

A G R E E M E N T

B E T W E E N

THE GOVERNMENT OF THE REPUBLIC OF BULGARIA

A N D

THE GOVERNMENT OF THE REPUBLIC OF ESTONIA

ON MUTUAL PROTECTION AND EXCHANGE

OF CLASSIFIED INFORMATION

The Government of the Republic of Bulgaria and the Government of the Republic of Estonia (hereinafter referred to as the "Parties"),

Having agreed to hold talks on political and security-related issues and to broaden and tighten their political, military and economic co-operation,

Being aware of the changes in the political situation in the world and recognising the important role of their mutual co-operation for the stabilisation of peace, international security and mutual confidence,

Realising that good co-operation may require exchange of Classified Information between the 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 Parties, containing or involving Classified Information,

Have agreed as follows:

Article 1

Definitions

For the purpose of this Agreement:

(1) **"Classified Information"** means information of whatever form, nature or method of transmission either manufactured or in the process of manufacture to which a security classification level has been attributed and which, in the interests of national security and in accordance with the national laws and regulations, require protection against unauthorised access or destruction.

(2) **"Unauthorised access to Classified Information"** means any form of disclosure of Classified Information, including misuse, damage, submission and incorrect classification thereof, as well as any other actions, resulting in breach of protection or loss of such information, as well as any actions or inactions that have resulted in making the information known to an unauthorised person.

(3) **"Classified Document"** means any form of recorded Classified Information, regardless of its characteristics or type of recording media.

(4) **"Classified Material"** means any classified document or technical item, 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.

(5) **"Security classification level"** means category, according to the national laws and regulations, which characterises importance of Classified Information, level of restriction of access to it and level of its protection by the Parties and also the category on the basis of which information is marked.

(6) **"Classification marking"** means a mark on any classified material, which shows the security classification level.

(7) **"Security clearance"** means a positive determination stemming from a vetting procedure that shall ascertain loyalty and trustworthiness of an individual or legal entity as well as other security aspects in accordance with national laws and regulations. Such determination enables to grant the individual or the legal entity access and allow them to handle Classified Information on a certain level without security risk.

(8) **"Originating Party"** means the Party initiating Classified Information.

(9) **"Receiving Party"** means the Party to which Classified Information is transmitted.

(10) **"User"** means individual or a legal entity that takes part in relevant co-operation activities or in implementation of classified contracts to which this Agreement will be applied.

(11) **"Competent Authority"** means the authority, which in compliance with the national laws and regulations of the respective 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. Such authorities are listed in Article 5 of this Agreement.

(12) **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude contracts and/or a party to a classified contract under the provisions of this Agreement.

(13) **"Classified Contract"** means an agreement between two or more users, which contains or provides for access to Classified Information.

(14) **"Need-to-know principle"** means the necessity to have access to Classified Information in connection with official duties and/or for the performance of a concrete official task.

(15) **"Third Party"** means a state or international organisation, which is not a Party to this Agreement or a user, which does not respond to the national requirements of access to Classified Information, including the "need-to-know" principle.

(16) **"Declassification of Information"** means the removal of the security classification level.

(17) **"Breach of security"** means an act or an omission contrary to the national laws and regulations, which results or may result in an unauthorised access or destruction of Classified Information.

Article 2 Objective

The objective of this Agreement is to ensure protection of Classified Information that is commonly generated or exchanged either directly or indirectly between the Parties.

Article 3 Security Classification levels

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national laws and regulations of the respective Party:

For the Republic of Bulgaria	Equivalent in English	For the Republic of Estonia
СТРОГО СЕКРЕТНО	TOP SECRET	TÄIESTI SALAJANE
СЕКРЕТНО	SECRET	SALAJANE
ПОВЕРЛИВО	CONFIDENTIAL	KONFIDENTSIAALNE
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED	PIIRATUD

Article 4 National measures

(1) In compliance with their national laws and regulations, the Parties shall implement all appropriate measures for protection of Classified Information, which is commonly generated or exchanged either directly or indirectly 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.

(2) The Parties shall in due time inform each other about any changes in the national laws and regulations affecting the protection of Classified Information. In such cases, the Parties shall inform each other in compliance with Paragraphs 3 and 4 of Article 5 in order to discuss possible amendments to this Agreement. Meanwhile, the Classified Information shall be protected according to the provisions of the Agreement, unless otherwise agreed in writing.

(3) No individual shall be entitled to access to Classified Information solely by virtue of his or her rank, official position or security clearance. Access to Classified Information shall be granted only to those individuals who have been issued a security clearance and in accordance with the "need to know" principle.

(4) The Receiving Party is obligated:

- a) not to disclose Classified Information to a Third Party without a prior written consent of the Competent Authority of the Originating Party;
- b) to grant Classified Information a security classification level equivalent to that provided by the Originating Party;

c) not to use Classified Information for other purposes 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.

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

Article 5

Competent Authorities

(1) The Competent Authorities of the Parties are:

For the Republic of Bulgaria:

- State Commission for Information Security.
Angel Kanchev 1 Str.
Sofia
BULGARIA

For the Republic of Estonia:

- National Security Authority
Security Department
Ministry of Defence
Sakala 1
15094 Tallinn
ESTONIA

(2) The Competent Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information.

(3) In order to ensure close co-operation in the implementation of the present Agreement, the Competent Authorities may hold consultations at the request made by one of them.

(4) In order to achieve and maintain comparable standards of security, the respective Competent Authorities shall, on request, provide each other with

information about the security standards, procedures and practices for protection of Classified Information employed by the respective Party.

(5) The respective Competent Authorities may conclude executive documents in relation with this Agreement.

(6) The Security Services of the Parties may exchange and return operative and/or intelligence information directly with each other in accordance with national laws and regulations.

Article 6

Transfer of Classified Information

(1) As a rule, Classified Information shall be transferred by means of diplomatic or military couriers or by other means satisfying the requirements of the national laws and regulations of the Parties. The Receiving Party shall confirm in writing the receipt of Classified Information.

(2) Classified Information may be transmitted via protected telecommunication systems, networks or other electromagnetic means approved by the Competent Authorities and holding a duly issued certificate pursuant to the national laws and regulations of either Party.

(3) Other approved means of transfer of Classified Information may only be used if agreed upon between the Competent Authorities.

(4) In case of transferring a large consignment containing Classified Information, the Competent Authorities shall mutually agree on and approve the means of transportation, the route and the other security measures.

Article 7

Translation, reproduction, destruction

(1) Classified Documents marked with a security classification level ЦРОГО СЕКРЕТНО / TOP SECRET / TÄIESTI SALAJANE shall be translated or reproduced only by written permission of the Competent Authority of the Originating Party.

(2) All translations of Classified Information shall be made by individuals who have appropriate security clearance. Such translation shall bear an equal security classification marking.

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

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

(5) The Originating Party may expressly prohibit reproduction, alteration or destruction of a classified material by marking the relevant carrier of Classified Information or sending subsequent written notice. If destruction of the classified material is prohibited, it shall be returned to the Competent Authority of the Originating Party.

(6) Classified material of CTPOFO CEKPETHO / TOP SECRET / TÄIESTI SALAJANE security classification level shall not be destroyed. It shall be returned to the Competent Authority of the Originating Party.

(7) In case of crisis situation, which makes it impossible to protect and return Classified Information generated or transferred according to this Agreement the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

Article 8

Classified Contracts

(1) Classified Contract shall be concluded and implemented in accordance with national laws and regulations of each Party. Upon request the Competent Authority of each Party shall furnish information whether a proposed contractor has been issued a national security clearance, corresponding to the required security classification level. If the proposed contractor does not hold a security clearance the Competent Authority of each Party may request for that contractor to be security cleared.

(2) A security annex will be an integral part of each classified contract or sub-contract. In this annex the contractor of the Originating Party will specify which Classified Information will be released to or generated by the Receiving Party, and which corresponding security classification level has been assigned to this information.

(3) The contractor's obligation to protect the Classified Information shall, in all cases, refer, at least, to the following:

a) an obligation that the contractor shall disclose the Classified Information only to a person who has been previously security cleared for access with regard to the relevant contract activities, who has "need-to-know" and who is employed or engaged in the carrying out of the contract;

b) the means to be used for the transfer of the Classified Information;

c) the procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its security classification level or because protection is no longer necessary;

d) the procedure for the approval of visits, access or inspection by personnel of one Party to facilities of the other Party which are covered by the contract;

e) an obligation to notify in due time the contractor's Competent Authority of any actual, attempted or suspected unauthorised access to Classified Information of the contract;

f) usage of the Classified Information under the contract only for the purposes related to the subject matter of the contract;

g) strict adherence to the procedures for destruction of the classified material;

h) provision of Classified Information under the contract to any third party only with the written consent of the Competent Authority of the Originating Party.

(4) The measures required for the protection of Classified Information as well as the procedure for assessment of and indemnification for possible

losses caused to the contractors by unauthorised access to Classified Information shall be specified in more detail in the respective classified contract.

(5) Contracts placed with contractors involving Classified Information at 3A СЛЮЖЕБНО ПОЛЗБАHE / RESTRICTED / PIIRATUD levels will contain an appropriate clause identifying the minimum measures to be applied for the protection of such Classified Information.

Article 9

Visits

(1) Security experts of the Competent Authorities may hold regular meetings to discuss the procedures for protection of Classified Information.

(2) Visitors shall receive prior authorization from the Competent Authority of the host state only if they are authorised for access to Classified Information in accordance with their national laws and regulations and if they need access to Classified Information or to premises where Classified Information is originated, handled or stored.

(3) Visiting procedures shall be agreed between the Competent Authorities.

(4) The request for visit shall contain the following information:

- a) name of the visitor, date and place of birth, passport (ID card) number;
- b) citizenship of the visitor;
- c) position title of the visitor and name of the organisation he represents;
- d) security clearance of the visitor of appropriate classification level;
- e) purpose, proposed working program and planned date of the visit;
- f) names of organisations and facilities requested to be visited.

(5) Each Party shall guarantee protection of personal data of the visitors, according to the respective national laws and regulations.

Article 10

Breach of Security

(1) In case of a breach of security, the Competent Authority in whose state a breach of security occurred shall inform the Competent Authority of the other Party as soon as possible and shall carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation.

(2) In any case, the other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of damage caused.

Article 11

Expenses

Each Party shall bear the expenses incurred in the course of implementing its obligations under this Agreement.

Article 12

Final Provisions

(1) This Agreement is concluded for an indefinite period of time and enters into force on the date of receiving the latest notice whereby the Parties inform each other of the fulfilment of all internal legal procedures necessary for its entry into force.

(2) This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

(3) Each Party may terminate this Agreement by written notice forwarded to the other Party. The termination shall enter into force six months after the date of receipt of the notification. Notwithstanding the termination of this Agreement, all Classified Information transferred 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.

(4) Any dispute regarding the interpretation or application of this Agreement shall be resolved amicably by consultation between the Parties without recourse to outside jurisdiction.

Done at Sofia on March 8th 2005 in two original copies, each in the Bulgarian, Estonian and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English language text shall prevail.

For the Government of
the Republic of Bulgaria



Tsveta Markova
Chairperson of the State
Commission for Information
Security

For the Government of
the Republic of Estonia



Herman Simm
Director of the Security
Department
Ministry of Defence
National Security Authority