No. 55413*

Poland
and
Romania

Agreement between the Government of the Republic of Poland and the Government of Romania on the mutual protection of classified information. Bucharest, 5 July 2006

Entry into force: *1 June 2007, in accordance with article 15*

Authentic texts: *English, Polish and Romanian*

Registration with the Secretariat of the United Nations: *Poland, 30 October 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.*

Pologne
et
Roumanie

Accord entre le Gouvernement de la République de Pologne et le Gouvernement de la Roumanie relatif à la protection mutuelle des informations classifiées. Bucarest, 5 juillet 2006

Entrée en vigueur : *1er juin 2007, conformément à l'article 15*

Textes authentiques : *anglais, polonais et roumain*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Pologne, 30 octobre 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.*

[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT

between

the Government of the Republic of Poland

and

the Government of Romania

on the Mutual Protection of Classified Information

The Government of the Republic of Poland and the Government of Romania,

hereinafter referred to as "the Contracting Parties",

Developing co-operation based on mutual interest and confidence,

Having due regard for guaranteeing mutual protection of all information

which has been classified pursuant to the internal legislation of either

Contracting Party and transmitted to the other Contracting Party,

Have agreed as follows:

ARTICLE 1

DEFINITIONS

For the purpose of this Agreement, the following terms are defined:

a) **"Classified Information"** - any information which, irrespective of the form and manner of expression thereof, also during the preparation thereof, is classified according to the internal legislation of each Contracting Party as requiring protection against unauthorized disclosure;

b) **"Competent Security Authority"** - a state authority competent for the protection of Classified Information as stated in Article 3;

c) **"Authorized Entity"** - a body or an institution with competencies in the field of protection of Classified Information specified in the internal legislations of the Contracting Parties, authorized to issue, transmit, receive, store, protect and use Classified Information;

d) **"Contractor/Subcontractor"** - an individual or a legal entity who intends to conclude or is a party to a Classified Contract;

e) **"Classified Contract"** - an agreement between two or more Contractors/Subcontractors creating and defining enforceable rights and obligations between them, which contains or involves Classified Information;

f) **"Prime-Contractor"** - a state body or legal entity which intends to grant or grants the performance of a Classified Contract in the territory of the state of the other Contracting Party;

g) **"Third Party"** - any individual, institution, national and international organization, public or private entity or a state that is not a party to this Agreement;

h) **"Personnel Security Clearance"** - a document attesting that the holder may have access to Classified Information in accordance with the internal legislation

of the Contracting Party;

i) **"Facility Security Clearance"** - a document issued by the Competent Security Authority attesting that the Contractor/Subcontractor has the physical and organizational capability of using and storing Classified Information in accordance with the internal legislation of the Contracting Party;

j) **"Security Aspects Letter"** - a document issued by the Prime-Contractor related to a Classified Contract, identifying the security requirements or those elements of the contract requiring protection;

k) **"Security Classification Check-List"** - a listing of the information connected with the various aspects of a Classified Contract that should be classified according to a specified security classification level.

ARTICLE 2

SECURITY CLASSIFICATIONS

The Contracting Parties agree that the following security classification levels are equivalent:

Republic of Poland	**Romania**	**English language equivalent**
ŚCIŚLE TAJNE	STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TOP SECRET
TAJNE	STRICT SECRET	SECRET
POUFNE	SECRET	CONFIDENTIAL
ZASTRZEŻONE	SECRET DE SERVICIU	RESTRICTED

ARTICLE 3

COMPETENT SECURITY AUTHORITY

1. For the purpose of this Agreement, the Competent Security Authority shall be:
   - for the Republic of Poland: the Head of the Internal Security Agency – in the civil sphere and the Head of the Military Information Services – in the military sphere;
   - for Romania: the National Registry Office for Classified Information.
2. In order to achieve and maintain comparable standards of security, the Competent Security Authorities of the Contracting Parties shall provide each other information about the adopted security standards, procedures and practices applicable for protection of Classified Information.
3. The Competent Security Authorities shall, upon request and taking into account their internal legislation, assist each other in the security clearance procedures for the issuance of the Personnel Security Clearance and the Facility Security Clearance.
4. The Competent Security Authorities may conclude agreements for the purpose of implementation of the provisions hereof.

ARTICLE 4

PROTECTION OF CLASSIFIED INFORMATION

1. In accordance with this Agreement and their internal legislation, the Contracting Parties shall adopt appropriate measures to protect Classified Information which is transmitted or originated as a result of their mutual co-operation.
2. The Contracting Parties shall provide for the information referred to in paragraph 1 at least the same protection as applicable to their own Classified Information

under relevant security classification level, pursuant to Article 2.

3. Classified Information shall be used exclusively in accordance with the purpose for which it has been transmitted or originated.
4. The Contracting Party which has received the information referred to in paragraph 1 shall not release such information to any Third Party, without the prior written consent of the originating Contracting Party.
5. Under the provisions of paragraph 4, when the receiving Contracting Party transmits to a Third Party Classified Information of the originating Contracting Party, the receiving Contracting Party shall inform the originating Contracting Party of any breach of security occurred on the territory of the Third Party.
6. Classified Information transmitted hereunder shall be accessible only to those persons who have a need to know, who have been security cleared and authorized to have access to such information in accordance with the internal legislation of the Contracting Party.
7. The originating Contracting Party is exclusively authorized to change the security classification level or to declassify the transmitted Classified Information. The Competent Security Authorities and the Authorized Entities of the Contracting Parties shall inform each other of any changes in security classification levels or declassification of transmitted information.
8. The assignment of a security classification level to jointly created Classified Information, its change or the declassification of this information shall be made upon common consent of the Competent Security Authorities and the Authorized Entities of the Contracting Parties.
9. If either Contracting Party decides that transmission of Classified Information or implementation of a joint venture could jeopardize the sovereignty of the state of this Contracting Party, threaten its security or other important interests, or could cause damages to the legal system, may partially or completely refuse co-operation or make it dependent on certain conditions.

10. The Competent Security Authorities shall mutually recognize the Personnel Security Clearance and the Facility Security Clearance issued upon the security clearance procedure conducted in accordance with their internal legislations, after a prior written confirmation of the authenticity thereof by the Competent Security Authority. The Competent Security Authorities shall inform each other without delay about changes in access to Classified Information related to the implementation of this Agreement.

ARTICLE 5

CLASSIFIED CONTRACTS

1. The Prime-Contractor may conclude a Classified Contract with the Contractor located in the territory of the State of the other Contracting Party. In such case the Prime-Contractor should obtain, through its Competent Security Authority, an assurance from the Competent Security Authority of the other Contracting Party that the Contractor is authorized to have access to Classified Information of the specified security classification level and that:

   a) the Contractor was granted the Facility Security Clearance;

   b) all of the Contractor's personnel whose positions and duties require access to Classified Information were granted the Personnel Security Clearance.

2. If the Contractor does not meet the requirements referred to in paragraph 1, the Competent Security Authority which is to issue the assurance shall immediately inform the Competent Security Authority of the other Contracting Party that, upon its request, necessary actions shall be taken for the issue to the Contractor of an authorization to have access to Classified Information.

3. Each Classified Contract shall be accompanied by the Security Aspects Letter and the Security Classification Check-List. Copies of these documents shall be

submitted to the Competent Security Authority.

ARTICLE 6

MARKING OF CLASSIFIED INFORMATION

1. Classified Information received from the other Contracting Party shall be marked with a security classification level, according to the corresponding classification level stipulated in Article 2.
2. Copies and translations of received Classified Information shall be marked and handled in the same manner as the originals, with the observance of the provisions stipulated in Article 8.
3. The requirements referred to in paragraphs 1 and 2 shall also apply to Classified Information originated in the performance of a Classified Contract.

ARTICLE 7

TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted between the Contracting Parties followed by a written confirmation of receipt, through diplomatic channels or through other channels, ensuring protection against unauthorized disclosure, agreed upon by the Competent Security Authorities of both Contracting Parties.
2. Classified Information may be transmitted via protected information technology systems and networks which have been authorized for use pursuant to the internal legislation of either Contracting Party.

ARTICLE 8

REPRODUCTION AND TRANSLATION OF CLASSIFIED INFORMATION

1. Classified Information marked with the ŚCIŚLE TAJNE / STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ security classification level shall be reproduced only with a prior written permission issued by the Authorized Entity of the Originating Contracting Party.
2. All reproduced Classified Information shall be placed under the same protection as the originals. The number of copies shall be restricted to that required for official purposes.
3. All translations of Classified Information shall be made by security cleared individuals. All translations shall bear an appropriate annotation in the language into which they have been translated stating that the translations contain Classified Information of the Authorized Entity.

ARTICLE 9

DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Information shall be destroyed only with a written approval or at the request of the Authorized Entity or the Competent Security Authority which provided the Classified Information in such a manner as to eliminate the partial or total reconstruction of the same. The Authorized Entity or the Competent Security Authority which provided the Classified Information shall be informed of its destruction.
2. In the case that the Authorized Entity or the Competent Security Authority which provided the Classified Information does not agree to the destruction of the same, such Classified Information shall be returned to it.

3. Classified Information marked as ȘCIȘLE TAJNE / STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ shall not be destroyed. It shall be returned to the Authorized Entity or the Competent Security Authority which provided the same.

ARTICLE 10

VISITS

1. Persons arriving on a visit from either Contracting Party to the territory of the state of the other Contracting Party shall be allowed access to Classified Information to the necessary extent as well as to the premises where such Classified Information is handled only after a prior receipt of a written permit issued by the Competent Security Authority or the Authorized Entity of the other Contracting Party. The Authorized Entity shall inform the Competent Security Authority of its intention to issue such permit.
2. The permit referred to in paragraph 1 shall be granted exclusively to persons authorized to have access to Classified Information pursuant to the internal legislation of the Contracting Party delegating such persons.
3. To the extent required to obtain the permit referred to in paragraph 1, the personal data of the persons arriving on a visit to the other Contracting Party shall be transferred 25 working days in advance to the Authorized Entity or the Competent Security Authority of that Contracting Party.
4. The Authorized Entities or the Competent Security Authorities of both Contracting Parties shall inform each other of the details of an application for a visit and shall ensure the protection of personal data. The application shall contain at least the following:

a) name of the proposed visitor, date and place of birth, nationality, passport/identity card number;

b) official status of the visitor together with the name of the establishment, company or organization which he/she represents or belongs to;
c) certification of level of security clearance of the visitor;
d) name and address of the establishment, company or organization to be visited;
e) name and status of the person(s) to be visited, if known;
f) purpose of the visit;
g) dates of arrival and departure.

ARTICLE 11

BREACH OF SECURITY REGULATIONS

1. In the case of a breach of security regulations that results in a disclosure or threat of disclosure of Classified Information received from the Authorized Entity or the Competent Security Authority of the other Contracting Party, the Competent Security Authority of the Contracting Party on whose territory such event occurred, shall immediately inform the Competent Security Authority of the other Contracting Party thereof.
2. A breach of security regulations concerning mutual protection of Classified Information shall be investigated and prosecuted in accordance with the internal legislation of the Contracting Party on whose territory such breach occurred.
3. The Competent Security Authority of the Contracting Party on whose state territory the breach occurred shall immediately inform the Competent Security Authority of the other Contracting Party of the result of the actions referred to in paragraph 2.

ARTICLE 12
EXPENSES

Each Contracting Party shall cover its own expenses incurred in connection with the implementation of this Agreement.

ARTICLE 13
CONSULTATIONS

1. In order to achieve and maintain comparable standards of security, the Competent Security Authorities of the Contracting Parties shall currently inform each other about any amendments in their internal legislation regarding the protection of Classified Information related to this Agreement.
2. The Competent Security Authorities of the Contracting Parties shall consult each other upon request of one of them in order to ensure close co-operation in the implementation of the provisions of this Agreement.
3. Each Contracting Party shall allow representatives of the Competent Security Authority of the other Contracting Party to come on visits on its territory to discuss the procedures for protection of Classified Information transmitted to it by the other Contracting Party.

ARTICLE 14
SETTLEMENT OF DISPUTES

1. Any disputes concerning the interpretation or application of this Agreement shall be settled by means of mutual consultation between the Competent Security Authorities.

2. If the settlement of a dispute may not be reached in the manner referred to in paragraph 1, such dispute shall be settled through diplomatic channels.

ARTICLE 15

FINAL PROVISIONS

1. This Agreement shall enter into force on the first day of the second month after the receipt of the latter of the notifications through which the Contracting Parties mutually inform each other on the completion of the internal legal procedures necessary in this regard.
2. This Agreement is concluded for an unlimited period of time. It may be denounced by either Contracting Party upon notice to the other Contracting Party. In such case this Agreement shall be terminated after six months following the receipt of the denunciation notice.
3. In the event of termination of this Agreement, Classified Information transmitted hereunder or originated in the course of the mutual co-operation of the Contracting Parties shall continue to be protected pursuant to the provisions hereof as long as required according to the security classification level.
4. This Agreement may be amended on the basis of mutual written consent of both Contracting Parties. The amendments shall enter into force in accordance with the provisions of paragraph 1.

Done in Bucharest on 5th of July 2006, in two original copies, each in the Polish, Romanian and English languages, all texts being equally authentic. In the case of any differences in interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND

MAREK PASIONEK
Under-Secretary of Sate in the Chancellery of the Prime Minister

FOR THE GOVERNMENT OF ROMANIA

Prof. dr. MARIUS PETRESCU
Secretary of State
Director General
of the National Registry Office for Classified Information

[POLISH TEXT – TEXTE POLONAIS]

UMOWA

między Rządem Rzeczypospolitej Polskiej

a Rządem Rumunii

o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Rumunii,

zwane dalej „Umawiającymi się Stronami",

rozwijając współpracę w oparciu o wzajemny interes i zaufanie,

mając na uwadze zagwarantowanie wzajemnej ochrony wszystkich informacji, które zostały zaklasyfikowane jako informacje niejawne zgodnie z prawem wewnętrznym jednej z Umawiających się Stron i przekazane drugiej Umawiającej się Stronie,

uzgodniły co następuje:

ARTYKUŁ 1

DEFINICJE

Dla celów niniejszej Umowy poniższe terminy oznaczają:

a) **„informacje niejawne"** – wszelkie informacje, które niezależnie od formy i sposobu ich wyrażenia, także w trakcie ich opracowywania, są zaklasyfikowane, zgodnie z prawem wewnętrznym każdej z Umawiających się Stron, jako wymagające ochrony przed nieuprawnionym ujawnieniem,

b) **„właściwy organ bezpieczeństwa"** – organ państwowy, właściwy w sprawie ochrony informacji niejawnych, wskazany w artykule 3,

c) **„podmiot uprawniony"** – określony w prawie wewnętrznym Umawiających się Stron podmiot (albo instytucja), właściwy w zakresie ochrony informacji niejawnych, uprawniony do wytwarzania, przekazywania, otrzymywania, przechowywania, ochrony i wykorzystywania informacji niejawnych,

d) **„kontrahent/podwykonawca"** – osoba fizyczna lub prawna, która zamierza zawrzeć albo jest stroną kontraktu niejawnego,

e) **„kontrakt niejawny"** – umowa pomiędzy dwoma lub więcej kontrahentami/podwykonawcami powołująca i określająca wzajemne prawa i zobowiązania między nimi, która dotyczy albo zawiera informacje niejawne,

f) **„zlecający"** – organ państwa albo osoba prawna, która zamierza przekazać lub przekazuje wykonanie kontraktu niejawnego na terytorium państwa drugiej Umawiającej się Strony,

g) **„strona trzecia"** – osoba fizyczna, instytucja, państwowa i międzynarodowa organizacja, podmiot publiczny lub prywatny albo państwo, które nie jest stroną niniejszej Umowy,

h) **„poświadczenie bezpieczeństwa"** – dokument potwierdzający, że jego posiadacz może uzyskać dostęp do informacji niejawnych zgodnie z prawem wewnętrznym Umawiającej się Strony,

i) **„świadectwo bezpieczeństwa przemysłowego"** – dokument wydany przez właściwy organ bezpieczeństwa potwierdzający, że kontrahent/ podwykonawca posiada fizyczną i organizacyjną zdolność do wykorzystywania i przechowywania informacji niejawnych zgodnie z prawem wewnętrznym Umawiającej się Strony,

j) **„instrukcja bezpieczeństwa przemysłowego"** – dokument wydany przez zlecającego dotyczący kontraktu niejawnego, określający wymagania bezpieczeństwa lub te fragmenty kontraktu, które wymagają ochrony,

k) **„wykaz kontrolny informacji niejawnych"** – wykaz informacji związanych z różnymi aspektami kontraktu niejawnego, które powinny być objęte określoną klauzulą tajności.

ARTYKUŁ 2

KLAUZULE TAJNOŚCI

Umawiające się Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

Rzeczpospolita Polska	**Rumunia**	**odpowiednik w języku angielskim**
ŚCIŚLE TAJNE	STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TOP SECRET
TAJNE	STRICT SECRET	SECRET
POUFNE	SECRET	CONFIDENTIAL
ZASTRZEŻONE	SECRET DE SERVICIU	RESTRICTED

ARTYKUŁ 3

WŁAŚCIWE ORGANY BEZPIECZEŃSTWA

1. W rozumieniu niniejszej Umowy, właściwymi organami bezpieczeństwa, są:
   - w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego – w sferze cywilnej i Szef Wojskowych Służb Informacyjnych – w sferze wojskowej,
   - w Rumunii: Narodowy Urząd Ochrony Informacji Niejawnych.
2. W celu osiągnięcia i utrzymania porównywalnych standardów bezpieczeństwa, właściwe organy bezpieczeństwa Umawiających się Stron będą przekazywały sobie wzajemnie informacje o przyjętych standardach bezpieczeństwa, procedurach i praktyce odpowiedniej dla ochrony informacji niejawnych.
3. Właściwe organy bezpieczeństwa na wniosek i z uwzględnieniem prawa wewnętrznego będą pomagać sobie nawzajem w przeprowadzaniu postępowań sprawdzających w celu wydania poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego.
4. Właściwe organy bezpieczeństwa mogą zawierać między sobą porozumienia wykonawcze w celu realizacji postanowień niniejszej Umowy.

ARTYKUŁ 4

OCHRONA INFORMACJI NIEJAWNYCH

1. Zgodnie z niniejszą Umową i swoim prawem wewnętrznym, Umawiające się Strony podejmą stosowne działania w celu ochrony informacji niejawnych, które będą przekazywane lub powstaną w wyniku ich wzajemnej współpracy.
2. Umawiające się Strony zapewnią informacjom, o których mowa w ustępie 1, co najmniej taką samą ochronę, jaka obowiązuje w stosunku do własnych

informacji niejawnych objętych odpowiednią klauzulą tajności, zgodnie z artykułem 2.

3. Informacje niejawne będą wykorzystywane wyłącznie zgodnie z celem, w jakim zostały przekazane lub wytworzone.
4. Umawiająca się Strona, która otrzymała informację, o której mowa w ustępie 1, nie będzie udostępniać stronie trzeciej tych informacji, bez uprzedniej pisemnej zgody Umawiającej się Strony wytwarzającej.
5. W przypadku gdy, zgodnie z postanowieniami ustępu 4, Umawiająca się Strona otrzymująca przekaże stronie trzeciej informacje niejawne Umawiającej się Strony wytwarzającej, Umawiająca się Strona otrzymująca będzie informować Umawiającą się Stronę wytwarzającą o wszelkich naruszeniach zasad bezpieczeństwa, które wydarzyły się na terytorium strony trzeciej.
6. Informacje niejawne przekazywane na podstawie niniejszej Umowy będą udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które, po przeprowadzeniu niezbędnego postępowania sprawdzającego, zostały upoważnione do dostępu do nich, zgodnie z prawem wewnętrznym Umawiających się Stron.
7. Do zmiany albo zniesienia klauzuli tajności przekazanych informacji niejawnych upoważniona jest wyłącznie Umawiająca się Strona wytwarzająca. Właściwe organy bezpieczeństwa i podmioty uprawnione Umawiających się Stron będą wzajemnie informować się o każdym przypadku zmiany albo zniesienia klauzuli tajności przekazanych informacji.
8. Zmiana albo zniesienie przyznanej klauzuli tajności informacji niejawnych wytworzonych wspólnie może nastąpić na podstawie wspólnej zgody właściwych organów bezpieczeństwa i podmiotów uprawnionych Umawiających się Stron.
9. Jeżeli jedna z Umawiających się Stron uzna, że przekazanie informacji niejawnych lub realizacja wspólnego przedsięwzięcia mogłaby naruszyć

suwerenność jej Państwa, zagrażać jego bezpieczeństwu lub innym istotnym interesom albo też naruszałaby zasady jego porządku prawnego, może odmówić częściowo lub całkowicie współpracy lub uzależnić ją od spełnienia określonych warunków.

10. Właściwe organy bezpieczeństwa będą wzajemnie uznawać poświadczenia bezpieczeństwa osób i świadectwa bezpieczeństwa przemysłowego, wydane po przeprowadzeniu postępowania sprawdzającego zgodnie z ich prawem wewnętrznym, po uprzednim pisemnym potwierdzeniu ich autentyczności przez właściwy organ bezpieczeństwa. Właściwe organy bezpieczeństwa będą bezzwłocznie wzajemnie informować się o zmianach w zakresie dostępu do informacji niejawnych dotyczących realizacji niniejszej Umowy.

ARTYKUŁ 5

KONTRAKTY NIEJAWNE

1. Zlecający może zawrzeć kontrakt niejawny z kontrahentem, który posiada siedzibę na terytorium Państwa drugiej Umawiającej się Strony. W takim przypadku zlecający winien uzyskać zapewnienie od właściwego organu bezpieczeństwa tej Umawiającej się Strony, że zaproponowany kontrahent jest upoważniony do dostępu do informacji niejawnych oznaczonych określoną klauzulą tajności, oraz że:
   a) kontrahentowi wydano świadectwo bezpieczeństwa przemysłowego,
   b) wszyscy pracownicy kontrahenta, którzy z racji zajmowanego stanowiska i wykonywanych obowiązków muszą mieć dostęp do informacji niejawnych, posiadają właściwe poświadczenie bezpieczeństwa.
2. Jeżeli kontrahent nie spełnia wymogów, o których mowa w ustępie 1, właściwy organ bezpieczeństwa mający udzielać zapewnienia, informuje niezwłocznie właściwy organ bezpieczeństwa drugiej Umawiającej się

Strony, że na jego wniosek zostaną podjęte niezbędne działania do wydania kontrahentowi upoważnienia do dostępu do informacji niejawnych.

3. Do każdego kontraktu niejawnego dołącza się instrukcję bezpieczeństwa przemysłowego i wykaz kontrolny informacji niejawnych. Kopie tych dokumentów przekazywane są właściwemu organowi bezpieczeństwa.

ARTYKUŁ 6

OZNACZANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne otrzymywane od drugiej Umawiającej się Strony będą oznaczane klauzulami tajności zgodnie z odpowiednikiem klauzuli ustalonym w artykule 2.
2. Kopie i tłumaczenia otrzymywanych informacji niejawnych będą oznaczane i traktowane w ten sam sposób co oryginały, z zachowaniem warunków przewidzianych w artykule 8.
3. Zasady wyrażone w ustępach 1 i 2 odnoszą się również do informacji niejawnych wytworzonych w związku z realizacją kontraktu niejawnego.

ARTYKUŁ 7

PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne będą przekazywane pomiędzy Umawiającymi się Stronami za pisemnym potwierdzeniem odbioru, kanałami dyplomatycznymi albo innymi kanałami zapewniającymi ochronę przed nieuprawnionym ujawnieniem, uzgodnionymi przez właściwe organy bezpieczeństwa obu Umawiających się Stron.
2. Informacje niejawne mogą być przekazywane chronionymi systemami i sieciami teleinformatycznymi dopuszczonymi do eksploatacji zgodnie z prawem wewnętrznym jednej z Umawiających się Stron.

ARTYKUŁ 8

POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą ŚCIŚLE TAJNE/STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ będą powielane tylko po uprzednim wydaniu pisemnego zezwolenia przez podmiot uprawniony Umawiającej się Strony wytwarzającej.
2. Wszystkie powielane informacje niejawne będą podlegały takiej samej ochronie, jak oryginały. Liczba kopii będzie ograniczona do liczby wymaganej dla celów służbowych.
3. Wszystkie tłumaczenia informacji niejawnych będą dokonywane przez osoby posiadające poświadczenie bezpieczeństwa. Wszystkie tłumaczenia będą nosić odpowiednią adnotację w języku, na który dokonano przekładu, stwierdzającą, że tłumaczenie zawiera informacje niejawne podmiotu uprawnionego.

ARTYKUŁ 9

NISZCZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne będą niszczone jedynie za pisemnym pozwoleniem lub na prośbę podmiotu uprawnionego lub właściwych organów bezpieczeństwa, które przekazały informacje niejawne, w taki sposób, żeby wyeliminować ich częściową lub całkowitą rekonstrukcję. Podmiot uprawniony lub właściwy organ bezpieczeństwa, który przekazał informacje niejawne będzie poinformowany o ich zniszczeniu.
2. W przypadku, gdy podmiot uprawniony lub właściwy organ bezpieczeństwa, który przekazał informacje niejawne nie zgadza się na ich zniszczenie, takie informacje niejawne zostaną mu zwrócone.
3. Informacje niejawne oznaczone jako ŚCIŚLE TAJNE/STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ nie będą niszczone. Będą one zwracane

podmiotowi uprawnionemu lub właściwemu organowi bezpieczeństwa, który je przekazał.

ARTYKUŁ 10

WIZYTY

1. Osobom przybywającym z wizytą z Państwa jednej Umawiającej się Strony do Państwa drugiej Umawiającej się Strony zezwala się na dostęp w niezbędnym zakresie do informacji niejawnych, a także do obiektów, w których pracuje się nad informacjami niejawnymi, tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ bezpieczeństwa lub podmiot uprawniony drugiej Umawiającej się Strony. Podmiot uprawniony poinformuje właściwy organ bezpieczeństwa o swoim zamiarze wydania takiego zezwolenia.
2. Zezwolenie, o którym mowa w ustępie 1, udzielane będzie tylko osobom upoważnionym do dostępu do informacji niejawnych na podstawie prawa wewnętrznego tej Umawiającej się Strony, która wysyła te osoby.
3. Dane osobowe przybywających z wizytą do drugiej Umawiającej się Strony, w zakresie niezbędnym do uzyskania zezwolenia, o którym mowa w ustępie 1, zostaną przekazane z wyprzedzeniem 25 dni roboczych podmiotowi uprawnionemu lub właściwemu organowi bezpieczeństwa tej Umawiającej się Strony.
4. Podmioty upoważnione lub właściwe organy bezpieczeństwa obu Umawiających się Stron poinformują się wzajemnie o szczegółach zgłoszenia i zapewnią ochronę danych osobowych. Zgłoszenie zawierać będzie co najmniej następujące dane:
   a) imię i nazwisko, datę i miejsce urodzenia, narodowość, numer paszportu lub dowodu tożsamości zaproponowanej osoby odwiedzającej;
   b) stanowisko osoby odwiedzającej wraz z nazwą organu, przedsiębiorstwa albo organizacji, którą reprezentuje albo do której należy;

c) poziom posiadanego przez osobę odwiedzającą poświadczenia bezpieczeństwa;

d) nazwę i adres instytucji, przedsiębiorstwa albo organizacji, którą ma odwiedzić;

e) imię i nazwisko oraz stanowisko osoby (osób), którą (e) ma odwiedzić, jeśli są znane;

f) cel wizyty;

g) datę przybycia i wyjazdu.

ARTYKUŁ 11

NARUSZENIE ZASAD BEZPIECZEŃSTWA

1. W przypadku naruszenia zasad bezpieczeństwa, którego skutkiem jest ujawnienie lub zagrożenie ujawnienia informacji niejawnych otrzymanych od podmiotu uprawnionego lub właściwego organu bezpieczeństwa drugiej Umawiającej się Strony, właściwy organ bezpieczeństwa Umawiającej się Strony, na terytorium której ten wypadek miał miejsce, niezwłocznie poinformuje o tym właściwy organ bezpieczeństwa drugiej Umawiającej się Strony.
2. Naruszenia zasad bezpieczeństwa dotyczących wzajemnej ochrony informacji niejawnych będą wyjaśniane i ścigane zgodnie z prawem wewnętrznym tej Umawiającej się Strony, na terytorium której doszło do takiego naruszenia.
3. Właściwy organ bezpieczeństwa Umawiającej się Strony, na terytorium państwa której doszło do takiego naruszenia, niezwłocznie poinformuje właściwy organ bezpieczeństwa drugiej Umawiającej się Strony o rezultatach podjętych czynności, o których mowa w ustępie 2.

ARTYKUŁ 12

KOSZTY

Każda Umawiająca się Strona pokryje swoje wydatki wynikające z realizacji niniejszej Umowy.

ARTYKUŁ 13

KONSULTACJE

1. W celu osiągnięcia i utrzymania odpowiednich standardów bezpieczeństwa właściwe organy bezpieczeństwa Umawiających się Stron będą na bieżąco wzajemnie informować się o zmianach w swoim prawie wewnętrznym w zakresie ochrony informacji niejawnych, dotyczących postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy bezpieczeństwa Umawiających się Stron będą konsultować się na wniosek jednego z tych organów.
3. Każda z Umawiających się Stron zezwoli przedstawicielom właściwego organu bezpieczeństwa drugiej Umawiającej się Strony na składanie wizyt na swoim terytorium, w celu omówienia procedur służących ochronie informacji niejawnych, które zostały jej przekazane przez drugą Umawiającą się Stronę.

ARTYKUŁ 14

ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące interpretacji lub stosowania niniejszej Umowy będą rozstrzygane w drodze wzajemnych konsultacji między właściwymi organami bezpieczeństwa.

2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, będzie on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 15

POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa podlega przyjęciu zgodnie z prawem wewnętrznym każdej z Umawiających się Stron, co zostanie stwierdzone w drodze wymiany not dyplomatycznych. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.
2. Niniejsza Umowa zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze notyfikacji przez każdą z Umawiających się Stron. W takim przypadku niniejsza Umowa traci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
3. W przypadku wypowiedzenia, przekazane na podstawie niniejszej Umowy lub powstałe w wyniku wzajemnej współpracy Umawiających się Stron informacje niejawne, należy nadal chronić zgodnie z postanowieniami niniejszej Umowy tak długo, jak tego wymaga obowiązywanie klauzuli tajności.
4. Niniejsza Umowa może być zmieniona na podstawie pisemnego porozumienia Umawiających się Stron. Zmiany te wejdą w życie zgodnie z postanowieniami ustępu 1.

Sporządzono w Bukareszcie dnia 5 lipca 2006 roku w dwóch egzemplarzach, każdy w językach polskim, rumuńskim i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W razie rozbieżności przy ich interpretacji tekst w języku angielskim uważany będzie za rozstrzygający.

Z UPOWAŻNIENIA
RZĄDU RZECZYPOSPOLITEJ
POLSKIEJ

MAREK PASIONEK
Podsekretarz Stanu
w Kancelarii Prezesa
Rady Ministrów

Z UPOWAŻNIENIA
RZĄDU RUMUNII

Prof. dr MARIUS PETRESCU
Sekretarz Stanu
Dyrektor Generalny
Narodowego Urzędu Ochrony
Informacji Niejawnych

[ROMANIAN TEXT – TEXTE ROUMAIN]

ACORD

între

Guvernul Republicii Polonia

şi Guvernul României

privind protecţia reciprocă a Informaţiilor Clasificate

Guvernul Republicii Polonia şi Guvernul României,
denumite în continuare „Părţi Contractante",
Dezvoltând o cooperare bazată pe interese comune şi încredere
reciprocă, Intenţionând să asigure protecţia reciprocă a tuturor
informaţiilor
care au fost clasificate în conformitate cu legislaţia naţională
a fiecărei Părţi Contractante şi transmise celeilalte Părţi Contractante,
Au convenit următoarele:

ARTICOLUL 1

DEFINIȚII

În sensul prezentului Acord, următorii termeni se definesc astfel:

a) „**Informații Clasificate**" - orice informații care, indiferent de forma și modul lor de exprimare, sunt clasificate, chiar și pe parcursul elaborării lor, în conformitate cu legislația națională a fiecăreia dintre Părțile Contractante, deoarece necesită protecție împotriva dezvăluirii neautorizate;

b) „**Autoritate Competentă de Securitate**" – autoritate la nivel național cu atribuții în domeniul protecției Informațiilor Clasificate, prevăzută la articolul 3;

c) „**Instituție Autorizată**" – un organism sau o instituție cu atribuții în domeniul protecției Informațiilor Clasificate, prevăzută în legislațiile naționale ale Părților Contractante, autorizată să emită, să transmită, să primească, să stocheze, să protejeze și să utilizeze Informații Clasificate;

d) „**Contractant/Sub-contractant**" - o persoană fizică sau juridică ce intenționează să încheie sau este parte a unui Contract Clasificat;

e) „**Contract Clasificat**" – un acord între doi sau mai mulți Contractanți/Sub-contractanți prin care se stabilesc și se definesc între părți drepturi și obligații, care conține sau implică Informații Clasificate;

f) „**Contractant Principal**" – o instituție publică sau o altă persoană juridică ce intenționează să acorde sau acordă executarea unui Contract Clasificat pe teritoriul statului celeilalte Părți Contractante;

g) „**Terț**" – orice persoană, instituție, organizație națională sau internațională, persoană juridică de drept public sau privat ori un stat care nu este parte la prezentul Acord;

h) „**Certificat de Securitate a Personalului**" – document care atestă că posesorul acestuia poate avea acces la Informații Clasificate, în conformitate cu legislația

națională a Părții Contractante;

i) „**Certificat de Securitate Industrială**" – document emis de Autoritatea Competentă de Securitate care atestă faptul că un Contractant/Sub-contractant are capacitatea fizică și organizațională de a utiliza și stoca Informații Clasificate, în conformitate cu legislația națională a Părții Contractante;

j) „**Anexa de Securitate**" – document emis de Contractantul Principal ca parte a unui Contract Clasificat și care identifică cerințele de securitate sau acele elemente ale contractului ce necesită protecție;

k) „**Lista Clasificărilor de Securitate**" – document ce conține informații referitoare la aspectele care urmează a fi clasificate dintr-un Contract Clasificat și nivelurile de clasificare ce vor fi atribuite acestora.

ARTICOLUL 2

CLASIFICĂRI DE SECURITATE

Părțile Contractante convin că următoarele niveluri de clasificare de securitate sunt echivalente:

ÎN REPUBLICA POLONIA	ÎN ROMÂNIA	ECHIVALENT ÎN LIMBA ENGLEZĂ
ŚCIŚLE TAJNE	STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TOP SECRET
TAJNE	STRICT SECRET	SECRET
POUFNE	SECRET	CONFIDENTIAL
ZASTRZEŻONE	SECRET DE SERVICIU	RESTRICTED

ARTICOLUL 3

AUTORITATEA COMPETENTĂ DE SECURITATE

1. În sensul prezentului Acord, Autoritatea Competentă de Securitate va fi:
   - pentru Republica Polonia: Şeful Agenţiei de Securitate Internă – în domeniul civil şi Şeful Serviciilor de Informaţii Militare – în domeniul militar;
   - pentru România: Oficiul Registrului Naţional al Informaţiilor Secrete de Stat.
2. În vederea realizării şi păstrării unor standarde de securitate echivalente, Autorităţile Competente de Securitate ale Părţilor Contractante se vor informa reciproc în privinţa standardelor de securitate adoptate, a procedurilor şi practicilor aplicabile pentru protecţia Informaţiilor Clasificate.
3. La cerere şi ţinând cont de legislaţiile lor naţionale, Autorităţile Competente de Securitate îşi vor acorda asistenţă reciprocă în procedurile de verificare de securitate pentru eliberarea Certificatului de Securitate a Personalului şi a Certificatului de Securitate Industrială.
4. Autorităţile Competente de Securitate pot încheia acorduri în vederea implementării prezentelor dispoziţii.

ARTICOLUL 4

PROTECŢIA INFORMAŢIILOR CLASIFICATE

1. În conformitate cu prezentul Acord şi cu legislaţiile lor naţionale, Părţile Contractante vor adopta măsurile corespunzătoare pentru protecţia Informaţiilor Clasificate transmise sau emise ca rezultat al cooperării reciproce.
2. Pentru informaţiile prevăzute la alin. (1), Părţile Contractante vor asigura cel puţin aceeaşi protecţie ca şi propriilor Informaţii Clasificate, corespunzător

nivelului de clasificare a acestora, în conformitate cu articolul 2.

3. Informațiile Clasificate vor fi folosite exclusiv în scopul pentru care au fost transmise sau emise.

4. Partea Contractantă care a primit informațiile menționate la alin. (1) nu le va transmite unui Terț fără acordul prealabil scris al Părții Contractante emitente.

5. În conformitate cu prevederile alin. (4), când Partea Contractantă primitoare transmite unui Terț Informațiile Clasificate ale Părții Contractante emitente, Partea Contractantă primitoare va aduce la cunoştința Părții Contractante Emitente orice incident de securitate apărut pe teritoriul Terțului.

6. Accesul la Informațiile Clasificate transmise în baza prezentului Acord va fi permis numai acelor persoane care au „necesitatea de a cunoaşte", au fost verificate şi autorizate pentru accesul la astfel de informații, în conformitate cu legislația națională a Părții Contractante.

7. Partea Contractantă emitentă este exclusiv autorizată să modifice nivelul de clasificare de securitate sau să declasifice Informațiile Clasificate transmise. Autoritățile Competente de Securitate şi Instituțiile Autorizate ale Părților Contractante se vor informa reciproc cu privire la orice modificare adusă nivelului de clasificare de securitate sau la declasificarea informațiilor transmise.

8. Atribuirea sau schimbarea nivelului de clasificare de securitate a Informațiilor Clasificate elaborate în comun, ori declasificarea acestora se va realiza cu acordul Autorităților Competente de Securitate şi al Instituțiilor Autorizate ale Părților Contractante.

9. Dacă una dintre Părțile Contractante decide că transmiterea Informațiilor Clasificate sau implementarea unui proiect comun ar putea periclita suveranitatea statului acelei Părți Contractante, ar putea ameninta securitatea sau alte interese importante ale acestuia, ori ar putea aduce prejudicii sistemului juridic, aceasta poate refuza parțial sau total cooperarca ori o poate condiționa.

10. Autoritățile Competente de Securitate vor recunoaşte reciproc Certificatele de Securitate a Personalului şi Certificatele de Securitate Industrială emise în urma verificărilor de securitate desfăşurate în conformitate cu legislațiile naționale ale Părților Contractante, cu confirmarea prealabilă scrisă a Autorității Competente de Securitate referitoare la autenticitatea certificatelor. Autoritățile Competente de Securitate se vor informa reciproc, fără întârziere, asupra schimbărilor privind accesul la Informațiile Clasificate legate de aplicarea prezentului Acord.

ARTICOLUL 5

CONTRACTELE CLASIFICATE

1. Contractantul Principal poate încheia un Contract Clasificat cu Contractantul de pe teritoriul statului celeilalte Părți Contractante. În acest caz, Contractantul Principal trebuie să obțină, prin intermediul Autorității Competente de Securitate din statul său, o asigurare din partea Autorității Competente de Securitate a celeilalte Părți Contractante care să ateste faptul că respectivul Contractant este autorizat să aibă acces la Informații Clasificate de un anumit nivel de clasificare şi că:

   a) Contractantul deține Certificat de Securitate Industrială;

   b) Personalul Contractantului care prin funcții şi îndatoriri necesită acces la Informații Clasificate deține Certificat de Securitate a Personalului.

2. În cazul în care Contractantul nu întruneşte cerințele prevăzute la alin. (1), Autoritatea Competentă de Securitate care urmează să emită asigurarea va informa imediat Autoritatea Competentă de Securitate a celeilalte Părți Contractante asupra faptului că, la cererea acesteia din urmă, vor fi luate măsurile necesare pentru a i se emite Contractantului o autorizație de acces la Informații Clasificate.

3. Fiecare Contract Clasificat va fi însoțit de Anexa de Securitate și de Lista Clasificărilor de Securitate. Copii ale acestor documente vor fi transmise Autorității Competente de Securitate.

ARTICOLUL 6

MARCAREA INFORMAȚIILOR CLASIFICATE

1. Informațiile Clasificate primite de la cealaltă Parte Contractantă vor fi marcate cu nivelul de clasificare de securitate potrivit nivelului de clasificare corespunzător prevăzut la Articolul 2.
2. Copiile și traducerile Informațiilor Clasificate primite vor fi marcate și gestionate în același mod ca și originalele, cu respectarea prevederilor Articolului 8.
3. Cerințele menționate în alin. (1) și (2) se vor aplica și Informațiilor Clasificate emise în timpul executării unui Contract Clasificat.

ARTICOLUL 7

TRANSMITEREA INFORMAȚIILOR CLASIFICATE

1. Informațiile Clasificate vor fi transmise între Părțile Contractante prin canale diplomatice sau alte canale, convenite între Autoritățile Competente de Securitate ale Părților Contractante, pe baza unei confirmări scrise de primire, asigurându-se protecția împotriva dezvăluirii neautorizate.
2. Informațiile Clasificate pot fi transmise prin sistemele și rețelele IT protejate, autorizate spre utilizare în conformitate cu legislația națională a fiecărei Părți Contractante.

ARTICOLUL 8

MULTIPLICAREA ŞI TRADUCEREA INFORMAŢIILOR CLASIFICATE

1. Informaţiile Clasificate marcate cu nivelul de clasificare de securitate ŚCIŚLE TAJNE / STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ vor fi multiplicate numai cu acordul prealabil scris al Instituţiei Autorizate a Părţii Contractante emitente.
2. Toate Informaţiile Clasificate multiplicate vor fi protejate ca şi originalele. Numărul de copii va fi limitat la cel necesar scopurilor oficiale.
3. Toate traducerile Informaţiilor Clasificate se vor efectua de către persoane certificate din punct de vedere al securităţii. Toate traducerile vor fi însoţite de o notă, în limba în care au fost traduse, care să confirme că traducerile conţin Informaţii Clasificate ale Instituţiei Autorizate.

ARTICOLUL 9

DISTRUGEREA INFORMAŢIILOR CLASIFICATE

1. Informaţiile Clasificate vor fi distruse numai cu aprobarea scrisă sau la solicitarea Instituţiei Autorizate, ori a Autorităţii Competente de Securitate care a furnizat Informaţiile Clasificate, astfel încât reconstituirea, parţială sau integrală, a acestora să fie imposibilă. Instituţia Autorizată sau Autoritatea Competentă de Securitate care a furnizat Informaţiile Clasificate va fi informată despre distrugerea acestora.
2. Dacă Instituţia Autorizată sau Autoritatea Competentă de Securitate care a furnizat Informaţiile Clasificate nu este de acord cu distrugerea acestora, Informaţiile Clasificate respective îi vor fi returnate.

3. Informațiile Clasificate marcate ȘCIȘLE TAJNE / STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ nu se vor distruge. Ele vor fi returnate Instituției Autorizate sau Autorității Competente de Securitate care le-a furnizat.

ARTICOLUL 10

VIZITE

1. Persoanelor din statul unei Părți Contractante care vizitează statul celeilalte Părți Contractante li se va permite accesul la Informații Clasificate de un anumit nivel, precum și în incintele unde sunt gestionate astfel de Informații Clasificate, numai după primirea permisiunii scrise emise de Autoritatea Competentă de Securitate sau de Instituția Autorizată a celeilalte Părți Contractante. Instituția Autorizată va informa Autoritatea Competentă de Securitate despre intenția sa de a emite o astfel de permisiune.
2. Permisiunea menționată la alin. (1) se va acorda exclusiv persoanelor autorizate să aibă acces la Informații Clasificate, în conformitate cu legislația națională a Părții Contractante care deleagă aceste persoane.
3. Dacă este necesară obținerea permisiunii prevăzute la alin. (1), datele personale ale celor care vizitează cealaltă Parte Contractantă vor fi transmise Instituției Autorizate sau Autorității Competente de Securitate a respectivei Părți Contractante cu 25 de zile lucrătoare înaintea vizitei.
4. Instituțiile Autorizate sau Autoritățile Competente de Securitate ale Părților Contractante se vor informa reciproc asupra conținutului cererilor de vizită și vor asigura protecția datelor personale. Cererea va cuprinde cel puțin următoarele:
    a) numele vizitatorului propus, data și locul nașterii, naționalitatea, numărul pașaportului/cărții de identitate;

b) funcția vizitatorului și numele instituției, companiei sau organizației pe care o reprezintă sau din care face parte;
c) confirmarea nivelului certificatului de securitate al vizitatorului;
d) denumirea și adresa instituției, companiei sau organizației ce urmează a fi vizitată;
e) numele și funcția persoanei/persoanelor ce urmează a fi vizitate, dacă sunt cunoscute;
f) scopul vizitei;
g) data sosirii și cea a plecării.

ARTICOLUL 11

ÎNCĂLCAREA REGLEMENTĂRILOR DE SECURITATE

1. În cazul încălcării reglementărilor de securitate, al cărei rezultat este dezvăluirea sau amenințarea cu dezvăluirea Informațiilor Clasificate primite de la Instituția Autorizată sau de la Autoritatea Competentă de Securitate a celeilalte Părți Contractante, Autoritatea Competentă de Securitate a Părții Contractante pe al cărei teritoriu a avut loc un astfel de eveniment va informa imediat despre aceasta Autoritatea Competentă de Securitate a celeilalte Părți Contractante.
2. Încălcarea reglementărilor de securitate privind protecția reciprocă a Informațiilor Clasificate va fi investigată și sancționată în conformitate cu legislația națională a Părții Contractante pe al cărei teritoriu s-a produs incidentul.
3. Autoritatea Competentă de Securitate a Părții Contractante pe teritoriul statului căreia s-a produs incidentul va înștiința imediat Autoritatea Competentă de Securitate a celeilalte Părți Contractante asupra rezultatului acțiunilor menționate la alin. (2).

ARTICOLUL 12

CHELTUIELI

Fiecare Parte Contractantă va suporta cheltuielile proprii rezultate din aplicarea prezentului Acord.

ARTICOLUL 13

CONSULTĂRI

1. În vederea realizării şi menţinerii unor standarde de securitate similare, Autorităţile Competente de Securitate ale Părţilor Contractante se vor informa periodic asupra oricăror modificări ale legislaţiilor lor naţionale referitoare la protecţia Informaţiilor Clasificate la care se face referire în prezentul Acord.
2. La solicitarea uneia dintre Autorităţile Competente de Securitate ale Părţilor Contractante, se vor realiza consultări reciproce, în vederea asigurării unei strânse cooperări pentru implementarea prevederilor prezentului Acord.
3. Fiecare Parte Contractantă va permite reprezentanţilor Autorităţii Competente de Securitate a celeilalte Părţi Contractante să efectueze vizite pe teritoriul său în vederea discutării procedurilor referitoare la protecţia Informaţiilor Clasificate transmise de către cealaltă Parte Contractantă.

ARTICOLUL 14

SOLUŢIONAREA DIFERENDELOR

1. Orice diferend referitor la interpretarea sau aplicarea prezentului Acord se va soluţiona prin consultări reciproce între Autorităţile Competente de Securitate.
2. Dacă diferendul nu se poate soluţiona conform prevederilor alin. (1),

soluționarea acestuia se va realiza pe canale diplomatice.

ARTICOLUL 15

DISPOZIȚII FINALE

1. Prezentul Acord intră în vigoare în prima zi a celei de-a doua luni după primirea ultimei notificări prin care Părțile Contractante se informează reciproc cu privire la îndeplinirea procedurilor legale interne necesare în acest scop.
2. Prezentul Acord se încheie pe o perioadă nedeterminată. Acesta poate fi denunțat de oricare dintre Părțile Contractante după notificarea celeilalte Părți Contractante. În acest caz, valabilitatea prezentului Acord va înceta după șase luni de la primirea notificării de denunțare.
3. În cazul încetării valabilității prezentului Acord, Informațiile Clasificate transmise în baza acestuia sau emise pe parcursul cooperării dintre Părțile Contractante vor continua să fie protejate în conformitate cu prevederile Acordului atât timp cât este necesar, potrivit nivelului clasificării de securitate.
4. Prezentul Acord poate fi amendat prin acordul scris al Părților Contractante. Amendamentele vor intra în vigoare conform dispozițiilor alin. (1).

Semnat la Bucureşti, la data 5 iulie 2006, în două exemplare originale, fiecare în limbile poloneză, română şi engleză, toate textele fiind egal autentice. În caz de diferenţe în interpretare, textul în limba engleză va prevala.

PENTRU
GUVERNUL REPUBLICII
POLONIA

MAREK PASIONEK
Subsecretar de Stat
în cadrul Cancelariei Primului-Ministru

PENTRU
GUVERNUL ROMÂNIEI

Prof. dr. MARIUS PETRESCU
Secretar de Stat
Directorul General
al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE DE POLOGNE ET LE GOUVERNEMENT DE LA ROUMANIE SUR LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

Le Gouvernement de la République de Pologne et le Gouvernement de la Roumanie, ci-après dénommés « les Parties contractantes »,

Établissant une coopération fondée sur l'intérêt et la confiance mutuels,

Soucieux de garantir la protection mutuelle de toutes les informations qui ont été classifiées conformément à la législation interne de l'une des Parties contractantes et transmises à l'autre Partie contractante,

Sont convenus de ce qui suit :

ARTICLE PREMIER.DÉFINITIONS

Les définitions ci-après sont applicables aux fins du présent Accord :

a) Le terme « information classifiée » désigne toute information qui, indépendamment de sa forme et de son mode d'expression, y compris pendant son élaboration, est classée selon la législation interne de chaque Partie contractante comme devant être protégée contre une divulgation non autorisée ;

b) Le terme « autorité de sécurité compétente » désigne une autorité étatique compétente pour la protection des informations classifiées, comme indiqué à l'article 3 ;

c) Le terme « entité autorisée » désigne un organisme ou une institution ayant des compétences dans le domaine de la protection des informations classifiées spécifiées dans les législations internes des Parties contractantes, autorisé à émettre, transmettre, recevoir, stocker, protéger et utiliser des informations classifiées ;

d) Le terme « contractant/sous-traitant » désigne une personne physique ou morale qui a l'intention de conclure ou qui est partie à un contrat classifié ;

e) Le terme « contrat classifié » désigne un accord souscrit entre deux ou plusieurs prestataires/sous-traitants qui crée et définit des droits et obligations contraignants entre eux et qui prévoit des dispositions pour l'utilisation d'informations classifiées ;

f) Le terme « entrepreneur principal » désigne un organisme public ou une entité juridique qui a l'intention d'accorder ou d'accorder l'exécution d'un contrat classifié sur le territoire de l'État de l'autre Partie contractante ;

g) Le terme « tierce partie » désigne toute personne, institution, organisation nationale et internationale, entité publique ou privée ou un État qui n'est pas partie au présent Accord ;

h) Le terme « habilitation de sécurité du personnel » désigne un document attestant que le titulaire peut avoir accès à des informations classifiées conformément à la législation interne de la Partie contractante ;

i) Le terme « habilitation de sécurité d'établissement » désigne un document délivré par l'autorité de sécurité compétente attestant que le contractant/sous-traitant dispose de la capacité physique et organisationnelle d'utiliser et de stocker des informations classifiées conformément à la législation interne de la Partie contractante ;

j) Le terme « lettre sur les aspects liés à la sécurité » désigne un document émis par l'entrepreneur principal concernant un contrat classifié, identifiant les exigences de sécurité ou les éléments du contrat nécessitant une protection ;

k) Le terme « liste de contrôle de la classification de sécurité » désigne une liste des informations liées aux différents aspects d'un contrat classifié qui doivent être classifiées selon un niveau de classification de sécurité spécifié.

ARTICLE 2. CLASSIFICATIONS DE SÉCURITÉ

Les Parties contractantes conviennent que les niveaux de classification de sécurité suivants sont équivalents :

République de Pologne	Roumanie	Équivalent français
ŚCIŚLE TAJNE	STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	TOP SECRET
TAJNE	STRICT SECRET	SECRET
POUFNE	SECRET	CONFIDENTIEL
ZASTRZEŻONE	SECRET DE SERVICIU	RESTREINT

ARTICLE 3. AUTORITÉ COMPÉTENTE EN MATIÈRE DE SÉCURITÉ

1. Aux fins du présent Accord, l'autorité compétente en matière de sécurité est :

— pour la République de Pologne : le chef de l'Agence de sécurité intérieure dans le domaine civil et le chef des Services d'information militaire dans le domaine militaire ;

— pour la Roumanie : le Bureau d'enregistrement des informations classifiées.

2. Afin d'élaborer des normes de sécurité comparables et de les maintenir, les autorités compétentes en matière de sécurité des Parties contractantes se communiquent des informations sur les normes, procédures et pratiques de sécurité adoptées en matière de protection des informations classifiées.

3. Les autorités compétentes en matière de sécurité se prêtent mutuellement assistance, sur demande et en tenant compte de leur législation interne, dans les procédures d'habilitation de

sécurité pour la délivrance de l'habilitation de sécurité du personnel et de l'habilitation de sécurité de l'établissement.

4. Les autorités compétentes en matière de sécurité peuvent conclure des accords aux fins de l'application des dispositions des présentes.

ARTICLE 4 PROTECTION DES INFORMATIONS CLASSIFIÉES

1. Conformément au présent Accord et à leur législation interne, les Parties contractantes adoptent les mesures appropriées pour protéger les informations classifiées qui sont transmises ou proviennent de leur coopération mutuelle.

2. Les Parties contractantes accordent aux informations visées au paragraphe 1 au moins la même protection que celle applicable à leurs propres informations classifiées au niveau de classification de sécurité équivalent, conformément à l'article 2.

3. Les informations classifiées ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été communiquées ou émises.

4. La Partie contractante qui a reçu les informations visées au paragraphe 1 ne les communique à aucun tiers, sans le consentement écrit préalable de la Partie contractante d'origine.

5. En vertu des dispositions du paragraphe 4, lorsque la Partie contractante destinataire transmet à une tierce partie des informations classifiées de la Partie contractante d'origine, la Partie contractante destinataire informe la Partie contractante d'origine de toute atteinte à la sécurité survenue sur le territoire de la tierce partie.

6. Les informations classifiées transmises en vertu des présentes ne sont accessibles qu'aux personnes qui ont besoin d'en connaître, qui ont fait l'objet d'une habilitation de sécurité et qui sont autorisées à avoir accès à ces informations conformément à la législation interne de la Partie contractante.

7. La Partie contractante d'origine est exclusivement autorisée à modifier le niveau de classification de sécurité ou à déclassifier les informations classifiées transmises. Les autorités compétentes en matière de sécurité et les entités autorisées des Parties contractantes s'informent mutuellement de toute modification des niveaux de classification de sécurité ou de la déclassification des informations transmises.

8. L'attribution d'un niveau de classification de sécurité à des informations classifiées créées conjointement, leur modification ou leur déclassification se font d'un commun accord entre les autorités compétentes en matière de sécurité et les entités autorisées des Parties contractantes.

9. Si l'une des Parties contractantes décide que la transmission d'informations classifiées ou la mise en œuvre d'une entreprise commune pourrait compromettre la souveraineté de l'État de cette Partie contractante, menacer sa sécurité ou d'autres intérêts importants, ou pourrait causer des dommages au système juridique, elle peut refuser partiellement ou totalement la coopération ou la faire dépendre de certaines conditions.

10. Les autorités compétentes en matière de sécurité reconnaissent mutuellement l'habilitation de sécurité du personnel et l'habilitation de sécurité de l'établissement délivrées à l'issue de la procédure d'habilitation de sécurité menée conformément à leurs législations internes, après confirmation écrite préalable de leur authenticité par l'autorité compétente en matière de sécurité. Les autorités compétentes en matière de sécurité s'informent mutuellement et sans délai

des modifications de l'accès aux informations classifiées liées à la mise en œuvre du présent Accord.

ARTICLE 5. CONTRATS CLASSIFIÉS

1. L'entrepreneur principal peut conclure un contrat classifié avec le contractant situé sur le territoire de l'État de l'autre Partie contractante. Dans ce cas, l'entrepreneur principal doit obtenir, par l'intermédiaire de son autorité compétente en matière de sécurité, l'assurance de l'autorité compétente en matière de sécurité de l'autre Partie contractante que le contractant est autorisé à avoir accès aux informations classifiées du niveau de classification de sécurité spécifié et que :

a) le contractant a obtenu l'habilitation de sécurité de l'établissement ;

b) tous les membres du personnel du contractant dont les postes et les fonctions nécessitent l'accès à des informations classifiées ont reçu l'habilitation de sécurité du personnel.

2. Si le contractant ne satisfait pas aux exigences visées au paragraphe 1, l'autorité compétente en matière de sécurité qui doit délivrer l'assurance informe immédiatement l'autorité compétente en matière de sécurité de l'autre Partie contractante que, à sa demande, les mesures nécessaires seront prises pour délivrer au contractant une autorisation d'accès aux informations classifiées.

3. Chaque contrat classifié doit être accompagné de la lettre relative aux aspects de sécurité et de la liste de contrôle de la classification de sécurité. Des copies de ces documents doivent être soumises à l'autorité compétente en matière de sécurité.

ARTICLE 6. MARQUAGE DES INFORMATIONS CLASSIFIÉES

1. Les informations classifiées reçues de l'autre Partie contractante sont marquées d'un niveau de classification de sécurité, conformément au niveau de classification correspondant stipulé à l'article 2.

2. Les copies et les traductions des informations classifiées reçues sont marquées et traitées de la même manière que les originaux, dans le respect des dispositions de l'article 8.

3. Les exigences visées aux paragraphes 1 et 2 s'appliquent également aux informations classifiées provenant de l'exécution d'un contrat classifié.

ARTICLE 7 TRANSMISSION DES INFORMATIONS CLASSIFIÉES

1. Les informations classifiées sont transmises entre les Parties contractantes, suivies d'un accusé de réception écrit, par la voie diplomatique ou par d'autres voies, garantissant la protection contre toute divulgation non autorisée, convenues par les autorités compétentes en matière de sécurité des deux Parties contractantes.

2. Les informations classifiées peuvent être transmises par l'intermédiaire de systèmes et de réseaux informatiques protégés dont l'utilisation a été autorisée conformément à la législation interne de l'une ou l'autre des Parties contractantes.

ARTICLE 8. REPRODUCTION ET TRADUCTION D'INFORMATIONS CLASSIFIÉES

1. Les informations classifiées marquées du niveau de classification de sécurité SCISLE TAJNE/STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ ne peuvent être reproduites qu'avec une autorisation écrite préalable délivrée par l'entité autorisée de la Partie contractante d'origine.

2. Toute reproduction d'informations classifiées bénéficie du même niveau de protection que les originaux. Le nombre d'exemplaires se limite à ceux qui sont requis à des fins officielles.

3. Toutes les traductions d'informations classifiées doivent être effectuées par des personnes ayant une habilitation de sécurité appropriée. Les traductions contiennent une annotation appropriée rédigée dans leur langue d'arrivée, indiquant que les traductions contiennent des informations classifiées de l'entité autorisée.

ARTICLE 9. DESTRUCTION D'INFORMATIONS CLASSIFIÉES

1. Les informations classifiées ne seront détruites qu'avec une autorisation écrite ou à la demande de l'entité autorisée ou de l'autorité compétente en matière de sécurité qui a fourni les informations classifiées, de manière à empêcher leur reconstitution partielle ou totale. L'entité autorisée ou l'autorité compétente en matière de sécurité qui a fourni les informations classifiées est informée de leur destruction.

2. Si l'entité autorisée ou l'autorité compétente en matière de sécurité qui a fourni les informations classifiées ne consent pas à leur destruction, ces informations classifiées lui seront restituées.

3. Les informations classifiées marquées SCISLE TAJNE/STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ ne sont pas détruites. Elles sont renvoyées à l'entité autorisée ou à l'autorité compétente en matière de sécurité qui les a fournies.

ARTICLE 10. VISITES

1. Les personnes arrivant en visite de l'une des Parties contractantes sur le territoire de l'État de l'autre Partie contractante ne sont autorisées à accéder aux informations classifiées dans la mesure nécessaire ainsi qu'aux locaux où ces informations classifiées sont traitées qu'après réception préalable d'une autorisation écrite délivrée par l'autorité compétente en matière de sécurité ou l'entité autorisée de l'autre Partie contractante. L'entité autorisée informe l'autorité de sécurité compétente de son intention de délivrer ce permis.

2. L'autorisation visée au paragraphe 1 est accordée exclusivement aux personnes autorisées à avoir accès aux informations classifiées en vertu de la législation interne de la Partie contractante qui les délègue.

3. Dans la mesure où cela est nécessaire pour obtenir l'autorisation visée au paragraphe 1, les données à caractère personnel des personnes se rendant en visite dans l'autre Partie contractante sont transférées 25 jours ouvrables à l'avance à l'entité autorisée ou à l'autorité compétente en matière de sécurité de cette partie contractante.

4. Les entités autorisées ou les autorités compétentes en matière de sécurité des deux Parties contractantes s'informent mutuellement des détails d'une demande de visite et assurent la protection des données à caractère personnel. La demande doit contenir au moins les éléments suivants :

a) le nom du visiteur proposé, date et lieu de naissance, nationalité, numéro de passeport/carte d'identité ;
b) le statut officiel du visiteur ainsi que le nom de l'établissement, de la société ou de l'organisation qu'il représente ou à laquelle il appartient ;
c) la certification du niveau d'habilitation de sécurité du visiteur ;
d) le nom et l'adresse de l'établissement, de l'entreprise ou de l'organisation à visiter ;
e) le nom et le statut de la ou des personnes à visiter, s'ils sont connus ;
f) l'objet de la visite ;
g) les dates d'arrivée et de départ.

ARTICLE 11 VIOLATION DES RÈGLES DE SÉCURITÉ

1. En cas de violation des règles de sécurité entraînant la divulgation ou la menace de divulgation d'informations classifiées reçues de l'entité autorisée ou de l'autorité compétente en matière de sécurité de l'autre Partie contractante, l'autorité compétente en matière de sécurité de la Partie contractante sur le territoire de laquelle l'événement s'est produit en informe immédiatement l'autorité compétente en matière de sécurité de l'autre Partie contractante.

2. Les violations des dispositions relatives à la protection mutuelle des informations font l'objet d'enquêtes et de poursuites conformément à la législation nationale de la Partie sur le territoire national de laquelle la violation s'est produite.

3. L'autorité compétente en matière de sécurité de la Partie contractante sur le territoire national de laquelle la violation s'est produite informe immédiatement l'autorité compétente en matière de sécurité de l'autre Partie contractante du résultat des actions visées au paragraphe 2.

ARTICLE 12. FRAIS

Chaque Partie prend en charge les dépenses qu'elle a engagées dans le cadre de la mise en œuvre du présent Accord.

ARTICLE 13. CONSULTATIONS

1. Afin d'atteindre et de maintenir des normes de sécurité comparables, les autorités compétentes en matière de sécurité des Parties contractantes s'informent mutuellement de toute modification de leur législation interne concernant la protection des informations classifiées liées au présent Accord.

2. Les autorités de sécurité compétentes des Parties se consultent, à la demande de l'une d'entre elles, en vue de garantir une étroite collaboration dans la mise en application des dispositions du présent Accord.

3. Chaque Partie autorise les représentants de l'autorité compétente en matière de sécurité de l'autre Partie à se rendre sur son propre territoire pour discuter des procédures de protection des informations classifiées transmises par l'autre Partie.

ARTICLE 14. RÈGLEMENT DES DIFFÉRENDS

1. Tout différend concernant l'interprétation ou l'application du présent Accord est réglé exclusivement par voie de consultations entre les Parties contractantes.

2. Si le règlement d'un différend ne peut être obtenu de la manière visée au paragraphe 1, ce différend est réglé par la voie diplomatique.

ARTICLE 15. DISPOSITIONS FINALES

1. Le présent Accord entre en vigueur le premier jour du deuxième mois suivant la réception de la dernière des notifications par lesquelles les Parties contractantes s'informent mutuellement de l'accomplissement des procédures juridiques internes nécessaires à cet égard.

2. Le présent Accord est conclu pour une durée indéterminée. Il peut être dénoncé par l'une ou l'autre des Parties contractantes sur notification à l'autre Partie contractante. Dans ce cas, le présent Accord cesse d'être en vigueur six mois après la réception de l'avis de dénonciation.

3. En cas de résiliation du présent Accord, les informations classifiées transmises en vertu du présent Accord ou provenant de la coopération mutuelle des Parties contractantes continuent d'être protégées conformément aux dispositions du présent Accord aussi longtemps que le niveau de classification de sécurité l'exige.

4. Le présent Accord peut être modifié avec le consentement écrit mutuel des deux Parties contractantes. Les modifications entrent en vigueur conformément aux dispositions prévues au paragraphe 1.

FAIT à Bucarest le 5 juillet 2006 en deux exemplaires originaux, chacun en langues polonaise, roumaine et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, le texte anglais prévaut.

Pour le Gouvernement de la République de Pologne :

MAREK PASIONEK

Sous-secrétaire d'État à la Chancellerie du Premier ministre

Pour le Gouvernement de la Roumanie :

MARIUS PETRESCU

Secrétaire d'État Directeur général du Bureau d'enregistrement des informations classifiées