LAW No. 282 of 10 July 2009
on the ratification of the Security Agreement between Romania and the Portuguese Republic on the Mutual Protection of Classified Information, signed in Bucharest on 14 May 2008

ISSUER: The PARLIAMENT
PUBLISHED IN: The Official Journal no. 518 of 28 July 2009

The Parliament of Romania adopts this law.

SINGLE ARTICLE
The Security Agreement between Romania and the Portuguese Republic on the Mutual Protection of Classified Information, signed in Bucharest on 14 May 2008 is ratified.

This law was adopted by the Parliament of Romania, with the observance of the provisions of Article 75 and Article 76 paragraph (2) of the Constitution of Romania, republished.

PRESIDENT OF THE CHAMBER OF DEPUTIES
ROBERTA ALMA ANASTASE

p. PRESIDENT OF THE SENATE
ALEXANDRU PERES

Bucharest, 10 July 2009
No. 282

SECURITY AGREEMENT BETWEEN ROMANIA AND THE PORTUGUESE REPUBLIC ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

Romania and the Portuguese Republic,

Hereinafter called the Parties,

Considering the need to safeguard the Classified Information exchanged between them through their state bodies or other legal public and private entities which deal with Classified Information of the other Party;

Desiring to create a set of rules on the mutual protection of Classified Information exchanged between the Parties,

Have agreed as follows:

ARTICLE 1
OBJECT

This Security Agreement, hereinafter referred to as Agreement, establishes the security rules applicable to all co-operation arrangements or contracts, which envisage the exchange of Classified Information, concluded or to be concluded between state bodies or other legal public and private entities of the Parties, duly authorized to that purpose.

ARTICLE 2
SCOPE OF APPLICATION

1. This Agreement forms the legal basis of any activity, involving the exchange of Classified Information between the Parties, concerning cases such as:

- co-operation between the Parties concerning the national defense and any other issue related to national security;

- co-operation, joint ventures, contracts or any other relation between state bodies or other public or private entities of the Parties in the field of national defense and any other issue related to national security;

- sales of equipment, products and know-how.

2. Either Party may not invoke this Agreement in order to obtain Classified Information that the other Party has received from a Third Party.

ARTICLE 3
DEFINITIONS

For the purpose of this Agreement:

Classified Information means any information, document or material, regardless of its physical form, to which a particular Security Classification has been assigned in compliance with the respective Law in force and which shall be protected accordingly;

Classified Document means any sort of record containing Classified Information regardless of its form or physical characteristics, including, without limitation, written or printed matters, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions produced by any means or processes, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable automated data processing equipment with resident computer storage media, and removable computer storage media;

Classified Material means any object or item of machinery, prototype, equipment, weapon, or similar, mechanically or hand made, manufactured or in process of manufacture, to which a Security Classification has been assigned;

Security Classification means the assignment of a class or level of classification in accordance with the respective Law in force of the Parties;

Classified Contract means an arrangement between two or more contractors establishing and defining their rights and obligations and containing or implying access to Classified Information;

Contractor or Sub-Contractor means an individual or legal entity possessing the legal capacity to conclude Classified Contracts;

Breach of Security means an act or an omission contrary to the respective Law in force of the Parties that result in an actual or possible Compromise of Classified Information;

Compromise of Classified Information means a situation when, due to a Breach of Security or adverse activity, Classified Information has lost its confidentiality, integrity or availability, or when supporting services and resources have lost their integrity or availability, including loss, partial or total disclosure, unauthorized modification and destruction or denial of service;

Security Aspects Letter means a document issued by the appropriate authority as a part of any Classified Contract or sub-contract, identifying the security requirements or those elements of the contract requiring security protection;

Security Classification Check-List means a listing of Classified Information, materials and activities related to a Classified Contract and their Security Classification, included in the Security Aspects Letter;

Personnel Security Clearance Certificate means a document certifying that the holder may have access to Classified Information of a certain Security Classification, in compliance with the Need-to-Know principle;

Facility Security Clearance Certificate means a document certifying that a legal body is authorized to carry out industrial activities requiring access to Classified Information of a certain Security Classification;

Need-to-Know means a principle by which access to Classified Information may be granted individually, only to those persons who, in performing their duties, need to work with or have access to such information;

Competent Security Authority means the institution empowered with authority at national level which, in compliance with the respective Law in force of the Parties, ensures the unitary implementation of the protective measures for Classified Information;

Designated Security Authority means the institution which, in compliance with the respective Law in force of the Parties, coordinated by the Competent Security Authority in the field of the protection of Classified Information, is empowered to establish, for its activity field and according to its competences, its own structures and measures;

Originating Party means the Party which transmits Classified Information to the other Party;

Receiving Party means the Party that receives the Classified Information transmitted to it by the Originating Party;

Third Party means any international organization or state that is not a Party to this Agreement.

ARTICLE 4
COMPETENT SECURITY AUTHORITIES

The Competent Security Authorities responsible, at national level, for the implementation and the control of the measures stipulated in this Agreement are:

For Romania: Guvernul României Oficiul Registrului Naţional al Informaţiilor Secrete de Stat Bucureşti – Str. Mureş nr. 4, Sect.1 ROMÂNIA	For the Portuguese Republic: Autoridade Nacional de Segurança Presidência do Conselho de Ministros Rua da Junqueira, 69 1300-342 Lisboa PORTUGAL

2. In order to keep the same security standards, each Competent Security Authority shall provide, upon request, to the other Competent Security Authority, information about its security organization, procedures and the respective Law in force regulating the protection of Classified Information.

3. In order to ensure close co-operation in the implementation of this Agreement, Competent Security Authorities may assist each other and may hold consultations on the request made by one of them.

ARTICLE 5
EQUIVALENCE OF THE SECURITY CLASSIFICATIONS

The Parties agree that the equivalence of their national Security Classifications is the following:

Romania	Portuguese Republic	English Equivalent
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	MUITO SECRETO	TOP SECRET
STRICT SECRET	SECRETO	SECRET
SECRET	CONFIDENCIAL	CONFIDENTIAL
SECRET DE SERVICIU	RESERVADO	RESTRICTED

ARTICLE 6
PROTECTION OF CLASSIFIED INFORMATION

1. The protection and use of the Classified Information exchanged between the Parties are regulated by the following rules:

a) the Receiving Party shall ensure to all the exchanged, received, produced or developed Classified Information the same protection as it is provided for its own Classified Information with the equivalent Security Classification;

b) the access to Classified Information shall be restricted to persons who, in order to perform their functions, need to have access to the Classified Information on a Need-to-Know basis and hold appropriate Personnel Security Clearance Certificates for access to information classified SECRET / CONFIDENCIAL / CONFIDENTIAL or above;

c) representatives of a Party have access to information classified SECRET DE SERVICIU / RESERVADO / RESTRICTED of the other Party on a Need-to-Know basis, provided they meet the requirements for access to such Classified Information according to the Law in force of the Party they represent.

2. The Receiving Party shall mark the received Classified Information with its own equivalent Security Classification marking, in accordance with the equivalences referred to in Article 5 of this Agreement.

3. The Originating Party shall inform the Receiving Party of any changes in Security Classification of the transmitted Classified Information.

4. The Receiving Party shall neither downgrade nor declassify the received Classified Information without the prior written consent of the Originating Party.

5. Translations and reproductions of Classified Information shall be made according to the following procedures:

a) the individuals shall hold the appropriate Personnel Security Clearance Certificates;
b) the translations and the reproductions shall be marked and placed under the same protection as the original Classified Information;
c) the translations and the number of reproductions shall be limited to that required for official purposes;
d) the translations shall bear an appropriate note in the language into which it is translated indicating that it contains Classified Information received from the Originating Party.

6. Classified Information marked as STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ / MUITO SECRETO / TOP SECRET shall be translated or reproduced only upon the written permission of the Competent Security Authority of the Originating Party, in accordance with the respective Law in force.

7. Classified Information marked as STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/ MUITO SECRETO / TOP SECRET shall not be destroyed and it shall be returned to the Originating Party.

8. For the destruction of Classified Information marked as STRICT SECRET / SECRETO / SECRET and SECRET / CONFIDENCIAL/ CONFIDENTIAL prior written consent of the Originating Party is required.

9. In case of a situation that makes it impossible to protect and return Classified Information generated or transmitted according to this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Originating Party about the destruction of the Classified Information as soon as possible.

ARTICLE 7
TRANSMISSION OF CLASSIFIED INFORMATION

Classified Information shall be transmitted by diplomatic channels, military couriers or other means approved by the Competent Security Authorities.

If a large consignment containing Classified Information is to be transmitted, the Competent Security Authorities shall mutually agree on the means of transportation, the route and security measures for each case.

The exchange of Classified Information through protected information and communication systems shall take place in accordance with the security procedures mutually agreed on by the Competent Security Authorities of the Parties.

The Receiving Party shall confirm in writing the receipt of the Classified Information.

ARTICLE 8
RELEASE OF INFORMATION

Release of Classified Information to Third Parties or to any public and private entity which holds the nationality of a third state can take place after written consent of the Competent Security Authority of the Originating Party, which may impose further limitations to the release.

Each Party shall ensure that Classified Information received from the other Party is used for the purpose for which such information has been released.

ARTICLE 9
SECURITY CLEARANCE PROCEDURES

1. Each Party shall recognize the Personnel Security Clearance Certificates and Facility Security Clearance Certificates issued in accordance with the Law in force of the other Party.

2. The Competent Security Authorities shall inform each other about any modifications regarding the Personnel Security Clearance Certificates and Facility Security Clearance Certificates.

3. On request, the Competent Security Authorities of the Parties, taking into account their respective Law in force, shall assist each other during the clearance procedures of their nationals living or facilities located in the territory of the other Party, preceding the issue of the Personnel Security Clearance Certificates and the Facility Security Clearance Certificates.

ARTICLE 10
CLASSIFIED CONTRACTS

1. In case of Classified Contracts to be concluded and implemented in the territory of one of the Parties, the Competent Security Authority of the other

Party shall obtain prior written assurance that the proposed Contractor holds a Facility Security Clearance Certificate of an appropriate level.

2. The Contractor commits itself to:
a) ensure that its premises have adequate conditions for the processing of Classified Information;
b) have an appropriate Facility Security Clearance Certificate granted to those premises;
c) have appropriate Personnel Security Clearance Certificates granted to persons who perform functions that require access to Classified Information;
d) ensure that all persons having access to Classified Information are informed of their responsibility towards the protection of Classified Information, according to the Law in force;
e) allow security inspections of its premises by representatives of the Competent Security Authorities.

3. Any Sub-Contractor must fulfill the same security obligations as the Contractor.

4. The Competent Security Authority shall be responsible for the supervision and control of the compliance of the Contractor with the commitments set in paragraph 2 of this Article.

5. Every Classified Contract concluded between Contractors of the Parties, under the provisions of this Agreement, shall include an appropriate Security Aspects Letter identifying at least the following aspects:

a) security Classification Check-List;

b) procedure for the communication of changes in the Security Classification;

c) communication channels and means for electromagnetic transmission;

d) procedure for the transportation of Classified Information;

e) authorities competent for the co-ordination of the safeguarding of Classified Information related to the Contract;

f) an obligation to notify any actual or suspected Compromise of Classified Information.

6. A copy of the Security Aspects Letter of any Classified Contract shall be forwarded to the Competent Security Authority of the Party where the

Classified Contract is to be performed in order to allow adequate security supervision and control.

7. The Competent Security Authorities may agree on mutual visits in order to analyze the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract. Notice of the visit shall be provided at least twenty working days in advance.

ARTICLE 11
VISITS

1. Visits entailing access to Classified Information by nationals from one Party to the other Party are subject to prior written authorization given by the Competent Security Authorities or Designated Security Authorities according to the respective Law in force.

2. The request for visit shall be submitted through the Competent Security Authority of the host Party.

3. Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party only if they:

-hold appropriate Personnel Security Clearance Certificates; and
-have been authorized to receive or to have access to Classified Information on a Need-to-Know basis, in accordance with the respective Law in force.

4. The Competent Security Authority of the Party requesting the visit shall notify the Competent Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least twenty working days in advance.

5. In urgent cases, the request for visit shall be transmitted at least five working days in advance.

6. The Competent Security Authority of the Party that receives the request for visit shall inform, in due time, the Competent Security Authority of the requesting Party about the decision.

7. Visits of individuals from a Third Party entailing access to Classified Information of the Originating Party shall only be authorized by a written consent given by the Competent Security Authority or Designated Security Authority in accordance with the respective Law in force.

8. Once the visit has been approved, the Competent Security Authority or Designated Security Authority of the host Party shall provide a copy of the request for visit to the security officer of the establishment, facility or organization to be visited.

9. The validity of the visit authorization shall not exceed twelve months.

10. For any Classified Contract the Parties may agree to establish lists of authorized persons to make recurring visits. Those lists are valid for an initial period of twelve months.

11. Once those lists have been approved by the Parties, further details of the specific visits shall be directly arranged between the appropriate representatives of the entities involved, according to the terms and conditions agreed upon.

12. The request for visit shall include:
a) visitor's first and last name, place and date of birth, nationality, passport or identification card number;

b) name of the establishment, facility or organization the visitor represents or belongs to;

c) name and address of the establishment, facility or organization to be visited;

d) confirmation of the visitor's Personnel Security Clearance Certificate and its validity;

e) object and purpose of the visit or visits;

f) expected date and duration of the requested visit or visits, and in case of recurring visits, the total period covered by the visits should be stated;

g) name and phone number of the point of contact at the establishment, facility or organization to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;

h) The date, signature and stamping of the official seal of the Competent Security Authority or of the appropriate Designated Security Authority.

ARTICLE 12
BREACH OF SECURITY

1. In case of Breach of Security related with Classified Information originated by or received from the other Party, the Competent Security Authority of the Party where the Breach of Security has occurred shall inform the Competent Security Authority of the other Party, as soon as possible, and ensure the appropriate investigation.

2. If a Breach of Security occurs in a third state, the Competent Security Authority of the dispatching Party shall take the actions stipulated in paragraph 1 of the present Article.

3. The other Party shall, if required, co-operate in the investigation.

In any case, the other Party shall be informed, in writing, of the results and the conclusions of the investigation, including the reasons for the Breach of Security, the extent of the damage and the respective measures taken to limit it.

ARTICLE 13
EXPENSES

Each Party shall bear its own expenses incurred in connection with the application and supervision of all aspects of this Agreement.

ARTICLE 14
SETTLEMENT OF DISPUTES

Any dispute concerning the interpretation or application of this Agreement, if not settled by consultations between the Competent Security Authorities, shall be settled by negotiations through diplomatic channels.

ARTICLE 15
ENTRY INTO FORCE

This Agreement shall enter into force on the thirtieth day following the receipt of the last of the notifications, in writing and through diplomatic channels, stating that all the internal legal procedures of both Parties have been fulfilled.

ARTICLE 16
AMENDMENTS

Both Parties may amend this Agreement on the basis of mutual written consent.
The amendments shall enter into force in accordance with the terms specified in Article 15 of this Agreement.

ARTICLE 17
DURATION AND TERMINATION

1. This Agreement shall remain in force for an indefinite period of time.

2. Each Party may, at any time, terminate this Agreement.

3. The termination shall be notified, in writing and through diplomatic channels, and shall become effective six months after the date of receipt of the respective notification.

4. Notwithstanding the termination, all Classified Information received pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

ARTICLE 18
REGISTRATION

After the entry into force of this Agreement, the Party in whose territory it was signed shall transmit it for registration to the Secretariat of the United Nations, according to article 102 of the Charter of the United Nations, and shall notify the other Party of the conclusion of this proceeding, indicating the respective number of registration.

Signed in Bucharest on 14th of May 2008 in two originals, each one in the Romanian, Portuguese and English languages, all texts being equally authentic. In case of any divergence of interpretation the English text shall prevail.

FOR
ROMANIA

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

FOR
THE PORTUGUESE REPUBLIC

ALEXANDRE VASSALO
Portuguese Ambassador