

Artikel 4 Geheimhaltungsgrade

(1) Auf im Rahmen dieses Abkommens ausgetauschte Verschlusssachen sind folgende Geheimhaltungsgrade anzuwenden:

- a) für Rumänien: STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ, STRICT SECRET, SECRET, SECRET DE SERVICIU;
- b) für die Bundesrepublik Deutschland: STRENG GEHEIM, GEHEIM, VS-VERTRAULICH, VS-NUR FÜR DEN DIENSTGEBRAUCH.

(2) Die Geheimhaltungsgrade in Rumänien sind wie folgt definiert:

- a) STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ wird Informationen zugewiesen, deren unbefugte Bekanntgabe der nationalen Sicherheit äußerst schwerwiegenden Schaden zufügen kann;
 - b) STRICT SECRET wird Informationen zugewiesen, deren unbefugte Bekanntgabe der nationalen Sicherheit schwerwiegenden Schaden zufügen kann;
 - c) SECRET wird Informationen zugewiesen, deren unbefugte Bekanntgabe der nationalen Sicherheit Schaden zufügen kann;
 - d) SECRET DE SERVICIU wird Informationen zugewiesen, deren Bekanntgabe einer juristischen Person des öffentlichen oder privaten Rechts Schaden zufügen kann.
- (3) Die Geheimhaltungsgrade in der Bundesrepublik Deutschland sind wie folgt definiert:
- a) STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann;
 - b) GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann;
 - c) VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann;
 - d) VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.
- (4) Die Vertragsparteien haben festgelegt, dass sich folgende innerstaatliche Geheimhaltungsgrade entsprechen:

Rumänien	Bundesrepublik Deutschland
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	STRENG GEHEIM
STRICT SECRET	GEHEIM
SECRET	VS-VERTRAULICH
SECRET DE SERVICIU	VS-NUR FÜR DEN DIENSTGEBRAUCH

(5) Die empfangende Vertragspartei kennzeichnet die ausgetauschten, empfangenen oder erzeugten Verschlusssachen mit dem entsprechenden Geheimhaltungsgrad, den die herausgebende Vertragspartei der Verschlusssache zugewiesen hat, und sichert für sie den gleichen Schutz zu wie für die eigenen Verschlusssachen des entsprechenden Geheimhaltungsgrades.

Artikel 5 **Schutz von Verschlusssachen**

(1) In Übereinstimmung mit den innerstaatlichen Vorschriften ergreifen die Vertragsparteien geeignete Maßnahmen zum Schutz von Verschlusssachen, die zwischen öffentlichen Stellen oder juristischen Personen des öffentlichen oder privaten Rechts der jeweiligen Staaten übermittelt, empfangen oder erzeugt werden.

(2) Die empfangende Vertragspartei und andere öffentliche Stellen oder juristische Personen des öffentlichen oder privaten Rechts verwenden für empfangene Verschlusssachen weder einen niedrigeren Geheimhaltungsgrad, noch heben sie den Geheimhaltungsgrad dieser Verschlusssachen ohne die vorherige schriftliche Zustimmung der zuständigen Sicherheitsbehörde der herausgebenden Vertragspartei auf. Die zuständige Sicherheitsbehörde der herausgebenden Vertragspartei teilt der zuständigen Sicherheitsbehörde der empfangenden Vertragspartei jede Änderung des Geheimhaltungsgrades der ausgetauschten Verschlusssachen mit.

(3) Jegliche Vervielfältigung oder Veränderung der empfangenen Verschlusssachen ist nur mit der schriftlichen Zustimmung des Herausgebers zulässig. Alle Kopien von Verschlusssachen werden mit demselben Geheimhaltungsgrad gekennzeichnet wie das Original und ebenso geschützt wie die ursprünglichen Verschlusssachen. Es werden nur so viele Kopien angefertigt, wie für amtliche Zwecke notwendig sind.

(4) Verschlussachen dürfen nur mit der vorherigen schriftlichen Zustimmung oder auf Ersuchen der herausgebenden Vertragspartei vernichtet werden, und zwar in Übereinstimmung mit den innerstaatlichen Vorschriften der Vertragsparteien und auf eine solche Weise, dass eine vollständige oder teilweise Wiederherstellung der Verschlussachen nicht möglich ist. Die empfangende Vertragspartei hat die herausgebende Vertragspartei unverzüglich von der Vernichtung von Verschlussachen zu unterrichten. Erklärt sich die herausgebende Vertragspartei mit der Vernichtung bestimmter Verschlussachen nicht einverstanden, so werden ihr diese zurückgesandt.

(5) Verschlussachen des Geheimhaltungsgrads STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / STRENG GEHEIM werden nicht vernichtet, sondern der herausgebenden Vertragspartei zurückgesandt. Im Fall einer unmittelbar drohenden Gefahr sind diese Verschlussachen auch ohne vorherige Zustimmung zu vernichten. Die zuständige Sicherheitsbehörde der herausgebenden Vertragspartei ist von der Vernichtung und deren Umständen unverzüglich zu unterrichten.

(6) Zugang zu Orten und Einrichtungen, an denen mit Verschlussachen in Verbindung stehende Tätigkeiten ausgeübt oder Verschlussachen aufbewahrt werden, ist unter Berücksichtigung des Grundsatzes „Kenntnis nur, wenn nötig“ ausschließlich Personen zu gewähren, die über eine Verschlussachenermächtigung entsprechend der Einstufung der Verschlussachen verfügen.

(7) Zugang zu Verschlussachen wird unter Berücksichtigung des Grundsatzes „Kenntnis nur, wenn nötig“ ausschließlich Personen gewährt, die über eine gültige Verschlussachenermächtigung entsprechend der Einstufung der Verschlussachen verfügen, zu denen der Zugang erforderlich ist.

Artikel 6

Verschlussachenermächtigung

(1) Jede Vertragspartei gewährleistet, dass alle Personen, die aufgrund ihrer Aufgaben Zugang zu Verschlussachen benötigen, über eine gültige Verschlussachenermächtigung für den entsprechenden Geheimhaltungsgrad verfügen.

(2) Der Nachweis der Verschlusssachenermächtigung wird im Anschluss an eine Sicherheitsüberprüfung ausgestellt, die in Übereinstimmung mit den innerstaatlichen Vorschriften der Vertragsparteien durchgeführt wird und den Anforderungen für den Zugang zu innerstaatlichen Verschlusssachen des entsprechenden Geheimhaltungsgrades genügen muss.

(3) Die zuständigen Sicherheitsbehörden und gegebenenfalls die beauftragten Sicherheitsbehörden unterstützen einander auf Ersuchen und unter Beachtung der jeweiligen innerstaatlichen Vorschriften bei den Überprüfungsverfahren, die mit der Ausstellung des Nachweises der Verschlusssachenermächtigung beziehungsweise des Sicherheitsbescheids in Zusammenhang stehen. Zu diesem Zweck können die zuständigen Sicherheitsbehörden und gegebenenfalls die beauftragten Sicherheitsbehörden besondere Vereinbarungen treffen.

(4) Die Vertragsparteien erkennen die in Übereinstimmung mit den innerstaatlichen Vorschriften ausgestellten Nachweise der Verschlusssachenermächtigung und Sicherheitsbescheide gegenseitig an.

(5) Die zuständigen Sicherheitsbehörden unterrichten einander über alle Änderungen der Verschlusssachenermächtigungen und Sicherheitsbescheide, insbesondere im Falle ihrer Aufhebung.

Artikel 7

Weitergabe von Verschlusssachen

(1) Die Weitergabe von Verschlusssachen an Dritte kann nur mit der schriftlichen Zustimmung der zuständigen Sicherheitsbehörde der herausgebenden Vertragspartei, die zusätzliche Einschränkungen für die Weitergabe vorschreiben kann, erfolgen.

(2) Jede Vertragspartei stellt sicher, dass von der anderen Vertragspartei empfangene Verschlusssachen zu dem Zweck verwendet werden, zu dem sie übermittelt wurden.

Artikel 8

Besuche

- (1) Besuchern aus dem Hoheitsgebiet einer Vertragspartei wird im Hoheitsgebiet der anderen Vertragspartei Zugang zu Verschlussachen des Geheimhaltungsgrades SECRET / VS-VERTRAULICH und höher sowie zu Orten und Einrichtungen, in denen an diesen gearbeitet wird, nur mit vorheriger Erlaubnis der zuständigen Sicherheitsbehörde der zu besuchenden Vertragspartei gewährt. Besuche, die nur den Zugang zu Verschlussachen des Geheimhaltungsgrades SECRET DE SERVICIU / VS-NUR FÜR DEN DIENSTGEBRAUCH voraussetzen, können zwischen dem Sicherheitsbeauftragten des Besuchers und der zu besuchenden Einrichtung vereinbart werden.
- (2) Der Besuchsantrag sollte mindestens 20 Werktage vor dem geplanten Besuch eingegangen sein. In dringenden Fällen können die zuständigen Sicherheitsbehörden eine kürzere Frist vereinbaren.
- (3) Die zuständige Sicherheitsbehörde der Vertragspartei, die den Besuchsantrag erhält, unterrichtet die zuständige Sicherheitsbehörde der Antrag stellenden Vertragspartei rechtzeitig über die getroffene Entscheidung.
- (4) Nach Genehmigung des Besuchs sichert die zuständige Sicherheitsbehörde der Vertragspartei, in deren Hoheitsgebiet der Besuch stattfinden soll, die Übermittlung einer Kopie des Besuchsantrags an den Sicherheitsbeauftragten der zu besuchenden Stelle, Einrichtung oder Organisation zu.
- (5) Die Gültigkeitsdauer der Besuchsgenehmigung wird zwölf Monate nicht überschreiten.
- (6) Für jeden Verschlussachenauftrag können die Vertragsparteien Listen über Personen, die zu periodischen Besuchen ermächtigt sind, vereinbaren. Diese Listen sind nur für einen Zeitraum von zwölf Monaten gültig.
- (7) Nach der Genehmigung der Listen durch die Vertragsparteien werden nachträgliche, mit den Besuchen in Verbindung stehende Einzelheiten unmittelbar von Vertretern der beteiligten Organisationen in Übereinstimmung mit den vereinbarten Fristen und Bedingungen festgelegt.

(8) Der Besuchs Antrag ist in der Sprache des zu besuchenden Landes oder in englischer Sprache vorzulegen und wird folgende Angaben beinhalten:

- a) Namen und Vornamen, Geburtsdatum und -ort, sowie die Pass- oder Personalausweisnummer des Besuchers;
- b) Staatsangehörigkeit des Besuchers;
- c) Dienstbezeichnung des Besuchers und Bezeichnung der Behörde oder Stelle, die er vertritt;
- d) den Geheimhaltungsgrad der Ermächtigung des Besuchers zum Zugang zu Verschlusssachen;
- e) Besuchszweck sowie Datum oder Zeitraum, an dem oder in dem der Besuch vorgesehen ist;
- f) Anführung der zu besuchenden Stellen, Ansprechpersonen und Einrichtungen.

(9) Jede Vertragspartei gewährleistet den Schutz der personenbezogenen Daten der Besucher in Übereinstimmung mit den einschlägigen innerstaatlichen Vorschriften.

Artikel 9 Industrieller Geheimschutz

(1) Beabsichtigt eine Vertragspartei beziehungsweise beabsichtigen öffentliche oder private Stellen im Gebiet einer Vertragspartei, einen Verschlusssachenauftrag an eine öffentliche oder private Stelle auf dem Gebiet der anderen Vertragspartei zu vergeben, so übernimmt die Vertragspartei, in deren Gebiet der Verschlusssachenauftrag durchgeführt werden soll, die Verantwortung für den Schutz der mit dem Verschlusssachenauftrag in Verbindung stehenden Verschlusssachen in Übereinstimmung mit ihren Vorschriften und den Bestimmungen dieses Abkommens.

(2) Vor Vergabe eines Verschlusssachenauftrags holt der Auftraggeber über die für ihn zuständige Sicherheitsbehörde bei der für den Auftragnehmer zuständigen Sicherheitsbehörde den Nachweis eines Sicherheitsbescheids ein, der bestätigt, dass der betreffende Auftragnehmer sich in der Geheimschutzbetreuung der zuständigen Sicherheitsbehörde der Vertragspartei befindet und dass er die für die Auftragsdurchführung erforderlichen Geheimschutzvorkehrungen getroffen hat.

(3) Ein Sicherheitsbescheid ist auch dann erforderlich, wenn ein Auftragnehmer zur Abgabe eines Angebots aufgefordert worden ist und im Rahmen des Ausschreibungsverfahrens bereits vor Auftragserteilung Verschlusssachen übergeben werden müssen.

(4) Ersuchen um Übermittlung des Nachweises eines Sicherheitsbescheids für Auftragnehmer aus dem Gebiet der anderen Vertragspartei enthalten Angaben über das Vorhaben sowie die Art, den Umfang und den Geheimhaltungsgrad der dem Auftragnehmer voraussichtlich zu überlassenden oder bei ihm entstehenden Verschlusssachen.

(5) Der Nachweis des Sicherheitsbescheids muss die vollständige Bezeichnung des Auftragnehmers, seine Postanschrift und den Namen des Sicherheitsbevollmächtigten, dessen Telefon- und Faxverbindung, seine E-Mail-Adresse sowie den Geheimhaltungsgrad enthalten, bis zu dem der Auftragnehmer Geheimschutzmaßnahmen gemäß den innerstaatlichen Vorschriften getroffen hat.

(6) Die zuständigen Sicherheitsbehörden der Vertragsparteien teilen einander mit, wenn sich die den ausgestellten Sicherheitsbescheiden zugrunde liegenden Sachverhalte ändern, soweit der Schutz der unter diesem Abkommen ausgetauschten Verschlusssachen durch diese Änderung beeinträchtigt wird.

(7) Der Austausch dieser Mitteilungen zwischen den zuständigen Sicherheitsbehörden der Vertragsparteien erfolgt in der Landessprache der zu unterrichtenden Behörde oder in englischer Sprache.

(8) Der Nachweis des Sicherheitsbescheids und an die jeweils zuständigen Sicherheitsbehörden der Vertragsparteien gerichtete Ersuchen um Übermittlung des Nachweises des Sicherheitsbescheids sind schriftlich zu übermitteln.

(9) Die Vertragsparteien tragen dafür Sorge, dass jeder Verschlussachenauftrag eine vom Auftraggeber erstellte Geheimschutzklausel enthält, die zumindest folgende Angaben beinhaltet:

- a) Umfang und Geheimhaltungsgrad der Verschlussachen, die dem Auftragnehmer übermittelt werden oder bei diesem entstehen sollen,
- b) die vom Auftragnehmer zu treffenden Geheimschutzmaßnahmen,
- c) das Verfahren zur Benachrichtigung über eingetretene Änderungen der Geheimhaltungsgrade,
- d) Modalität der Verschlussachenbeförderung,
- e) die Verpflichtung, jede tatsächliche oder mögliche Preisgabe von Verschlussachen zur Kenntnis zu bringen.

(10) Ein Exemplar der Geheimschutzklausel ist der zuständigen Sicherheitsbehörde der Vertragspartei, in deren Hoheitsgebiet der Verschlussachenauftrag durchgeführt werden soll, zu übermitteln.

(11) Ein Unterauftragnehmer hat die gleichen Sicherheitsauflagen zu erfüllen wie der Auftragnehmer.

Artikel 10 **Übermittlung von Verschlussachen**

(1) Verschlussachen werden auf diplomatischem beziehungsweise militärischem Kurierweg oder auf einem anderen von den zuständigen Sicherheitsbehörden vereinbarten Weg befördert. Verschlussachen des Geheimhaltungsgrades STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / STRENG GEHEIM werden nur als diplomatisches Kuriergepäck übermittelt. Die zuständige Sicherheitsbehörde der empfangenden Vertragspartei bestätigt schriftlich den Empfang von Verschlussachen.

(2) Für die Beförderung von Verschlussachen in erheblichem Umfang werden Transport, Transportweg und Sicherheitsmaßnahmen in jedem Einzelfall von den zuständigen Sicherheitsbehörden vereinbart.

(3) Die zuständigen Sicherheitsbehörden können in Ausnahmefällen für ein genau bezeichnetes Vorhaben vereinbaren, dass Verschluss­sachen der Geheimhaltungsgrade SECRET / VS-VERTRAULICH und STRICT SECRET / GEHEIM auf anderen als den in Absatz 1 genannten Wegen befördert werden dürfen, und zwar nur dann, wenn die Benutzung der in Absatz 1 genannten Wege der nationalen Sicherheit Schaden zufügen oder die Durchführung eines Verschluss­sachenauftrags beeinträchtigen könnte. In derartigen Fällen müssen folgende Mindestvoraussetzungen erfüllt sein.

- a) Der Beförderer muss in Übereinstimmung mit den innerstaatlichen Vorschriften zum Zugang zu Verschluss­sachen des entsprechenden Geheimhaltungsgrads ermächtigt sein;
- b) bei der absendenden Stelle muss ein Verzeichnis der beförderten Verschluss­sachen verbleiben; ein Exemplar dieses Verzeichnisses ist dem Empfänger zur Weiterleitung an die zuständige Sicherheitsbehörde zu übergeben;
- c) die Verschluss­sachen müssen in Übereinstimmung mit den innerstaatlichen Vorschriften der absendenden Vertragspartei verpackt sein;
- d) die Übergabe der Verschluss­sachen muss gegen Empfangsbescheinigung erfolgen;
- e) der Beförderer muss einen Kurierausweis mit sich führen, der in Übereinstimmung mit den innerstaatlichen Vorschriften ausgestellt wurde.

(4) Verschluss­sachen der Geheimhaltungsgrade SECRET / VS-VERTRAULICH und STRICT SECRET / GEHEIM können nur in verschlüsselter Form über von den zuständigen Sicherheitsbehörden akkreditierte Informations- und Kommunikationssysteme übermittelt werden. Verschluss­sachen des Geheimhaltungsgrads SECRET DE SERVICIU / VS-NUR FÜR DEN DIENSTGEBRAUCH können in verschlüsselter Form über öffentliche Informations- und Kommunikationssysteme unter Benutzung von durch die zuständigen Sicherheitsbehörden zertifizierten Verschlüsselungsmitteln übertragen werden. Die Vertragsparteien erkennen die Zertifizierung ihrer Informations- und Kommunikationssysteme, in denen die erhaltenen Verschluss­sachen aufbewahrt und verarbeitet werden, gegenseitig an. Im Falle einer Vernetzung vereinbaren die Vertragsparteien die zum Austausch von Verschluss­sachen einzusetzenden Verschlüsselungsmittel in gegenseitigem Einvernehmen.

Artikel 11

Preisgabe von Verschlusssachen

(1) Die Vertragsparteien benachrichtigen einander umgehend in schriftlicher Form über jede tatsächliche oder vermutete Preisgabe von Verschlusssachen.

(2) Die Untersuchung jeder Preisgabe von Verschlusssachen ist unverzüglich in Übereinstimmung mit den innerstaatlichen Vorschriften der Vertragspartei, in deren Hoheitsgebiet sich die Preisgabe ereignete, durchzuführen. Falls erforderlich, arbeiten die zuständigen Sicherheitsbehörden bei dieser Untersuchung zusammen.

(3) Die zuständige Sicherheitsbehörde der Vertragspartei, in deren Hoheitsgebiet sich die Preisgabe ereignet hat, benachrichtigt die zuständige Sicherheitsbehörde der anderen Vertragspartei schriftlich über die Umstände der Preisgabe von Verschlusssachen, den Umfang des Schadens, die zur Begrenzung der Auswirkungen getroffenen Maßnahmen und die Ergebnisse der Untersuchung.

Artikel 12

Beilegung von Streitigkeiten

Streitigkeiten über die Auslegung oder Anwendung dieses Abkommens werden ausschließlich durch Verhandlungen zwischen den zuständigen Sicherheitsbehörden der Vertragsparteien beigelegt. Während dieser Verhandlungen setzen die Vertragsparteien die Erfüllung ihrer Verpflichtungen aus diesem Abkommen fort.

Artikel 13

Kosten

Jede Vertragspartei trägt etwaige im Zusammenhang mit der Durchführung dieses Abkommens entstehende Kosten in Übereinstimmung mit ihren Vorschriften. Von einer Vertragspartei verursachte Kosten dürfen der anderen Vertragspartei nicht auferlegt werden.

Artikel 14 **Konsultationen**

- (1) Die zuständigen Sicherheitsbehörden der Vertragsparteien unterrichten einander auf Ersuchen über die geltenden Bestimmungen zum Schutz von Verschlusssachen.
- (2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die zuständigen Sicherheitsbehörden einander auf Ersuchen.
- (3) Jede Vertragspartei erlaubt Besuche von Vertretern der zuständigen Sicherheitsbehörden oder beauftragten Sicherheitsbehörden der anderen Vertragspartei im eigenen Hoheitsgebiet zum Zwecke von Konsultationen über für den Schutz von Verschlusssachen geltende Sicherheitsorganisation und -verfahren. Die Einzelheiten der Besuche werden von den zuständigen Sicherheits- oder beauftragten Behörden im gegenseitigen Einvernehmen festgelegt.

Artikel 15 **Schlussbestimmungen**

- (1) Dieses Abkommen wird auf unbestimmte Zeit geschlossen.
- (2) Dieses Abkommen tritt an dem Tag in Kraft, an dem die Regierung von Rumänien der Regierung der Bundesrepublik Deutschland notifiziert, dass die innerstaatlichen Voraussetzungen für das Inkrafttreten erfüllt sind. Maßgebend ist der Tag des Eingangs der Notifikation.
- (3) Jede Vertragspartei kann dieses Abkommen unter Einhaltung einer Frist von sechs Monaten auf diplomatischem Wege schriftlich kündigen. Die Frist beginnt mit dem Zugang der Notifizierung. Im Fall der Kündigung sind die aufgrund dieses Abkommens übermittelten oder beim Auftragnehmer entstandenen Verschlusssachen weiterhin gemäß den Bestimmungen dieses Abkommens zu behandeln, solange die fortbestehende Einstufung dies rechtfertigt.
- (4) Dieses Abkommen kann einvernehmlich in Schriftform von den Vertragsparteien geändert werden. Solche Änderungen treten in Übereinstimmung mit Absatz 2 in Kraft.

1997 unterzeichnete Abkommen zwischen der Regierung von Rumänien und der Regierung der Bundesrepublik Deutschland über den gegenseitigen Schutz von Verschlusssachen außer Kraft. Ab diesem Zeitpunkt werden alle übermittelten Verschlusssachen nach den Bestimmungen dieses Abkommens geschützt.

(6) Die Registrierung dieses Abkommens beim Sekretariat der Vereinten Nationen nach Artikel 102 der Charta der Vereinten Nationen wird unverzüglich nach seinem Inkrafttreten von der Vertragspartei veranlasst, in deren Staatsgebiet das Abkommen geschlossen wird. Die andere Vertragspartei wird unter Angabe der VN-Registriernummer von der erfolgten Registrierung unterrichtet, sobald diese vom Sekretariat der Vereinten Nationen bestätigt worden ist.

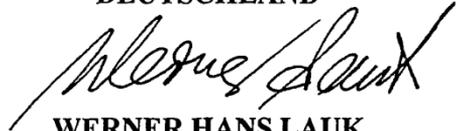
Geschehen zu Bukarest am 14. Dezember 2016 in zwei Urschriften, jede in rumänischer und deutscher Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist.

**FÜR DIE REGIERUNG
VON RUMÄNIEN**



Prof. Dr. MARIUS PETRESCU
Staatssekretär
Leiter des Amtes des Nationalen
Registers für
geheimhaltungsbedürftige
Informationen des Staates – ORNISS

**FÜR DIE REGIERUNG
DER BUNDESREPUBLIK
DEUTSCHLAND**



WERNER HANS LAUK
Außerordentlicher und
Bevollmächtigter Botschafter
der Bundesrepublik Deutschland in
Rumänien

[ROMANIAN TEXT – TEXTE ROUMAIN]

ACORD
ÎNTRE
GUVERNUL ROMÂNIEI
ȘI
GUVERNUL REPUBLICII FEDERALE GERMANIA
PRIVIND PROTECȚIA RECIPROCĂ
A INFORMAȚIILOR CLASIFICATE

Guvernul României și Guvernul Republicii Federale Germania, denumite în continuare Părți Contractante, în scopul asigurării protecției informațiilor clasificate, schimbate direct sau prin intermediul altor instituții publice ori persoane juridice de drept public sau privat care gestionează Informații Clasificate transmise de cealaltă Parte Contractantă, și în cadrul activităților care cad sub incidența responsabilității Autorităților Competente de Securitate ale Părților Contractante au convenit următoarele:

ARTICOLUL 1 DOMENIUL DE APLICARE

(1) Prezentul Acord va sta la baza tuturor activităților în cadrul cărora sunt schimbate, în conformitate cu reglementările naționale, Informații Clasificate între Părțile Contractante, prin intermediul Autorităților Competente de Securitate sau prin intermediul altor instituții publice ori persoane juridice de drept public sau privat.

Aceasta are în vedere următoarele situații:

- a) cooperarea între Părțile Contractante în domeniul apărării naționale și orice alte aspecte legate de securitatea națională;
- b) proiectele comune, contractele sau alte forme de cooperare bilaterală între instituții publice ori persoane juridice de drept public sau privat în domeniul apărării naționale și orice alt aspect legat de securitatea națională;
- c) înstrăinarea de echipamente, produse și know-how.

(2) Prezentul Acord nu va afecta obligațiile celor două Părți Contractante ce derivă din alte acorduri internaționale și nu va fi folosit împotriva intereselor, securității și integrității teritoriale ale altor state.

ARTICOLUL 2 DEFINIȚII

În sensul prezentului Acord:

- a) **„Informație Clasificată”** înseamnă:

orice informație, document sau material, indiferent de forma sa fizică și căreia i s-a atribuit un anumit nivel de clasificare în conformitate cu reglementările naționale și care va fi protejată corespunzător;

b) **„Contract Clasificat”** înseamnă:

acordul între Contractanți și Contractorii prin care se stabilesc și se definesc drepturile și obligațiile acestora și care conține sau implică accesul la Informații Clasificate;

c) **„Contractor”** înseamnă:

instituția publică ori persoana juridică de drept public sau privat care atribuie un Contract Clasificat;

d) **„Contractant”** înseamnă:

persoana juridică de drept public sau privat care participă la o procedură de atribuire care implică accesul la Informații Clasificate sau căreia i s-a atribuit și care derulează un Contract Clasificat;

e) **„Compromiterea Informației Clasificate”** înseamnă:

situația când, din cauza unui incident de securitate, Informațiile Clasificate și-au pierdut confidențialitatea, integritatea sau disponibilitatea;

f) **„Certificatul de Securitate a Personalului”** înseamnă:

documentul emis conform reglementărilor naționale care atestă faptul că, în exercitarea atribuțiilor, titularul acestuia poate avea acces la Informații Clasificate de un anumit nivel de clasificare, cu respectarea principiului „Necesității de a Cunoaște”;

g) **„Certificatul de Securitate Industrială”** înseamnă:

documentul emis conform reglementărilor naționale care confirmă că, din punct de vedere al securității, un Contractant îndeplinește cerințele minime pentru gestionarea Informațiilor Clasificate, în scopul participării la o procedură de atribuire sau este abilitat să efectueze activități legate de derularea unui Contract Clasificat;

h) **„Necesitatea de a Cunoaște”** înseamnă:

principiul pentru aplicarea căruia accesul la Informații Clasificate se acordă individual și anume numai acelor persoane care, pentru îndeplinirea atribuțiilor, lucrează cu Informații Clasificate sau trebuie să aibă acces la asemenea informații;

i) **„Autoritatea Competentă de Securitate”** înseamnă:

instituția cu autoritate la nivel național care, în conformitate cu reglementările naționale, asigură implementarea unitară a măsurilor de protecție a informațiilor clasificate. Aceste autorități sunt menționate la art. 3;

j) „**Autoritate Desemnată de Securitate**” înseamnă: instituția care, în conformitate cu reglementările naționale, este abilitată să stabilească și să implementeze, pentru domeniul său de activitate și responsabilitate, structuri și măsuri proprii privind coordonarea și controlul activității referitoare la protecția Informațiilor Clasificate.

ARTICOLUL 3 AUTORITĂȚILE COMPETENTE DE SECURITATE

(1) Autoritățile Competente de Securitate responsabile, la nivel național, de implementarea și controlul măsurilor luate în aplicarea prevederilor prezentului Acord sunt:

În România	În Republica Federală Germania
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS) Str. Mureș nr. 4, Sector 1 RO-București	1. Autoritatea Națională de Securitate (principalul interlocutor): Ministerul Federal de Interne Alt-Moabit 101 D-10557 Berlin 2. Autoritatea de securitate desemnată pentru protecția secretului în economie: Ministerul Federal al Economiei și Energiei D-53107 Bonn 3. Autoritatea de securitate desemnată pentru protecția secretului în domeniul militar: Ministerul Federal al Apărării D-53003 Bonn

(2) Părțile Contractante se vor informa reciproc în scris asupra oricăror modificări ale competențelor sau ale adreselor Autorităților Competente de Securitate menționate la alin. (1), în măsura în care acestea sunt relevante pentru cooperarea în cadrul prezentului Acord.

ARTICOLUL 4 NIVELURILE DE CLASIFICARE

(1) Nivelurile de clasificare ce se aplică informațiilor schimbate în cadrul prezentului Acord sunt:

a) pentru România: **STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ, STRICT SECRET, SECRET ȘI SECRET DE SERVICIU;**

b) pentru Republica Federală Germania: **STRENG GEHEIM, GEHEIM, VS-VERTRAULICH și VS-FÜR DEN DIENSTGEBRAUCH.**

(2) Nivelurile de clasificare pentru România sunt definite după cum urmează:

a) **STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ** se atribuie informațiilor a căror divulgare neautorizată este de natură să producă daune de o gravitate excepțională securității naționale;

b) **STRICT SECRET** se atribuie informațiilor a căror divulgare neautorizată este de natură să producă daune grave securității naționale;

c) **SECRET** se atribuie informațiilor a căror divulgare neautorizată este de natură să producă daune securității naționale;

d) **SECRET DE SERVICIU** se atribuie informațiilor a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat.

(3) Nivelurile de clasificare pentru Republica Federală Germania sunt definite după cum urmează:

a) **STRENG GEHEIM**, în situația în care cunoașterea de către persoane neautorizate poate pune în pericol existența sau interese vitale ale Republicii Federale Germania sau ale unuia dintre landurile sale;

b) **GEHEIM**, în situația în care cunoașterea de către persoane neautorizate poate pune în pericol securitatea Republicii Federale Germania sau a unuia dintre landurile sale sau dacă poate provoca daune grave intereselor lor;

c) **VS-VERTRAULICH**, în situația în care cunoașterea de către persoane neautorizate poate dăuna intereselor Republicii Federale Germania sau intereselor unuia dintre landurile sale;

d) **VS-FÜR DEN DIENSTGEBRAUCH**, în situația în care cunoașterea de către persoane neautorizate poate fi în dezavantajul Republicii Federale Germania sau al unuia dintre landurile sale.

(4) Părțile Contractante au stabilit că echivalența nivelurilor de clasificare naționale este următoarea:

România	Republica Federală Germania
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	STRENG GEHEIM
STRICT SECRET	GEHEIM
SECRET	VS-VERTRAULICH
SECRET DE SERVICIU	VS-FÜR DEN DIENSTGEBRAUCH

(5) Partea Contractantă primitoare va marca Informațiile Clasificate schimbate, primite sau produse cu nivel de clasificare echivalent cu cel atribuit Informațiilor Clasificate de Partea Contractantă emitentă și le va acorda același grad de protecție prevăzut pentru propriile Informații Clasificate cu nivel echivalent de clasificare.

ARTICOLUL 5 PROTECȚIA INFORMAȚIILOR CLASIFICATE

(1) În conformitate cu reglementările naționale, Părțile Contractante vor lua măsuri adecvate pentru protecția Informațiilor Clasificate care sunt transmise, primite sau produse între instituții publice ori persoane juridice de drept public sau privat din statele lor.

(2) Partea Contractantă primitoare și alte instituții publice ori persoanele juridice de drept public sau privat nu vor utiliza un nivel mai scăzut de clasificare pentru Informațiile Clasificate primite și nici nu vor declassifica aceste informații, fără acordul prealabil scris al Autorității Competente de Securitate a Părții Contractante emitente. Autoritatea Competentă de Securitate a Părții Contractante emitente va informa Autoritatea Competentă de Securitate a Părții Contractante primitoare asupra oricăror modificări ale nivelului de clasificare a Informațiilor Clasificate schimbate.

(3) Multiplicarea sau modificarea, în orice mod, a Informațiilor Clasificate primite se va face numai cu acordul scris al emitentului. Toate copiile de pe Informațiile Clasificate vor fi marcate cu același nivel de clasificare ca și originalul și vor fi protejate în aceeași manieră ca și Informațiile Clasificate originale. Numărul de copii va fi limitat la cel necesar scopurilor oficiale.

(4) Informațiile Clasificate vor fi distruse numai cu acordul prealabil scris sau la solicitarea Părții Contractante emitente, în conformitate cu reglementările naționale ale Părților Contractante, astfel încât reconstituirea, integrală sau parțială, a acestora să fie imposibilă. Partea Contractantă primitoare va notifica de îndată Părții Contractante emitente distrugerea Informațiilor Clasificate. În cazul în care Partea Contractantă emitentă nu își dă acordul cu privire la distrugerea unor Informații Clasificate, acestea îi vor fi returnate.

(5) Informațiile cu nivel de clasificare **STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / STRENG GEHEIM** nu vor fi distruse ci vor fi returnate Părții Contractante emitente. În cazul unui pericol iminent, aceste informații trebuie distruse și fără o autorizare prealabilă. Autoritatea Competentă de Securitate a Părții Contractante emitente va fi imediat notificată despre distrugere și împrejurările acesteia.

(6) Accesul în zonele și în obiectivele în care se desfășoară activități ce implică folosirea Informațiilor Clasificate sau unde se stochează astfel de informații va fi permis exclusiv persoanelor care dețin Certificat de Securitate a Personalului corespunzător clasificării acelor Informații Clasificate, cu respectarea principiului „Necesității de a Cunoaște”.

(7) Accesul la Informații Clasificate este permis, cu respectarea principiului „Necesității de a Cunoaște”, exclusiv persoanelor care dețin Certificat de Securitate a Personalului valabil pentru clasificarea informațiilor la care este necesar accesul.

ARTICOLUL 6 CERTIFICATUL DE SECURITATE A PERSONALULUI

(1) Fiecare Parte Contractantă va garanta că orice persoană care, în exercitarea atribuțiilor, necesită acces la Informații Clasificate deține un Certificat de Securitate a Personalului valabil și de nivel corespunzător.

(2) Certificatul de Securitate a Personalului va fi eliberat în urma verificării de securitate efectuate în conformitate cu reglementările naționale ale Părților Contractante, corespunzător nivelului de exigență cerut pentru accesul la Informații Clasificate naționale cu nivel de clasificare echivalent.

(3) La cerere, Autoritățile Competente de Securitate sau, după caz, Autoritățile Desemnate de Securitate, cu respectarea reglementărilor naționale, își vor acorda asistență reciprocă la procedurile de verificare privind eliberarea Certificatului de Securitate a Personalului și a Certificatului de Securitate Industrială. În acest sens, se pot încheia înțelegeri specifice între Autoritățile Competente de Securitate sau, după caz, Autoritățile Desemnate de Securitate.

(4) Părțile Contractante își recunosc reciproc Certificatele de Securitate a Personalului și Certificatele de Securitate Industrială, eliberate în conformitate cu reglementările naționale.

(5) Autoritățile Competente de Securitate se vor informa reciproc asupra oricăror modificări ale Certificatelor de Securitate a Personalului și Certificatelor de Securitate Industrială, în special asupra cazurilor de retragere a acestora.

ARTICOLUL 7 DISEMINAREA INFORMAȚIILOR CLASIFICATE

(1) Diseminarea Informațiilor Clasificate către terți poate avea loc numai cu acordul scris al Autorității Competente de Securitate a Părții Contractante emitente, care poate impune noi limitări asupra diseminării.

(2) Fiecare Parte Contractantă va asigura utilizarea Informațiilor Clasificate primite de la cealaltă Parte Contractantă doar în scopul pentru care au fost transmise.

ARTICOLUL 8 VIZITELE

(1) Vizitatorilor din teritoriul național al unei Părți Contractante li se acordă, pe teritoriul național al celeilalte Părți Contractante, acces la Informații Clasificate de nivel SECRET / VS-VERTRAULICH și superior și în zone și obiective în care se lucrează cu acestea, numai cu aprobarea anterioară a Autorității Competente de Securitate a Părții Contractante ce urmează a fi vizitată. Vizitele care presupun accesul numai la informații clasificate SECRET DE SERVICIU / VS-FÜR DEN DIENSTGEBRAUCH pot fi convenite direct între funcționarii de securitate ai vizitatorului și obiectivului vizitat.

(2) Cererea de vizită va trebui să fie primită cu cel puțin douăzeci de zile lucrătoare înainte de vizita planificată. În cazuri urgente, Autoritățile Competente de Securitate pot conveni un termen mai scurt.

(3) Autoritatea Competentă de Securitate a Părții Contractante care primește cererea de vizită va informa în timp util Autoritatea Competentă de Securitate a Părții Contractante solicitante despre decizia luată.

(4) După aprobarea vizitei, Autoritatea Competentă de Securitate a Părții Contractante pe al cărei teritoriu urmează a se efectua vizita va asigura transmiterea unei copii a cererii de vizită funcționarului de securitate al instituției, obiectivului sau organizației ce urmează a fi vizitată.

(5) Valabilitatea autorizației de vizită nu va depăși douăsprezece luni.

(6) Pentru fiecare Contract Clasificat, Părțile Contractante pot conveni liste cu persoanele autorizate să efectueze vizite periodice. Aceste liste sunt valabile pentru o perioadă de douăsprezece luni.

(7) După ce listele au fost aprobate de către Părțile Contractante, detaliile ulterioare privind vizitele se vor stabili direct între reprezentanții organizațiilor implicate, în conformitate cu termenii și condițiile convenite.

(8) Cererea de vizită va fi înaintată în limba țării ce urmează a fi vizitată sau în limba engleză și va conține următoarele date:

- a) numele și prenumele, data și locul nașterii, precum și numărul pașaportului sau al actului de identitate al vizitatorului;
- b) cetățenia vizitatorului;
- c) funcția vizitatorului și numele autorității sau entității pe care o reprezintă;
- d) nivelul autorizării de acces la Informații Clasificate deținute de vizitator;
- e) scopul vizitei și data sau perioada prevăzută pentru vizită;
- f) menționarea instituțiilor, persoanelor de contact și a obiectivelor ce urmează a fi vizitate.

(9) Fiecare Parte Contractantă va garanta protecția datelor cu caracter personal ale vizitatorilor în conformitate cu reglementările naționale în domeniu.

ARTICOLUL 9 SECURITATEA INDUSTRIALĂ

(1) În cazul în care o Parte Contractantă, respectiv entitățile publice sau private de pe teritoriul acesteia, intenționează să atribuie un Contract Clasificat unor entități publice sau private localizate pe teritoriul celeilalte Părți Contractante, atunci Partea Contractantă în statul căreia urmează a fi derulat Contractul Clasificat își va asuma responsabilitatea de a proteja Informațiile Clasificate referitoare la contract, în conformitate cu reglementările sale și cu prevederile prezentului Acord.

(2) Înainte de atribuirea unui Contract Clasificat, Contractorul solicită, prin Autoritatea Competentă de Securitate a acestuia, de la Autoritatea Competentă de Securitate a Contractantului, confirmarea existenței unui Certificat de Securitate Industrială, care să ateste că respectivul Contractant se află în coordonarea din punctul de vedere al protecției informațiilor clasificate a Autorității Competente de Securitate a Părții Contractante și că acesta a întreprins măsurile de protecție a Informațiilor Clasificate necesare pentru derularea contractului.

(3) Certificatul de Securitate Industrială este necesar și în situația în care Contractantul a fost invitat să prezinte o ofertă, iar în cadrul procedurii de licitație urmează să i se încredințeze Informații Clasificate încă înainte de atribuirea contractului.

(4) Cererile de transmitere a confirmării existenței Certificatului de Securitate Industrială pentru Contractanți din teritoriul celeilalte Părți Contractante vor conține date referitoare la proiect, precum și la natura, volumul și nivelul de clasificare a Informațiilor Clasificate ce urmează să fie transmise Contractantului sau să fie generate de acesta.

(5) Confirmarea existenței Certificatului de Securitate Industrială va conține denumirea completă a Contractantului, adresa poștală a acestuia, numele funcționarului de securitate, numerele de telefon și fax, adresa de e-mail, precum și nivelul de clasificare a informațiilor până la care Contractantul respectiv a întreprins măsuri de protecție în conformitate cu reglementările naționale.

(6) Autoritățile Competente de Securitate ale Părților Contractante se informează reciproc în legătură cu modificarea elementelor ce au stat la baza eliberării Certificatelor de Securitate Industrială, în măsura în care este afectată protecția Informațiilor Clasificate schimbate în cadrul prezentului Acord.

(7) Schimbul de informații între Autoritățile Competente de Securitate se efectuează în limba națională a autorității care este informată sau în limba engleză.

(8) Confirmarea existenței Certificatului de Securitate Industrială și cererile adresate Autorităților Competente de Securitate ale Părților Contractante privind transmiterea confirmării Certificatului de Securitate Industrială trebuie transmise în scris.

(9) Părțile Contractante vor lua măsuri ca fiecare Contract Clasificat să cuprindă o anexă de securitate elaborată de Contractor, care va conține cel puțin date referitoare la:

- a) volumul și nivelurile de clasificare ale Informațiilor Clasificate ce urmează să fie transmise Contractantului sau să fie generate de acesta;
- b) măsurile de protecție ce trebuie aplicate de Contractant;
- c) procedura de comunicare a modificărilor survenite în legătură cu nivelurile de clasificare;
- d) modalitatea de transport al Informațiilor Clasificate;
- e) obligația de a notifica orice compromitere reală sau posibilă a Informațiilor Clasificate.

(10) Un exemplar al anexei de securitate va fi transmis Autorității Competente de Securitate a Părții Contractante pe teritoriul căreia urmează să se deruleze Contractul Clasificat.

(11) Sub-contractantul trebuie să îndeplinească aceleași cerințe de securitate ca și Contractantul.

ARTICOLUL 10 TRANSMITEREA INFORMAȚIILOR CLASIFICATE

(1) Informațiile Clasificate se transmit prin curier diplomatic sau militar ori pe alte căi, convenite de Autoritățile Competente de Securitate. Informațiile Clasificate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / STRENG GEHEIM se transmit numai prin curier diplomatic. Autoritatea Competentă de Securitate a Părții Contractante primitoare va confirma în scris primirea Informațiilor Clasificate.

(2) Dacă există un volum mare de Informații Clasificate ce trebuie transmise, Autoritățile Competente de Securitate vor conveni modalitățile de transport, ruta și măsurile de securitate pentru fiecare caz în parte.

(3) Autoritățile Competente de Securitate pot conveni, în situații excepționale, pentru un proiect precizat cu exactitate, ca Informațiile Clasificate cu nivel de clasificare SECRET / VS-VERTRAULICH și STRICT SECRET/ GEHEIM să poată fi transportate prin alte căi decât cele prevăzute la alin. (1) și numai atunci când utilizarea căilor prevăzute la alin. (1) ar aduce prejudicii securității naționale sau ar afecta derularea unui Contract Clasificat. În astfel de cazuri se vor îndeplini următoarele cerințe minime:

- a) transportatorul trebuie să fie autorizat conform reglementărilor naționale pentru acces la Informații Clasificate cu nivel de clasificare corespunzător;
- b) la entitatea expeditoare trebuie să rămână o listă a Informațiilor Clasificate transportate; un exemplar al acestei liste va fi înmănat destinatarului în vederea transmiterii lui către Autoritatea Competentă de Securitate;
- c) Informațiile Clasificate trebuie să fie ambalate în conformitate cu reglementările naționale ale Părții Contractante trimițătoare;
- d) predarea Informațiilor Clasificate trebuie efectuată pe baza confirmării primirii;
- e) transportatorul trebuie să aibă asupra sa o dovadă de curier eliberată în conformitate cu reglementările naționale.

(4) Informațiile Clasificate de nivel SECRET / VS-VERTRAULICH și STRICT / SECRET GEHEIM pot fi transmise criptat numai prin intermediul unor sisteme informatice și de comunicații acreditate de Autoritățile Competente de Securitate. Informațiile Clasificate de nivel SECRET DE SERVICIU / VS-FÜR DEN DIENSTGEBRAUCH pot fi transmise criptat prin intermediul sistemelor informatice și de comunicații publice, cu utilizarea unor mijloace de criptare certificate de Autoritățile Competente de Securitate. Părțile Contractante vor recunoaște reciproc certificarea sistemelor informatice și de comunicații proprii folosite pentru stocarea și procesarea Informațiilor Clasificate primite. În cazul interconectării, Părțile Contractante vor conveni de comun acord asupra mijloacelor de criptare folosite pentru schimbul de Informații Clasificate.

ARTICOLUL 11 COMPROMITEREA INFORMATIILOR CLASIFICATE

(1) Părțile Contractante se vor informa în scris, cu promptitudine, cu privire la producerea oricărei compromiteri reale sau presupuse a Informațiilor Clasificate.

(2) Investigația oricărei Compromiteri a Informațiilor Clasificate se va efectua, fără întârziere, în conformitate cu reglementările naționale ale Părții Contractante pe teritoriul căreia s-a produs compromiterea. Dacă este necesar, Autoritățile Competente de Securitate vor coopera în această investigație.

(3) Autoritatea Competentă de Securitate a Părții Contractante pe teritoriul statului căreia a avut loc Compromiterea Informațiilor Clasificate va informa în scris Autoritatea Competentă de Securitate a celeilalte Părți Contractante, despre circumstanțele Compromiterii Informațiilor Clasificate, întinderea prejudiciului, măsurile adoptate pentru diminuarea proporțiilor prejudiciului și rezultatul investigației.

ARTICOLUL 12 SOLUȚIONAREA DIFERENDELOR

Diferențele privind interpretarea sau aplicarea prezentului Acord vor fi soluționate exclusiv prin negocieri între Autoritățile Competente de Securitate ale Părților Contractante. În timpul negocierilor, Părțile Contractante continuă îndeplinirea obligațiilor ce le revin din prezentul Acord.

ARTICOLUL 13 COSTURI

Fiecare Parte Contractantă va suporta eventualele costuri legate de aplicarea prezentului Acord în conformitate cu reglementările proprii. Costurile generate de o Parte Contractantă nu vor putea fi impuse celeilalte Părți Contractante.

ARTICOLUL 14 CONSULTĂRI

(1) Autoritățile Competente de Securitate ale Părților Contractante se informează reciproc la cerere în legătură cu prevederile în vigoare referitoare la protecția Informațiilor Clasificate.

(2) Pentru a asigura o cooperare strânsă în aplicarea prezentului Acord, Autoritățile Competente de Securitate se consultă reciproc, la cerere.

(3) Fiecare Parte Contractantă va permite celeilalte Părți Contractante efectuarea de vizite pe teritoriul propriu efectuate de reprezentanți ai Autorităților Competente de Securitate sau Autorităților Desemnate de Securitate pentru consultări în legătură cu organizarea și procedurile de securitate în vigoare pentru protecția Informațiilor Clasificate permise. Detaliile vizitelor sunt stabilite de comun acord de către Autoritățile Competente de Securitate sau între Autoritățile Desemnate de Securitate.

ARTICOLUL 15 DISPOZITII FINALE

(1) Prezentul Acord este încheiat pe perioadă nedeterminată.

(2) Prezentul Acord intră în vigoare în ziua în care Guvernul României notifică Guvernului Republicii Federale Germania îndeplinirea procedurilor interne pentru intrarea în vigoare. Decisivă este ziua în care a fost primită notificarea.

(3) Fiecare Parte Contractantă poate denunța prezentul Acord în scris, pe cale diplomatică, cu respectarea unui termen de șase luni. Termenul începe să curgă în momentul primirii notificării. În cazul denunțării, Informațiile Clasificate transmise în baza prezentului Acord sau generate de către Contractant vor fi gestionate conform prevederilor prezentului Acord, atât timp cât clasificarea existentă justifică acest lucru.

(4) Prezentul Acord poate fi modificat de comun acord de către Părțile Contractante, în formă scrisă. Asemenea modificări intră în vigoare în conformitate cu alin. (2).

(5) Odată cu intrarea în vigoare a prezentului Acord, „Acordul între Guvernul României și Guvernul Republicii Federale Germania privind protecția reciprocă a informațiilor clasificate, semnat la 24 noiembrie 1997 la București” își încetează valabilitatea. Din acest moment, toate Informațiile Clasificate transmise vor fi protejate conform prevederilor prezentului Acord.

(6) Înregistrarea prezentului Acord la Secretariatul Națiunilor Unite, în conformitate cu articolul 102 al Cartei Națiunilor Unite, va fi efectuată fără întârziere după intrarea în vigoare, de către Partea Contractantă pe teritoriul căreia a fost încheiat Acordul. Cealaltă Parte Contractantă este informată în legătură cu efectuarea înregistrării, prin indicarea numărului de înregistrare ONU, de îndată ce aceasta a fost confirmată de către Secretariatul Națiunilor Unite.

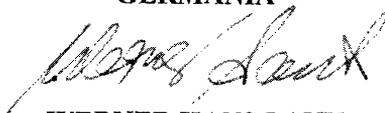
Semnat la București la 14 decembrie 2016, în două exemplare originale, fiecare în limbile română și germană, fiecare text fiind autentic în egală măsură.

**PENTRU
GUVERNUL ROMÂNIEI**



**Prof.univ.dr. MARIUS PETRESCU
Secretar de Stat
Directorul General
al Oficiului Registrului Național al
Informațiilor Secrete de Stat**

**PENTRU GUVERNUL
REPUBLICII FEDERALE
GERMANIA**



**WERNER HANS LAUK
Ambasadorul Extraordinar și
Plenipotențiar al Republicii Federale
Germania în România**

[TRANSLATION – TRADUCTION]¹

**AGREEMENT
BETWEEN
THE GOVERNMENT OF ROMANIA
AND
THE GOVERNMENT OF FEDERAL REPUBLIC OF GERMANY
CONCERNING MUTUAL PROTECTION
OF CLASSIFIED INFORMATION**

¹ Translation provided by the Government of Romania – Traduction fournie par le Gouvernement de la Roumanie.

The Government of Romania and the Government of Federal Republic of Germany, hereinafter referred to as Contracting Parties, in order to ensure the protection of Classified Information, exchanged directly or through other public institutions or public or private legal entities, managing the Classified Information sent by the other Contracting Party and within the activities that fall under the responsibility of the Competent Security Authorities of the Contracting Parties, agreed the following:

ARTICLE 1

SCOPE

- (1) This Agreement will stay at the basis of all the activities in which Classified Information is exchanged between the Contracting Parties, in accordance with the national regulations, through the Competent Security Authorities or through other public institutions or public or private legal entities.
- (2) It considers the following situations:
 - a) cooperation between the Contracting Parties in the field of national defence and any other aspects related to nationals security;
 - b) joint projects, contracts or other forms of bilateral cooperation between public institutions or public or private legal entities in the field of national defence and any other aspects related to nationals security.
 - c) alienation of equipment, products and know-how.
- (3) This Agreement will not affect the obligations of both Contracting Parties that derive from other international agreements and will not be used against the interests, security and territorial integrity of other states.

ARTICLE 2

DEFINITIONS

In the meaning of this Agreement:

- a) “**Classified Information**” means:

any information, document or material, irrespective of its physical form and to which a certain level of classification was assigned, in accordance with the national regulations and that will be protected accordingly;

b) **“Classified Contract”** means:

the agreement between Contractors and Beneficiaries, establishing and defining their rights and obligations and containing or implying the access to Classified Information

c) **“Beneficiary”** means:

the public institution or public or private legal entity that awards a Classified Contract;

d) **“Contractor”** means:

the public institution or public or private legal entity participating to an awarding procedure, implying the access to Classified Information or to whom a Classified Contract was awarded and develops a Classified Contract;

e) **“Compromising the Classified Information”** means:

the situation when, because of a security event, the Classified Information lost confidentiality, integrity or availability;

f) **“Staff Security Certificate”** means:

the document issued according to national regulations attesting the fact that, in exercising task, its owner may have access to Classified Information of a certain classification level, in compliance with the “need-to-know” principle;

g) **“Industrial Security Certificate”** means:

the document issued according to national regulations, confirming that, in terms of security, a Contractor fulfils the minimum requirements for managing Classified Information, in order to participate to an awarding procedure or is authorized to carry out activities related to the development of a Classified Contract;

h) **“Need to know”** means:

the principle for the application of which, the access to Classified Information is granted individually and namely, to those persons only who, for the fulfilment of their task, work with Classified Information or who must have access to such information;

i) **“Competent Security Authority”** means:

the institution with authority at national level that, in accordance with the national regulations, ensures the unitary implementation of Classified Information protection measures. These authorities are mentioned at the art. 3;

j) “Designated Security Authority” means:

the institution that, in accordance with the national regulations is authorized to establish and to implement, for its field of activity and responsibility, own structures and measures concerning the coordination and control of the activity relating to protection of Classified Information.

ARTICLE 3

COMPETENT SECURITY AUTHORITIES

(1) The Competent Security Authorities responsible at national level, for the implementation and control of the measures taken in the application of the provisions of this Agreement are:

In Romania	In Federal Republic of Germany
Government of Romania National Registry Office for Classified Information Str. Mures no. 4, 1 st District RO-Bucharest	1. National Security Authority (main interlocutor): Federal Ministry of Internal Affairs Alt-Moabit 101 D – 10557 Berlin 2. Security Authority Designated for The Protection of Secrecy In Economy: Federal Ministry of Economy and Energy D – 53107 Bonn 3 Security Authority designated for the protection of secrecy in military field : Federal Ministry of Defense D-53003 Bonn

(2) The Contracting Parties will inform each other in writing over any changes of the competences or of the addresses of the Competent Security Authorities mentioned at the paragraph (1), to the extent that they are relevant for the cooperation under this Agreement.

ARTICLE 4

CLASSIFICATION LEVELS

(1) The classification levels that are applicable to the information exchanged under this Agreement are:

- a) for Romania: STRICT SECRET DE IMPORTANTA DEOSEBITA (STRICT SECRET OF SPECIAL IMPORTANCE), STRICT SECRET (STRICT SECRET), SECRET (SECRET) AND SECRET DE SERVICIU (PROFESSIONAL SECRET);
- b) for Federal Republic of Germany: STRENG GEHEIM, GEHEIM, VS.VERTRAULICH qi VS.FUR DEN DIENSTGEBRAUCH

(2) The classification levels for Romania are defined as it follows:

- a) **STRICT SECRET DE IMPORTANTA DEOSEBITA (STRICT SECRET OF SPECIAL IMPORTANCE)** is assigned to information, of which unauthorized disclosure is likely to cause exceptional serious damages to national security;
- b) **STRICT SECRET (STRICT SECRET)** is assigned to information, of which unauthorized disclosure is likely to cause serious damages to national security;
- c) **SECRET (SECRET)** is assigned to information, of which unauthorized disclosure is likely to cause damages to national security;
- d) **SECRET DE SERVICIU (PROFESSIONAL SECRET)** is assigned to information, of which unauthorized disclosure is likely to cause prejudices to a public or private legal entity.

(3) The levels of classification for Federal Republic of Germany are defined as follows:

- a) **STRENG GEHEIM**, in case that the knowledge by other unauthorized person endangers the existence or vital interests of the Federal Republic of Germany or one of its lands;
- b) **GEHEIM**, in case that the knowledge by other unauthorized person endangers the security of the Federal Republic of Germany or of one of its lands or if it may cause serious damages to their interests;
- c) **VS-VERTRAULICH**, in case that the knowledge by other unauthorized person may harm the interests of the Federal Republic of Germany or the interests of one of its lands;
- a) **VS-FUR DEN DIENSTGEBRAUCH**, in case that the knowledge by other unauthorized person may be a disadvantage to the Federal Republic of Germany or to one of its lands.

(4) The Contracting Parties established that the equivalence of the national classification levels is the following :

Romania	Federal Republic of Germany
STRICT SECRET DE IMPORTANTA DEOSEBITA (STRICT SECRET OF SPECIAL IMPORTANCE)	STRENG GEHEIM
STRICT SECRET (STRICT SECRET),	GEHEIM
SECRET (SECRET)	VS-VERTRAULICH
	VS-FUR DEN DIENSTGEBRAUCH

- (5) The receiving Contracting Party will mark the Classified Information exchanged, received or produced with classification level equivalent to the one assigned to the Classified Information by the issuing Contracting Party and will assign them the same degree of protection provided for their own Classified Information with the same equivalent classification level.

ARTICLE 5 PROTECTION OF CLASSIFIED INFORMATION

- (1) In accordance with the national regulations, the Contracting Parties will take adequate measures for the protection of Classified Information that is sent, received or produced between public institutions or public or private legal entities from their states.
- (2) The receiving Contracting Party and other public institutions or public or private legal entities shall not use a lower level of classification for the received Classified Information and nor shall they declassify such information, without the prior consent in writing of the Competent Security Authority of the issuing Contracting Party. The Competent Security Authority of the issuing Contracting Party will inform the Competent Security Authority of the receiving Contracting Party over any modifications of the level of classification of the exchanged Classified Information.
- (3) The received Classified Information can be multiplied and amended only with the written consent of the issuer, all the copies of the Classified Information will be marked with the same level of classification like the original and they shall be protected in the same manner like the original Classified Information. The number of copies will be limited to the necessary number for official purposes.
- (4) The Classified Information will be destroyed only with the prior consent in writing or on demand of the issuing Contracting Party, in accordance with the national regulations of the Contracting Parties, so that its reconstitution, in full or in part, is impossible. The receiving Contracting Party will notify immediately the issuing Contracting Party about the destruction of the Classified Information. In case that the issuing Contracting Party does not give their consent concerning the destruction of some Classified Information, it will be returned.

- (5) The information with classification level of STRICT SECRET DE IMPORTANTA DEOSEBITA / STRENG GEFIEIM (STRICT SECRET OF SPECIAL IMPORTANCE) will not be destroyed but it will be returned to the issuing Contracting Party. In case of an imminent danger, such information must be destroyed also without a prior authorization, the Competent Security Authority of the issuing Contracting Party will be notified immediately about destruction and its circumstances.
- (6) The access in the areas and objectives where activities implying the use of Classified Information develop or where such information is stored, will be permitted exclusively for individuals that hold a Staff Security Certificate, corresponding to the classification of those pieces of Classified Information, in compliance with the “need-to-know” principle.
- (7) The access to Classified Information is permitted, by observing the “need-to-know” principle, exclusively to persons who already hold a Staff Security Certificate valid for classification of information to which access is necessary.

ARTICLE 6 STAFF SECURITY CERTIFICATE

- (1) Each Contracting Party will guarantee that every individual who requires access to Classified Information, in exercising his or her duties, holds a Staff Security Certificate valid and of appropriate level.
- (2) The Staff Security Certificate will be released after the security checking conducted in accordance with the national regulations of the Contracting Parties, corresponding to the level of exigency required for the access to national Classified Information with equivalent classification level.
- (3) On demand, the Competent Security Authorities or, as applicable, the Designated Security Authorities, in compliance with the national regulations, will grant mutual assistance to the checking procedures concerning the release of the Staff Security Certificate and of the Industrial Security Certificate, For that purpose, specific understandings may be concluded between the Competent Security Authorities or, as applicable, the Designated Security Authorities.
- (4) The Contracting Parties recognize to each other the Staff Security Certificates and the Industrial Security Certificates, issued in accordance with the national regulations.

- (5) The Competent Security Authorities will inform each other over all modifications of the Staff Security Certificates and of the Industrial Security Certificates, particularly as concerns the cases of their withdrawal.

**ARTICLE 7
DISSEMINATION OF CLASSIFIED INFORMATION**

- (1) The Classified Information to third parties may be disseminated to third parties only with the written consent of the Competent Security Authority of the issuing Contracting Party that may impose new restrictions over the dissemination.
- (2) Each Contracting Party will ensure the use of Classified Information received from the other Contracting Party for the purpose that it was transmitted only.

**ARTICLE 8
VISITS**

- (1) Visitors from the national territory of either Contracting Party are granted, on the national territory of the other Contracting Party, access to Classified Information at SECRET / VS-VERTRAULICH and upper level and in the areas and objectives in which it is used for work, only with the prior approval of the Competent Security Authority of the Contracting Party that follows to be visited. The visits that suppose the access only to SECRET DE SERVICIU / VS-FUR DEN DIENSTGEBRAUCH Classified Information may be agreed directly between the visitor's security officers and the visited objective.
- (2) The visit request shall be received at least twenty working days before the planned visit. In case of emergencies, the Competent Security Authorities may agree upon a shorter period.
- (3) The Competent Security Authority of the Contracting Party that received the visit request will inform timely the Competent Security Authority of the requesting Contracting Party about the decision taken.
- (4) After the visit approval, the Competent Security Authority of the Contracting Party on which territory the visit shall be made will ensure that a copy of the visit request will be sent to the security officer of the institution, objective or organization that shall be visited.

- (5) The validity of the visit permit shall not exceed twelve months.
- (6) For each classified contract, the Contracting Parties may agree upon lists with the persons authorized to make periodical visits. These lists are valid for a period of twelve months.
- (7) After the approval of the lists by the Contracting Parties, the subsequent details concerning visits will be established directly between the representatives of the involved organizations, in accordance with the agreed terms and conditions.
- (8) The visit request will be submitted in the language of the country that is to be visited or in English language and will contain the following data:
 - a) the surname and the given name, date and place of birth, as well as the number of passport or of the visitor's identity document;
 - b) visitor's citizenship;
 - c) position of the visitor and name of the authority or entity which he/she represents;
 - d) level of authorization of access to Classified Information held by the visitor;
 - e) purpose of the visit and date or period provided for the visit;
 - f) mentioning the institutions, contacts persons and objectives that shall be visited.
- (9) Each Contracting Party will guarantee the protection of personal data of visitors in accordance with the national regulations in the field.

ARTICLE 9 INDUSTRIAL SECURITY

- (1) In case a Contracting Party, respectively the public or private entities on its territory, intends to award a Classified Contract to a public or private entity located on the territory of the other Contracting Party, then the Contracting Party in the State in which the Classified Contract will be performed, will undertake the responsibility to protect the Classified Information related to the contract, in accordance with its regulations and with the provisions of this Agreement.

- (2) Before awarding a Classified Contract, the Beneficiary requests from the Contractor's Competent Security Authority, through its Competent Security Authority, the confirmation of the existence of an Industrial Security Certificate certifying that the relevant Contractor is under the coordination of the Contracting Party's Competent Security Authority from the point of view of the protection of Classified Information, and that it took the measures for protecting the Classified Information that is necessary for the performance of the contract.
- (3) The Industrial Security Certificate is also necessary if the Contractor was invited to submit a proposal, and, within the tender procedure, it will be entrusted with Classified Information even before the awarding of the contract.
- (4) The requests for the notification of the confirmation of the Industrial Security Certificate's existence for the Contractors on the territory of the other Contracting Party will comprise data on the project, as well as on the type, volume and classification level of the Classified Information to be notified to the Contractor or to be generated by it.
- (5) The confirmation of the Industrial Security Certificate's existence will comprise the full name of the Contractor, its mailing address, the name of the security officer, phone and fax numbers, e-mail address, as well as the classification level of the information up to which the relevant Contractor took protection measures in accordance with the national regulations.
- (6) The Competent Security Authorities of the Contracting Parties mutually notify the changes in the elements underlying the issuance of the Industrial Security Certificates, to the extent to which the protection of the Classified Information exchanged within this Agreement is affected.
- (7) The exchange of notifications between the Competent Security Authorities is carried out in the national language of the notified authority, or in English.
- (8) The confirmation of the Industrial Security Certificate's existence and the requests notified to the Competent Security Authorities of the Contracting Parties related to the notification of the Industrial Security Certificate confirmation must be submitted in writing.
- (9) The Contracting Parties will take measures that each Classified Contract comprises a security annex drafted by the Beneficiary, which will comprise at least information related to:

- a) the volume and classification levels of the Classified Information to be notified to the Contractor or to be generated by it;
 - b) the protection measures that must be implemented by the Contractor;
 - c) the procedure for the notification of the changes that occurred in the classification levels;
 - d) the means of transportation of the Classified Information;
 - e) the obligation to notify any actual or possible compromising related to the Classified Information.
- (10) A copy of the security annex will be notified to the Competent Security Authority of the Contracting Party on which territory the Classified Contract will be performed.
- (11) The Subcontractor must meet the same security requirements as the Contractor.

ARTICLE 10 TRANSMISSION OF THE CLASSIFIED INFORMATION

- (1) The Classified Information is transmitted by diplomatic or military courier or by other means agreed by the Competent Security Authorities. The STRICT SECRET OF SPECIAL IMPORTANCE/STRENG GEHEIM Classified Information is transmitted only by diplomatic courier. The Competent Security Authority of the receiving Contracting Party will confirm in writing the receipt of the Classified Information.
- (2) If a large volume of Classified Information must be transmitted, the Competent Security Authorities will agree on the means of transportation, route and security measures on a case-by-case basis.
- (3) The Competent Security Authorities may agree, in exceptional cases, for an accurately specified project, that the Classified Information at a SECRET/VS-VERTRAULICH and STRICT SECRET/GEHEIM classification level is transported by other means than those provided by paragraph (1), and only if using the means provided by paragraph (1) could damage the national security or affect the performance of a Classified Contract. In such cases, the following minimum requirements will be met:
- a) the carrier must be certified in accordance with the national regulations for access to Classified Information with an adequate classification level;
 - b) the sending entity must keep a list of the transported Classified Information; a copy of this list will be handed over to the recipient for notifying it to the Competent Security Authority;
 - c) the Classified Information must be packed in accordance with the national regulations of the sending Contracting Party;

- d) the Classified Information must be handed over on the basis of the acknowledgement of receipt;
- e) the carrier must have on it a carrier proof issued in accordance with the national regulations.

(4) The encrypted Classified Information at a SECRET/VS-VERTRAULICH and STRICT SECRET/GEHEIM classification level may be notified only through information and communication systems certified by the Competent Security Authorities. The encrypted Classified Information at a PROFESSIONAL SECRET /VS-FÜR DEN DIENSTGEBRAUCH classification level may be notified through public information and communication systems, by using encryption means certified by the Competent Security Authorities. The Contracting Parties will mutually recognize the certification of their own information and communication systems used for storing and processing the received Classified Information. In the case of interconnection, the Contracting Parties will mutually agree the encryption means used for the exchange of Classified Information.

ARTICLE 11 COMPROMISING OF THE CLASSIFIED INFORMATION

- (1) The Contracting Parties will promptly notify each other in writing concerning the occurrence of any actual or possible compromising of the Classified Information.
- (2) The investigation of any Compromising of the Classified Information will be carried out without delay in accordance with the national regulations of the Contracting Party on which territory the compromising occurred. If necessary, the Competent Security Authorities will cooperate in this investigation.
- (3) The Competent Security Authority of the Contracting Party on which territory the Compromising of the Classified Information occurred will notify in writing the Competent Security Authority of the other Contracting Party, about the circumstances of the Compromising of the Classified Information, the extend of the damage, the measures that were adopted for mitigating the extent of the damage and the outcome of the investigation.

**ARTICLE 12
DISPUTE SETTLEMENT**

The disputes related to the construction or implementation of this Agreement will be exclusively settled by negotiations between the Competent Security Authorities of the Contracting Parties. During the negotiations, the Contracting Parties will continue to fulfil their obligations under this Agreement.

**ARTICLE 13
COSTS**

Each Contracting Party will bear the costs that may arise in connection with the implementation of this Agreement in accordance with its own regulations. The costs generated by a Contracting Party may not be levied against the other Contracting Party.

**ARTICLE 14
CONSULTATIONS**

- (1) The Competent Security Authorities of the Contracting Parties will notify each other, on request, of the provisions in force related to the protection of Classified Information.
- (2) In order to ensure a close cooperation in the implementation of this Agreement, the Competent Security Authorities will consult each other, on request.
- (3) Each Contracting Party will allow the other Contracting Party visits on its own territory of the representatives of the Competent Security Authorities or of the Designated Security Authorities for consultations related to the organization and security procedures in force for the protection of the received Classified Information. The details of the visits are mutually established by the Competent Security Authorities or by the Designated Security Authorities.

**ARTICLE 15
FINAL PROVISIONS**

- (1) This Agreement is concluded for indefinite period of time.
- (2) This Agreement enters into force on the day when the Government of Romania notifies the Government of Federal Republic of Germany the fulfilment of the internal procedures for entry into force. It is decisive the day in which the notifications as received.
- (3) Each Contracting Party may denounce this Agreement in writing, by diplomatic ways, by observing a six-month period. The period starts to run as of the time of receiving the notification. In case of denunciation, the Classified Information transmitted based on this Agreement or generated by the Contractor will be managed according to the provisions of this Agreement, as long as the existing classification justifies it.
- (4) This Agreement may be amended by mutual consent by the Contracting Parties in writing. Such amendments enter into force in accordance with the paragraph (2).
- (5) Upon the entry into force of this Agreement "Agreement Between the Government of Romania and the Government of Federal Republic of Germany concerning Mutual Protection of Classified Information, signed on November 24, 1997 at Bucharest" ceases validity. Since that time, all pieces of Classified Information sent, will be protected according to the provisions of this Agreement.
- (6) The registration of this Agreement by the Secretariat of the United Nations, in accordance with the article 102 of the Charter of the United National, will be made immediately after entry into force, by the Contracting Party on the territory of which this Agreement was concluded. The other Contracting Party is informed about the registration made, by indicating the UNO registration number, as soon as it was acknowledged by the United Nations' Secretariat.

Signed at Bucharest, on December 14, 2016, in two original counterparts, each copy in Romanian and German language, each text being equally authentic.

FOR THE GOVERNMENT OF ROMANIA

(Illegible signature applied)

Marius Petrescu, Univ. prof. PhD.

State Secretary

**General Manager of the
National Registry Office for Classified
Information**

**FOR THE GOVERNMENT OF THE
FEDERAL REPUBLIC OF GERMANY**

(Illegible signature applied)

WERNER HANS LAUK

**Ambassador Extraordinary and
Plenipotentiary of the Federal Republic of
Germany**

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DE LA ROUMANIE ET LE
GOUVERNEMENT DE LA RÉPUBLIQUE FÉDÉRALE D'ALLEMAGNE
RELATIF À LA PROTECTION MUTUELLE D'INFORMATIONS CLASSIFIÉES

Le Gouvernement de la Roumanie et le Gouvernement de la République fédérale d'Allemagne, ci-après dénommés les « Parties contractantes »,

Désireux d'assurer la protection des informations classifiées, échangées directement ou par l'intermédiaire d'autres institutions publiques ou personnes morales publiques ou privées, gérant les informations classifiées envoyées par l'autre Partie contractante et dans le cadre des activités qui relèvent de la responsabilité des autorités compétentes en matière de sécurité des Parties contractantes,

Sont convenus de ce qui suit :

Article premier. Portée

1) Le présent Accord reste à la base de toutes les activités dans lesquelles des informations classifiées sont échangées entre les Parties contractantes conformément aux réglementations nationales par l'intermédiaire des autorités compétentes en matière de sécurité ou d'autres institutions publiques ou personnes morales publiques ou privées ;

2) Il considère les situations suivantes :

a) la coopération entre les Parties contractantes dans le domaine de la défense nationale et de tout autre aspect lié à la sécurité nationale ;

b) des projets communs, des contrats ou d'autres formes de coopération bilatérale entre institutions publiques ou personnes morales publiques ou privées dans le domaine de la défense nationale et de tout autre aspect lié à la sécurité nationale ;

c) l'aliénation d'équipements, de produits et de savoir-faire.

3) Le présent Accord n'affecte pas les obligations des deux Parties contractantes qui découlent d'autres accords internationaux et ne sera pas utilisé à des fins contraires aux intérêts, à la sécurité et à l'intégrité territoriale d'autres États.

Article 2. Définitions

Dans le cadre du présent Accord :

a) Le terme « information classifiée » désigne toute information, document ou matériel, quelle que soit sa forme physique, auquel un certain niveau de classification a été attribué, conformément à la réglementation nationale, et qui sera protégé en conséquence ;

b) Le terme « contrat classifié » désigne l'accord entre les contractants et les bénéficiaires, établissant et définissant leurs droits et obligations et contenant ou impliquant l'accès à des informations classifiées ;

c) Le terme « bénéficiaire » désigne l'institution publique ou la personne morale publique ou privée qui attribue un contrat classifié ;

d) Le terme « contractant » désigne l'institution publique ou la personne morale publique ou privée participant à une procédure d'attribution, impliquant l'accès à des informations classifiées ou à laquelle un contrat classifié a été attribué et qui développe un contrat classifié ;

e) Le terme « compromission des informations classifiées » désigne la situation dans laquelle, en raison d'un événement de sécurité, les informations classifiées ont perdu leur confidentialité, leur intégrité ou leur disponibilité ;

f) Le terme « certificat de sécurité du personnel » désigne le document délivré conformément à la réglementation nationale attestant que, dans l'exercice de ses fonctions, son titulaire peut avoir accès à des informations classifiées d'un certain niveau de classification, conformément au principe du « besoin d'en connaître » ;

g) Le terme « certificat de sécurité industrielle » désigne le document délivré conformément à la réglementation nationale, confirmant qu'en matière de sécurité, un contractant remplit les exigences minimales pour la gestion des informations classifiées afin de participer à une procédure d'attribution ou est autorisé à mener des activités liées à la rédaction d'un contrat classifié ;

h) Le terme « besoin d'en connaître » désigne le principe selon lequel l'accès aux informations classifiées est accordé individuellement et notamment aux seules personnes qui, pour l'accomplissement de leur tâche, travaillent avec des informations classifiées ou qui doivent y avoir accès ;

i) Le terme « autorité compétente en matière de sécurité » désigne l'institution ayant autorité au niveau national qui, conformément à la réglementation nationale, assure l'application unitaire des mesures de protection des informations classifiées. Ces autorités sont mentionnées à l'article 3 ;

j) Le terme « autorité désignée en matière de sécurité » désigne l'institution qui, conformément à la réglementation nationale, est autorisée à établir et à mettre en œuvre, pour son domaine d'activité et de responsabilité, des structures et des mesures propres concernant la coordination et le contrôle de l'activité relative à la protection des informations classifiées.

Article 3. Autorités compétentes en matière de sécurité

1) Les autorités compétentes en matière de sécurité responsables, au niveau national, de la mise en œuvre et du contrôle des mesures prises en application des dispositions du présent Accord sont :

En Roumanie	En République fédérale d'Allemagne
<p>Le Gouvernement de la Roumanie Le Bureau d'enregistrement des informations classifiées Str. Mures no. 4, 1st District, Bucarest, Roumanie</p>	<p>1. Autorité de sécurité nationale (principal interlocuteur) : Ministère fédéral de l'intérieur Alt-Moabit 140 D - 10557 Berlin</p> <p>2. Autorité désignée en matière de sécurité pour la protection du secret dans le domaine de l'économie : Ministère fédéral de l'économie et de l'énergie D - 53107 Bonn</p> <p>3. Autorité désignée en matière de sécurité pour la protection du secret dans le domaine militaire : Ministère fédéral de la défense D - 53003 Bonn</p>

2) Les Parties contractantes s'informent mutuellement par écrit de toute modification des compétences ou des adresses des autorités compétentes en matière de sécurité mentionnées au paragraphe 1, dans la mesure où elles sont pertinentes pour la coopération dans le cadre du présent Accord.

Article 4. Niveaux de classification

1) Les niveaux de classification applicables aux informations échangées dans le cadre du présent Accord sont les suivants :

a) pour la Roumanie : STRICT SECRET DE IMPORTANTA DEOSEBITA (STRICT SECRET D'IMPORTANCE SPÉCIALE), STRICT SECRET (STRICT SECRET), SECRET (SECRET) ET SECRET DE SERVICIU (SECRET PROFESSIONNEL) ;

b) pour la République fédérale d'Allemagne : STRENG GEHEIM, GEHEIM, VS-VERTRAULICH ET VS-NUR FÜR DEN DIENSTGEBRAUCH.

2) Les niveaux de classification pour la Roumanie sont définis comme suit :

a) STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ (STRICT SECRET D'IMPORTANTANCE SPÉCIALE) est attribué aux informations dont la divulgation non autorisée est susceptible de causer des dommages exceptionnellement graves à la sécurité nationale ;

b) STRICT SECRET (STRICT SECRET) est attribué aux informations dont la divulgation non autorisée est susceptible de causer de graves dommages à la sécurité nationale ;

c) SECRET (SECRET) est attribué aux informations dont la divulgation non autorisée est susceptible de causer des dommages à la sécurité nationale ;

d) SECRET DE SERVICIU (SECRET PROFESSIONNEL) est attribué aux informations dont la divulgation non autorisée est susceptible de causer des préjudices à une personne morale publique ou privée.

3) Les niveaux de classification pour la République fédérale d'Allemagne sont définis comme suit :

a) STRENG GEHEIM, au cas où la connaissance par une autre personne non autorisée risque de porter atteinte à l'existence ou aux intérêts vitaux de la République fédérale d'Allemagne ou de l'un de ses territoires ;

b) GEHEIM, dans le cas où la connaissance par une autre personne non autorisée risque de porter atteinte à la sécurité de la République fédérale d'Allemagne ou de l'un de ses territoires ou si elle risque de causer des dommages sérieux à leurs intérêts ;

c) VS-VERTRAULICH, dans le cas où la connaissance par une autre personne non autorisée risque de nuire aux intérêts de la République fédérale d'Allemagne ou de l'un de ses territoires ;

d) VS-NUR FÜR DEN DIENSTGEBRAUCH, dans le cas où la connaissance par une autre personne non autorisée risque d'être un désavantage pour la République fédérale d'Allemagne ou pour l'un de ses territoires.

4) Les Parties contractantes ont établi que l'équivalence des niveaux de classification nationaux est la suivante :

Roumanie	République fédérale d'Allemagne
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ (STRICT SECRET D'UNE IMPORTANCE SPÉCIALE)	STRENG GEHEIM
STRICT SECRET (STRICT SECRET)	GEHEIM
SECRET (SECRET)	VS-VERTRAULICH
	VS-NUR FÜR DEN DIENSTGEBRAUCH

5) La Partie contractante réceptrice marque les informations classifiées échangées, reçues ou produites avec un niveau de classification équivalent à celui attribué aux informations classifiées par la Partie contractante émettrice et leur attribue le même degré de protection que celui prévu pour ses propres informations classifiées avec le même niveau de classification équivalent.

Article 5. Protection des informations classifiées

1) Conformément à la réglementation nationale, les Parties contractantes prennent les mesures adéquates pour protéger les informations classifiées qui sont envoyées, reçues ou produites entre des institutions publiques ou des personnes morales publiques ou privées de leurs États ;

2) La Partie contractante réceptrice et les organismes publics ou les personnes morales publiques ou privées de l'État qu'elle représente ne peuvent ni abaisser le niveau de classification de sécurité appliqué aux informations classifiées ni les déclassifier sans le consentement préalable, donné par écrit, de l'autorité compétente en matière de sécurité de l'État de la Partie contractante émettrice. L'autorité compétente en matière de sécurité de la Partie contractante émettrice informe l'autorité compétente en matière de sécurité de l'autre Partie de toute modification du niveau de classification des informations classifiées échangées ;

3) Les informations classifiées reçues ne peuvent être multipliées et modifiées qu'avec le consentement écrit de la Partie contractante émettrice. Toutes les copies des informations classifiées sont marquées du même niveau de classification que l'original et sont protégées de la même manière que les informations classifiées d'origine. Le nombre de copies est limité au nombre requis aux fins officielles ;

4) Les informations classifiées ne sont détruites qu'avec le consentement préalable écrit ou sur demande de la Partie contractante émettrice, conformément aux réglementations nationales des Parties contractantes, de sorte que leur reconstitution, en totalité ou en partie, soit impossible. La Partie contractante réceptrice informe immédiatement la Partie contractante émettrice de la destruction des informations classifiées. Si la Partie contractante émettrice ne donne pas son accord pour la destruction de certaines informations classifiées, celles-ci sont renvoyées ;

5) Les informations dont le niveau de classification est STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / STRENG GEHEIM (STRICT SECRET D'IMPORTANCE SPÉCIALE) ne sont pas détruites, mais sont renvoyées à la Partie contractante émettrice. En cas de danger imminent, ces informations doivent être détruites également sans autorisation préalable et l'autorité compétente en matière de sécurité de la Partie contractante émettrice est immédiatement informée de la destruction et de ses circonstances ;

6) L'accès aux zones et aux objectifs dans lesquels se déroulent des activités impliquant l'utilisation d'informations classifiées ou dans lesquels ces informations sont stockées, est exclusivement autorisé aux personnes titulaires d'un certificat de sécurité du personnel, correspondant à la classification de ces informations classifiées, conformément au principe du « besoin d'en connaître » ;

7) L'accès aux informations classifiées est autorisé, en respectant le principe du « besoin d'en connaître », exclusivement aux personnes qui sont déjà titulaires d'un certificat de sécurité du personnel valable pour la classification des informations auxquelles l'accès est nécessaire.

Article 6. Certificat de sécurité du personnel

- 1) Chaque Partie contractante garantit que toute personne qui doit accéder à des informations classifiées dans l'exercice de ses fonctions est titulaire d'un certificat de sécurité du personnel valide et de niveau approprié ;
- 2) Le certificat de sécurité du personnel est délivré après le contrôle de sécurité effectué conformément à la réglementation nationale des Parties contractantes, correspondant au niveau d'exigence requis pour accéder aux informations nationales classifiées de niveau de classification équivalent ;
- 3) Sur demande, les autorités compétentes en matière de sécurité ou, le cas échéant, les autorités désignées en matière de sécurité, conformément à la réglementation nationale, se prêtent mutuellement assistance pour les procédures de contrôle concernant la délivrance du certificat de sécurité du personnel et du certificat de sécurité industrielle ;
- 4) Les Parties contractantes reconnaissent mutuellement les certificats de sécurité du personnel et les certificats de sécurité industrielle, délivrés conformément aux réglementations nationales ;
- 5) Les autorités compétentes en matière de sécurité s'informeront de toute modification des certificats de sécurité du personnel et des certificats de sécurité industrielle, notamment en cas de retrait.

Article 7. Diffusion d'informations classifiées

- 1) Les informations classifiées ne peuvent être diffusées à des tiers qu'avec l'accord écrit de l'autorité compétente en matière de sécurité de la Partie contractante émettrice qui peut imposer de nouvelles restrictions sur leur diffusion ;
- 2) Chaque Partie contractante veille à ce que les informations classifiées reçues de l'autre Partie contractante soient utilisées uniquement aux fins pour lesquelles elles ont été transmises.

Article 8. Visites

- 1) Les visiteurs du territoire national de l'une des Parties contractantes sont autorisés, sur le territoire national de l'autre Partie contractante, à accéder aux informations classifiées de niveau SECRET / VS-VERTRAULICH et supérieur et dans les zones et objectifs dans lesquels elles sont utilisées pour le travail, uniquement avec l'accord préalable de l'autorité compétente en matière de sécurité de la Partie contractante qui fait l'objet d'une visite. Les visites qui supposent l'accès uniquement à des informations classifiées SECRET DE SERVICIU / VS-NUR FÜR DEN DIENSTGEBRAUCH peuvent faire l'objet d'un accord direct entre les agents responsables de la sécurité du visiteur et l'objectif visité ;
- 2) La demande de visite doit être reçue au moins vingt jours ouvrables avant la visite prévue. En cas d'urgence, les autorités compétentes en matière de sécurité peuvent convenir d'une période plus courte ;
- 3) L'autorité compétente en matière de sécurité de la Partie contractante qui a reçu la demande de visite informe en temps utile l'autorité compétente en matière de sécurité de l'autre Partie de la décision prise ;

4) Après l'approbation de la visite, l'autorité compétente en matière de sécurité de la Partie contractante sur le territoire de laquelle la visite doit être effectuée s'assure qu'une copie de la demande de visite est envoyée à l'agent responsable de la sécurité de l'institution, de l'objectif ou de l'organisation qui fait l'objet d'une visite ;

5) La validité de l'autorisation de visite ne doit pas dépasser douze mois ;

6) Pour chaque contrat classifié, les Parties contractantes peuvent convenir de listes reprenant les personnes autorisées à effectuer des visites périodiques. Ces listes sont valables pour une période de douze mois ;

7) Après l'approbation des listes par les Parties contractantes, les détails ultérieurs concernant les visites sont établis directement entre les représentants des organisations concernées, conformément aux modalités convenues ;

8) La demande de visite est soumise dans la langue du pays à visiter ou en langue anglaise et contiendra les informations suivantes :

a) le nom et le prénom, la date et le lieu de naissance, ainsi que le numéro du passeport ou du document d'identité du visiteur ;

b) la citoyenneté du visiteur ;

c) la fonction du visiteur et le nom de l'autorité ou de l'entité qu'il représente ;

d) le niveau d'autorisation d'accès aux informations classifiées détenues par le visiteur ;

e) le but de la visite et la date ou la période prévue pour la visite ;

f) les institutions, personnes de contact et objectifs qui seront visités.

9) Chaque Partie contractante garantit la protection des données à caractère personnel des visiteurs conformément à la réglementation nationale en la matière.

Article 9. Sécurité industrielle

1) Dans le cas où une Partie contractante, respectivement les entités publiques ou privées sur son territoire, a l'intention d'attribuer un contrat classifié à une entité publique ou privée située sur le territoire de l'autre Partie contractante, la Partie contractante de l'État dans lequel le contrat classifié est exécuté prend la responsabilité de protéger les informations classifiées relatives au contrat, conformément à sa réglementation et aux dispositions du présent Accord ;

2) Avant d'attribuer un contrat classifié, le bénéficiaire demande à l'autorité compétente en matière de sécurité du contractant, par l'intermédiaire de son autorité compétente en matière de sécurité, la confirmation de l'existence d'un certificat de sécurité industrielle attestant que ledit contractant est sous la coordination de l'autorité compétente en matière de sécurité de la Partie contractante du point de vue de la protection des informations classifiées, et qu'il a pris les mesures de protection nécessaires à l'exécution du contrat ;

3) Le certificat de sécurité industrielle est également nécessaire si le contractant a été invité à soumettre une proposition et que, dans le cadre de la procédure d'appel d'offres, il se voit confier des informations classifiées avant même l'attribution du contrat ;

4) Les demandes de notification de la confirmation de l'existence du certificat de sécurité industrielle pour les contractants sur le territoire de l'autre Partie contractante comprennent des données sur le projet, ainsi que sur le type, le volume et le niveau de classification des informations classifiées à notifier au contractant ou à générer par celui-ci ;

5) La confirmation de l'existence du certificat de sécurité industrielle comprend le nom complet du contractant, son adresse postale, le nom de l'agent responsable de la sécurité, les numéros de téléphone et de télécopieur, l'adresse électronique, ainsi que le niveau de classification des informations jusqu'auquel le contractant concerné a pris des mesures de protection conformément à la réglementation nationale ;

6) Les autorités compétentes en matière de sécurité des Parties contractantes notifient mutuellement les modifications apportées aux éléments qui sous-tendent la délivrance des certificats de sécurité industrielle, dans la mesure où la protection des informations classifiées échangées dans le cadre du présent Accord est affectée ;

7) L'échange de notifications entre les autorités compétentes en matière de sécurité s'effectue dans la langue nationale de l'autorité notifiée ou en anglais ;

8) La confirmation de l'existence du certificat de sécurité industrielle et les demandes notifiées aux autorités compétentes en matière de sécurité des Parties contractantes relatives à la notification de la confirmation du certificat de sécurité industrielle doivent être soumises par écrit ;

9) Les Parties contractantes prennent des mesures pour que chaque contrat classifié comprenne une annexe relative à la sécurité rédigée par le bénéficiaire, qui comprend au moins des informations relatives :

a) au volume et aux niveaux de classification des informations classifiées à notifier au contractant ou à générer par celui-ci ;

b) aux mesures de protection qui doivent être mises en œuvre par le contractant ;

c) à la procédure de notification des changements intervenus dans les niveaux de classification ;

d) aux moyens de transport des informations classifiées ;

e) à l'obligation de notifier toute compromission réelle ou possible liée aux informations classifiées.

10) Une copie de l'annexe relative à la sécurité est notifiée à l'autorité compétente en matière de sécurité de la Partie contractante sur le territoire de laquelle le contrat classifié est exécuté ;

11) Le sous-traitant doit satisfaire aux mêmes exigences de sécurité que le contractant.

Article 10. Transmission des informations classifiées

1) Les informations classifiées sont transmises par la voie diplomatique ou militaire ou par tout autre moyen convenu par les autorités compétentes en matière de sécurité. Les informations classifiées STRICT SECRET D'IMPORTANCE SPÉCIALE/STRENG GEHEIM sont transmises uniquement par la voie diplomatique. L'autorité compétente en matière de sécurité de la Partie contractante réceptrice confirme par écrit la réception des informations classifiées ;

2) Si un grand volume d'informations classifiées doit être transmis, les autorités compétentes en matière de sécurité conviennent au cas par cas du moyen de transport, de l'itinéraire et des mesures de sécurité ;

3) Les autorités compétentes en matière de sécurité peuvent accepter, dans des cas exceptionnels, pour un projet précisément spécifié, que les informations classifiées d'un niveau de classification SECRET / VS-VERTRAULICH et STRICT SECRET / GEHEIM soient transportées par d'autres moyens que ceux prévus au paragraphe 1, et seulement si l'utilisation des

moyens prévus audit paragraphe risque de porter atteinte à la sécurité nationale ou d'affecter l'exécution d'un contrat classifié. Dans ce cas, les exigences minimales suivantes sont respectées :

- a) le transporteur doit être certifié conformément à la réglementation nationale pour l'accès aux informations classifiées avec un niveau de classification adéquat ;
- b) l'entité expéditrice doit conserver une liste des informations classifiées transportées ; une copie de cette liste est remise au destinataire pour qu'il la notifie à l'autorité compétente en matière de sécurité ;
- c) les informations classifiées doivent être emballées conformément à la réglementation nationale de la Partie contractante expéditrice ;
- d) les informations classifiées doivent être remises sur la base de l'accusé de réception ;
- e) le transporteur doit avoir sur lui une preuve de transporteur délivrée conformément à la réglementation nationale.

4) Les informations classifiées cryptées d'un niveau de classification SECRET / VS-VERTRAULICH et STRICT SECRET / GEHEIM ne peuvent être notifiées que par des systèmes d'information et de communication certifiés par les autorités compétentes en matière de sécurité. Les informations classifiées cryptées d'un niveau de classification SECRET PROFESSIONNEL / VS-NUR FÜR DEN DIENSTGEBRAUCH peuvent être notifiées par le biais des systèmes d'information et de communication publics, en utilisant des moyens de cryptage certifiés par les autorités compétentes en matière de sécurité. Les Parties contractantes reconnaissent mutuellement la certification de leurs propres systèmes d'information et de communication utilisés pour le stockage et le traitement des informations classifiées reçues. En cas d'interconnexion, les Parties contractantes conviennent mutuellement des moyens de cryptage utilisés pour l'échange d'informations classifiées.

Article 11. Compromission des informations classifiées

- 1) Les Parties contractantes se notifient rapidement par écrit la survenance de toute compromission réelle ou possible des informations classifiées ;
- 2) L'enquête sur toute compromission d'informations classifiées est menée sans délai conformément à la réglementation nationale de la Partie contractante sur le territoire de laquelle la compromission s'est produite. Si nécessaire, les autorités compétentes en matière de sécurité coopèrent à cette enquête ;
- 3) L'autorité compétente en matière de sécurité de la Partie contractante sur le territoire de laquelle la compromission des informations classifiées s'est produite notifie par écrit à l'autorité compétente en matière de sécurité de l'autre Partie contractante les circonstances de la compromission des informations classifiées, l'étendue des dommages, les mesures qui ont été adoptées pour atténuer l'étendue des dommages et les résultats de l'enquête ;

Article 12. Règlement des différends

Les différends liés à l'élaboration ou à l'application du présent Accord sont exclusivement réglés par des négociations entre les autorités compétentes en matière de sécurité des Parties contractantes. Pendant les négociations, les Parties contractantes continuent à remplir leurs obligations en vertu du présent Accord.

Article 13. Frais

Chaque Partie contractante prend en charge les frais qui peuvent résulter de l'application du présent Accord conformément à sa propre réglementation. Les frais générés par une Partie contractante ne peuvent être prélevés sur l'autre Partie contractante.

Article 14. Consultations

- 1) Les autorités compétentes en matière de sécurité des Parties contractantes se notifient, sur demande, les dispositions en vigueur relatives à la protection des informations classifiées ;
- 2) Afin d'assurer une coopération étroite dans l'application du présent Accord, les autorités compétentes en matière de sécurité se consultent mutuellement, sur demande ;
- 3) Chaque Partie contractante autorise l'autre Partie contractante à recevoir sur son propre territoire la visite des représentants des autorités compétentes ou des autorités désignées en matière de sécurité pour des consultations relatives à l'organisation et aux procédures de sécurité en vigueur pour la protection des informations classées reçues. Les détails des visites sont établis mutuellement par les autorités compétentes ou par les autorités désignées en matière de sécurité.

Article 15. Dispositions finales

- 1) Le présent Accord est conclu pour une durée indéterminée ;
- 2) Le présent Accord entre en vigueur le jour où le Gouvernement de la Roumanie notifie au Gouvernement de la République fédérale d'Allemagne l'accomplissement des procédures internes nécessaires à cet effet. Le jour de la réception de la notification est déterminant ;
- 3) Chaque Partie contractante peut dénoncer le présent Accord par écrit, par la voie diplomatique, en observant un délai de six mois. Celui-ci commence à partir de la date de réception de la notification. En cas de dénonciation, les informations classifiées transmises sur la base du présent Accord ou générées par le contractant seront gérées conformément aux dispositions du présent Accord, tant que la classification existante le justifie ;
- 4) Le présent Accord peut être modifié par consentement mutuel écrit des Parties contractantes. Ces modifications entrent en vigueur conformément au paragraphe 2 ;
- 5) L'entrée en vigueur du présent Accord met fin à « l'Accord entre le Gouvernement de la Roumanie et le Gouvernement de la République fédérale d'Allemagne relatif à la protection mutuelle des informations classifiées, signé le 24 novembre 1997 à Bucarest ». Depuis cette date, toutes les informations classifiées envoyées seront protégées conformément aux dispositions du présent Accord ;
- 6) L'enregistrement du présent Accord par le Secrétariat des Nations Unies, conformément à l'article 102 de la Charte des Nations Unies, est effectué immédiatement après son entrée en vigueur, par la Partie contractante sur le territoire de laquelle le présent Accord a été conclu. L'autre Partie contractante est informée de l'enregistrement effectué, en indiquant le numéro d'enregistrement de l'ONU, dès qu'il a été reconnu par le Secrétariat des Nations Unies.

FAIT à Bucarest le 14 décembre 2016, en deux exemplaires originaux, en langues roumaine et allemande, les deux textes faisant également foi.

Pour le Gouvernement de la Roumanie :

MARIUS PETRESCU,

Professeur d'université, PhD.

Secrétaire d'État

Directeur général du Bureau d'enregistrement des informations classifiées

Pour le Gouvernement de la République fédérale d'Allemagne :

WERNER HANS LAUK

Ambassadeur extraordinaire et plénipotentiaire de la République fédérale d'Allemagne