LAW No. 67 of 21 March 2007
on the ratification of the Agreement between the Government of Romania and the Government of the Republic of Bulgaria on the Mutual Protection of Classified Information, signed in Bucharest on 13 April 2006

ISSUER: The PARLIAMENT
PUBLISHED IN: The Official Journal no.218 of 30 March 2007

The Parliament of Romania adopts this law.

SINGLE ARTICLE
The Agreement between the Government of Romania and the Government of the Republic of Bulgaria on the Mutual Protection of Classified Information, signed in Bucharest on 13 April 2006 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
BOGDAN OLTEANU
p. PRESIDENT OF THE SENATE
DORU IOAN TĂRĂCILĂ

Bucharest, 21 March 2007
No. 67

Agreement between the Government of Romania and the Government of the Republic of Bulgaria on Mutual Protection of Classified Information

The Government of Romania and the Government of the Republic of Bulgaria, hereafter called the Contracting Parties,

Realizing that good cooperation may require exchange of classified information between the Contracting Parties,

Desiring to create a set of rules regulating the mutual protection of classified information applicable to any future co-operation agreements and classified contracts, which will be implemented between the Contracting Parties, containing or providing for access to classified information,

Have agreed on the following:

ARTICLE 1
GENERAL PROVISIONS

(1) This Agreement shall form the basis of any activity involving, in compliance with national legislation, the exchange of Classified Information between the Contracting Parties directly or through other state bodies or legal entities.

(2) The decision concerning the exchange of the Classified Information between the Contracting Parties is taken in accordance with their national legislation.

(3) The Contracting Parties shall fulfill their obligations stipulated in this Agreement, according to the terms set forth herein, on the base of equality and mutual benefit principles.

(4) This Agreement shall not affect the obligations of both Contracting Parties which stem from other international agreements and shall not be used against the interests, security and territorial integrity of other states.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

a) **Classified Information** means:
any information, regardless of its physical form, to which a security classification level has been assigned in compliance with national legislation and which shall be protected accordingly;

b) **Classified Document** means:
any recorded Classified Information, regardless of its physical form and characteristics, including, without limitation, the following carriers: handwritten or typed paper, seals applications used for processing data, maps, tables, photographs, pictures, pigmentation, engravings, drawings or parts thereof, sketches, rough copies, notes, carbon copies, ink ribbons or for reproducing by any means or process sounds, voices, magnetic or video or electronic or optical recordings in any form, as well as portable automatic data processing equipment with a fixed or removable data storage carrier;

c**) Classified Material** means:
any technical item, prototype, equipment, installation, device or weapon either manufactured or in a process of manufacture, as well as the components used for their manufacture, containing Classified Information;

d) **Security Classification Marking** means:
a marking stating the security classification level of Classified Information, in accordance with the national legislation of the states of the Contracting Parties;

e) **Classified Contract** or **Sub-Contract** means:
an agreement concluded, in compliance with the national legislation, between Contractors or between Contractor and Sub-Contractor which contains and/or provides for access to Classified Information in the process of its execution;

f) **Contractor** or **Sub-Contractor** means:
an individual or a legal entity possessing the legal capability to conclude Classified Contracts or is a party to a Classified Contract;

g) **Breach of Security** means:
an act or omission contrary to national legislation, which results or may result in an Unauthorized Access to Classified Information;

h) **Unauthorized Access to Classified Information** means:
disclosure, misuse, change in, damage, submission, unauthorized destruction of Classified Information, as well as any other acts, resulting in breach of protective measures or loss of such information;

i) **Personnel Security Clearance** means:
a positive decision stemming from a vetting procedure which is to determine the loyalty and trustworthiness of a person and affirm the conformity with the conditions set out in national legislation. On the basis of this positive decision access to information of a certain level of classification may be granted to such a person;

j) **Facility Security Clearance** means:
a positive decision stemming from a vetting procedure which is to determine the physical and organizational capability of a legal entity to protect Classified Information appropriately and affirm the conformity with the conditions set out in national regulations. On the basis of this positive decision access to information of a certain level of classification may be granted to such an entity;

k) **"Need to Know" principle** means:
a principle according to which access to Classified Information may only be granted to a person who, in carrying out his official duties or tasks, needs access to such information;

l) **Competent Security Authority** means:
the authority which in compliance with the national legislation of the state of the respective Contracting Party performs the state policy for the protection of Classified Information, exercises overall control in this sphere as well as conducts the implementation of this Agreement, and is determined as such in Article 4 of this Agreement;

m) **Specialized Security Authority** means:
the institution which, in compliance with the national legislation has specific competences in the field of the protection of the Classified Information;

n) **Third Party** means:
a state or an international organization, which is not a party to this Agreement or an individual or a legal entity which does not respond to the respective national requirements of access to Classified Information, including the “need to know” principle.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

(1) The security classification levels applicable to information exchanged within the framework of this Agreement are:

a) for Romania: STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ (TOP SECRET), STRICT SECRET (SECRET), SECRET (CONFIDENTIAL) and SECRET DE SERVICIU (RESTRICTED);

b) for the Republic of Bulgaria: СТРОГО СЕКРЕТНО (TOP SECRET), СЕКРЕТНО (SECRET), ПОВЕРИТЕЛНО (CONFIDENTIAL) and ЗА СЛУЖЕБНО ПОЛЗВАНЕ (RESTRICTED).

(2) The Contracting Parties have determined that the equivalence of the security classification levels is as follows:

Romania	**Republic of Bulgaria**	**English Equivalent**
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	СТРОГО СЕКРЕТНО	TOP SECRET
STRICT SECRET	СЕКРЕТНО	SECRET
SECRET	ПОВЕРИТЕЛНО	CONFIDENTIAL
SECRET DE SERVICIU	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

(3) Only the originating Contracting Party is authorized to change the security classification level or to declassify the transmitted Classified Information. The assignment of security classification level to jointly created Classified Information, its change or the declassification of this information shall be made upon common consent of the Contracting Parties.

ARTICLE 4
COMPETENT SECURITY AUTHORITIES

(1) The Competent Security Authorities responsible for the implementation and the relevant control of all aspects of this Agreement are:

- In Romania: Guvernul României, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat – ORNISS Bucureşti, str. Mureş nr. 4, sect. 1, ROMÂNIA (Government of Romania, National Registry Office for Classified Information, Bucharest, 4 Mureş Street, Sector 1, ROMANIA);

- In the Republic of Bulgaria: Държавна Комисия по Сигурността на Информацията-ДКСИ, София, ул. Ангел Кънчев No 1, БЪЛГАРИЯ, (State Commission on Information Security, Sofia, Angel Kanchev 1 Street, BULGARIA).

(2) In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information applied by the respective Contracting Party. Each Competent Security Authority shall, by mutual consent, enable inspection visits of authorised officials in both countries.

ARTICLE 5
CLASSIFIED INFORMATION PROTECTION MEASURES

(1) In compliance with this Agreement and their national legislations, the Contracting Parties shall implement all appropriate measures for protection of Classified Information which is exchanged or created under this Agreement. The same level of protection shall be ensured for such Classified Information as it is provided for the national

Classified Information, with the corresponding security classification level pursuant to Article 3.

(2) The receiving Contracting Party shall neither use a lower security classification level for the received Classified Information nor declassify this information without the prior written consent of the Competent Security Authority of the originating Contracting Party.

(3) The receiving Contracting Party is obliged:

a) not to disclose Classified Information to a Third Party without a prior written consent of the originating Contracting Party;

b) to afford Classified Information a security classification level equivalent to that provided by the originating Contracting Party;

c) not to use Classified Information for purposes other than those it has been provided for;

d) to guarantee the private rights such as patent rights, copyrights or trade secrets that are involved in Classified Information.

(4) The originating Contracting Party shall ensure that the receiving Contracting Party is informed of:

a) Security Classification Markings of information and any conditions of release or limitation on its use, and that information is so marked;

b) any subsequent change in security classification levels.

(5) If any other Agreement concluded between the Contracting Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

(6) In case it is impossible to protect and return Classified Information created or exchanged according to this Agreement, the Classified Information shall be destroyed immediately. The receiving Contracting Party shall notify the Competent Security Authority of the originating Contracting Party about such a destruction of the Classified Information as soon as possible.

ARTICLE 6
TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified Information shall be transmitted by diplomatic or military couriers or other means approved by the Competent Security Authorities. The receiving Competent Security Authority shall acknowledge receipt of the Classified Information.

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

(3) The exchange of Classified Information through information and communications systems shall take place in accordance with the security procedures set out in national legislation.

ARTICLE 7
SECURITY CLASSIFICATION MARKINGS

(1) The receiving Contracting Party shall mark the Classified Information of the originating Contracting Party with equivalent Security Classification Marking in accordance with Article 3 of this Agreement.

(2) Classified Information created jointly shall be marked by the Contracting Party within the territory of which this information has been created. In this case, this Contracting Party shall be considered originating Contracting Party. The originating Contracting Party may transmit the jointly created Classified Information to a Third Party only upon prior written consent of the other Contracting Party.

(3) Classified Information created by the receiving Contracting Party on the basis of Classified Information or part of it transmitted by the originating Contracting Party shall be marked with a Security Classification Marking which is not lower than the Security Classification Marking of the transmitted Classified Information.

ARTICLE 8
TRANSLATION, REPRODUCTION, DESTRUCTION

(1) Classified Documents marked with a security classification level STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ / СТРОГО СЕКРЕТНО / TOP SECRET shall be translated or copied only by written permission of the Competent Security Authority of the originating Contracting Party.

(2) Any translation of Classified Information shall bear the Security Classification Marking of the original and a suitable annotation in the language of translation indicating that the translated material contains Classified Information of the originating Contracting Party.

(3) When Classified Information is reproduced or copied, all original Security Classification Markings thereon shall also be reproduced or marked on each copy. Such reproduced or copied information shall be placed under the same protective measures as the original information. The number of copies shall be limited to that required for official purposes.

(4) Classified Information shall be destroyed or modified insofar as to forestall its reconstruction in whole or in part.

(5) Classified Information of the security classification level STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/ СТРОГО СЕКРЕТНО / TOP SECRET shall not be destroyed. It shall be returned to the originating Contracting Party.

(6) The originating Contracting Party may expressly prohibit reproduction, alteration or destruction of a Classified Information by marking the relevant carrier of Classified Information or sending subsequent written notice. In such case, the Classified Information subject to destruction shall be returned to the originating Contracting Party, except in the case referred to in Article 5, paragraph 6.

ARTICLE 9
SECURITY CLEARANCES

(1) Each Contracting Party shall guarantee that any individual, who, due to his official duties or tasks, needs access to Classified Information, holds a valid and appropriate Personnel Security Clearance, issued in accordance with the national legislation.

(2) Upon request, the Competent Security Authorities/ Specialized Security Authorities of the Contracting Parties, in compliance with national legislation, shall exchange information related to the vetted individuals or legal entities.

(3) Upon request**,** the Competent Security Authority of each Contracting Party shall provide information whether an individual or a legal entity has been issued a national Personnel Security Clearance/ Facility Security Clearance corresponding to the required security classification level.
If an individual or a legal entity does not hold a Personnel Security Clearance/ Facility Security Clearance the Competent Security Authority of each Contracting Party may request for that individual or legal entity to be security cleared.

(4) The Contracting Parties shall mutually recognize the validity of Personnel Security Clearances and Facility Security Clearances, in accordance with national legislation.

(5) The Competent Security Authorities shall notify each other on any withdrawal or downgrading of Personnel Security Clearances or Facility Security Clearances, issued to individuals or legal entities which perform activities under the provisions of this Agreement.

ARTICLE 10
INDUSTRIAL SECURITY

(1) Classified Contracts shall be concluded and implemented in accordance with the national legislation of the Contracting Parties and the provisions of this Agreement.

(2) In case a Classified Contract is performed within the territory of the state of one of the Contracting Parties, the authorities of the state of

that Contracting Party are obliged to exercise control regarding the fulfillment of the Classified Information protection obligations by the Contractor.

(3) Prior to releasing to Contractors from the state of either Contracting Party any Classified Information of the other Contracting Party, the receiving Contracting Party shall:

a) grant an appropriate Facility Security Clearance to the Contractors on condition they have fulfilled the requirements for its issue;

b) grant an appropriate Personnel Security Clearance to all individuals whose official duties or tasks require access to Classified Information on condition they have fulfilled the requirements for its issue;

c) ensure that all individuals having access to received Classified Information have been appropriately briefed on security procedures and their security obligations. All such individuals shall acknowledge in writing that they fully understand their responsibilities and the consequences which the national legislation provides when Classified Information passes to unauthorized individuals either by intent or negligence.

(4) Every Classified Contract shall include an appropriate security annex. The Security annex shall specify the information connected with various aspects of the Classified Contract which require protection and the corresponding security classification level that is to be assigned thereto, as well as the security requirements that are to be met.

(5) Classified Contracts placed with contractors involving Classified Information at SECRET DE SERVICIU / ЗА СЛУЖЕБНО ПОЛЗВАНЕ / RESTRICTED level shall contain an appropriate clause identifying the minimum measures to be implemented for the protection of such Classified Information.

ARTICLE 11
VISITS

(1) Visits to premises where Classified Information is created, handled or stored, shall be allowed only by the Competent Security Authority of the visited state to visitors from the state of the other Contracting Party, if they need access to Classified Information.

(2) Each Contracting Party shall notify in due time the other Contracting Party of expected visitors prior to the planned visit. Short notice visits can be arranged in urgent cases by special mutually determined arrangements.

(3) The host Contracting Party shall be responsible for briefing specifically the personnel of the facilities and establishments that are to be visited on the decisions referring to the objective of the visit and the highest level of Classified Information that is to be released to the visiting Contracting Party.

(4) Request concerning carrying out the visit shall be forwarded in written form to the Competent Security Authority of the Contracting Party whose territory shall be visited.

(5) The request for visit shall contain the following information:
- name of the proposed visitor, date and place of birth, nationality and passport (ID card) number;

- official status of the visitor together with the name of the establishment, company or organization which he/she represents or to which he/she belongs;

- certification of level of security clearance of the visitor;

- name and address of the establishment, company or organization to be visited;

- name and status of the person(s) to be visited, if known;

- purpose of the visit;

- dates of arrival and departure.

(6) Each Contracting Party shall guarantee protection of personal data of the visitors, according to the respective national legislation.

(7) All visitors shall comply with the legislation on protection of Classified Information of the host Contracting Party's state.

ARTICLE 12
BREACH OF SECURITY

(1) In case of a Breach of Security, the Competent Security Authority of the state where the Breach of Security occurred shall inform promptly the Competent Security Authority of the other Contracting Party, shall ensure proper investigation of such event and shall take the necessary measures to reduce the prejudices, in accordance with national legislation. The authorities of the state of the other Contracting Party shall, if required, cooperate in the investigation.

(2) In case the Breach of Security occurs in a third country, the Competent Security Authority of the Contracting Party which transmitted the information to the third country shall take if possible the actions as of paragraph 1.

(3) The Competent Security Authority of the state where the Breach of Security occurred shall inform in writing the other Contracting Party of the results of the investigation regarding the causes of the event, the extent of the damage and the measures taken for its limitation and for the prevention of its recurrence.

ARTICLE 13
SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultation between the Competent Security Authorities of the two states, without recourse to outside jurisdiction.

ARTICLE 14
EXPENSES

Each Contracting Party shall cover its own expenses in the course of the implementation of this Agreement.

ARTICLE 15
MUTUAL ASSISTANCE

(1) Each Contracting Party and the authorities of its state with responsibilities in the field of protection of Classified Information, in compliance with the national legislation, shall assist the personnel from the state of the other Contracting Party in fulfilling the obligations and exercising the rights in accordance with the provisions of this Agreement.

(2) Should the need arise the Competent Security Authorities of the Contracting Parties shall consult each other on specific technical aspects concerning the implementation of this Agreement.

(3) The Competent Security Authorities shall mutually provide information required to the implementation of the provisions of this Agreement.

ARTICLE 16
FINAL PROVISIONS

(1) This Agreement is concluded for an indefinite period of time and enters into force on the date of receiving the last written notification whereby the Contracting Parties inform each other of the fulfillment of all internal procedures necessary for its entry into force.

(2) This Agreement may be amended and supplemented on the basis of the mutual consent of both Contracting Parties. Such amendments or supplements shall be made in writing and shall enter into force in accordance with the provisions of paragraph 1 of this Article.

(3) Each Contracting Party has the right to terminate this Agreement in writing at any time. In such case the validity of the Agreement will expire after 6 (six) months following the day on which the termination notice has been received by the other Contracting Party.

(4) Should the validity of this Agreement expire, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the originating Contracting Party dispenses the receiving Contracting Party from this obligation.

(5) Each Contracting Party shall promptly notify the other Contracting Party of any changes to its national legislation that would affect the protection of Classified Information under this Agreement. In such case, the Contracting Parties shall consult to consider possible changes to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein.

(6) When this Agreement enters into force, the Agreement between the Government of Romania and the Government of the Republic of Bulgaria on the protection of exchanged classified military information, signed at Sofia, on 29th March, 2000 shall be terminated.

Done in Bucharest, on 13th April 2006, in two original copies, each one in the Romanian, Bulgarian and English languages, all texts having equal validity. In case of differences in interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF ROMANIA	**FOR THE GOVERNMENT OF THE REPUBLIC OF BULGARIA**
Prof. dr. MARIUS PETRESCU **Secretary of State** **Director General** **of the National Registry Office for Classified Information**	**TSVETA MARKOVA** **Chairperson** **of the State Commission on Information Security**