

AGREEMENT
BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA
AND THE GOVERNMENT OF THE REPUBLIC OF POLAND
ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Estonia and the Government of the Republic of Poland, hereinafter referred to as “the Parties”,

Having due regard for the necessity of guaranteeing the effective protection of Classified Information exchanged between the Parties or generated in the course of the cooperation,

Being guided by the intention to adopt uniform regulations for both Parties in the scope of the protection of Classified Information,

Subject to respect binding rules of the international law and the national law of the Parties,

Have agreed as follows:

ARTICLE 1
SCOPE OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information that is generated by or exchanged between the Parties or individuals, legal entities or other forms of organisations under their jurisdiction.

2. This Agreement shall be applicable to any contract or agreement involving Classified Information concluded or performed between the Parties, individuals, legal entities or other forms of organisations under their jurisdiction as well as to any activity conducted between them.

ARTICLE 2

DEFINITIONS

For the purpose of this Agreement, the following definitions mean:

- 1) Classified Information – any information, irrespective of its form, carrier and manner of recording, as well as objects or any parts thereof, also in the process of being generated, which requires protection against unauthorised disclosure in accordance with the national law of either Party and this Agreement and which has been duly designated as such;
- 2) National Security Authority – the authority which, in accordance with the national law of either Party, is responsible for the implementation of this Agreement;
- 3) Originating Party – the Party or an individual, a legal entity or other form of organisation under its jurisdiction, which has generated the Classified Information;
- 4) Recipient Party – the Party or an individual, a legal entity or other form of organisation under its jurisdiction, which receives the Classified Information;
- 5) Classified Contract – a contract that contains or the performance of which involves access to Classified Information;
- 6) Contractor – an individual, a legal entity or other form of organisation under the law of one of the Parties, which in accordance with the national law is entitled to perform Classified Contracts;
- 7) Principal – an individual, a legal entity or other form of organisation under the law of one of the Parties, which in accordance with the national law is entitled to initiate Classified Contracts;
- 8) Third Party – any state or an individual, a legal entity or other form of organisation under the state’s jurisdiction or an international organisation that is not a Party to this Agreement;
- 9) Personnel Security Clearance – a determination made in accordance with the national law of one of the Parties that an individual is authorised to access Classified Information;
- 10) Facility Security Clearance – a determination made in accordance with the national law of one of the Parties that a Contractor is capable to protect Classified Information;
- 11) Need-to-Know – a principle by which access to Classified Information may be granted to an individual only in connection with his official duties and for the performance of a specific task;
- 12) Breach of Security – an act or an omission contrary to the national law, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

1. Classified Information is granted a security classification level in accordance to its content, pursuant to the national law of the Originating Party. The Recipient Party shall guarantee at least an equivalent level of protection of the received Classified Information, pursuant to the provisions of paragraph 3.
2. The security classification level may be altered or revoked only by the Originating Party. The Recipient Party shall be notified in writing of every alteration or revocation of the security classification level of previously received Classified Information.
3. The Parties agree that the following security classification levels are equivalent:

THE REPUBLIC OF ESTONIA	THE REPUBLIC OF POLAND	EQUIVALENT IN ENGLISH
TÄIESTI SALAJANE	ŚCIŚLE TAJNE	TOP SECRET
SALAJANE	TAJNE	SECRET
KONFIDENTSIAALNE	POUFNE	CONFIDENTIAL
PIIRATUD	ZASTRZEŻONE	RESTRICTED

4. The Recipient Party shall ensure that the Classified Information is marked with an equivalent classification marking in accordance with paragraph 3.

ARTICLE 4
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:
 - 1) for the Republic of Poland: the Head of the Internal Security Agency;
 - 2) for the Republic of Estonia: Estonian Foreign Intelligence Service, National Security Authority Department.
2. The Parties shall inform each other via diplomatic channels about changes of the National Security Authorities referred to in paragraph 1 or amendments to their competences.

ARTICLE 5
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. The Parties shall adopt every measure provided in this Agreement and subject to their national law in order to protect Classified Information transmitted or generated as a result of the cooperation between the Parties, including that generated in connection with the performance of Classified Contracts.
2. The Recipient Party shall use Classified Information exclusively for the purposes for which it has been transmitted.
3. Access to Classified Information shall be granted only to those individuals who have a Need-to-Know and who are authorised in accordance with the national law of the Recipient Party to have access to Classified Information of the equivalent security classification level.
4. The Recipient Party shall not release the Classified Information referred to in paragraph 1 to any Third Party without a prior written consent of the Originating Party.

ARTICLE 6
SECURITY CLEARANCES

1. Within the scope of this Agreement, the Parties shall recognise Personnel Security Clearances and Facility Security Clearances issued in accordance with the national law of the other Party.
2. The National Security Authorities of the Parties shall assist each other upon request of one of them in carrying out vetting procedures.
3. Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearances or Facility Security Clearances, in particular about their revocation or an alteration of the security classification level.
4. Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Recipient Party shall issue a written confirmation that an individual has the right to access Classified Information.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract involving access to information classified as KONFIDENTSIAALNE / POUFNE / CONFIDENTIAL or above, the Principal shall apply to its National Security Authority to request that the National Security Authority of the other Party issue a certificate that the Contractor is a holder of a valid Facility Security Clearance relevant to the security classification level of the Classified Information the Contractor is to have access to.

2. Classified Information shall not be released to the Contractor until the receipt of the certificate referred to in paragraph 1.

3. The Principal shall transmit to the Contractor a facility security instruction necessary to perform a Classified Contract, which is an integral part of every Classified Contract. The facility security instruction contains provisions on the security requirements, in particular:

1) the list of types of Classified Information related to a given Classified Contract, including their security classification levels;

2) the rules for granting security classification levels to information generated during the performance of a given Classified Contract.

4. The Principal shall put forward a copy of the facility security instruction to the National Security Authority of its Party, which shall transmit it to the National Security Authority of the Contractor's Party.

5. The performance of a Classified Contract in the part involving access to Classified Information shall be possible on condition that the Contractor meets the criteria necessary for the protection of Classified Information, pursuant to the facility security instruction.

6. Every subcontractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

ARTICLE 8
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted via diplomatic channels.
2. Classified Information may be transmitted through protected communications systems, networks, or other electromagnetic media approved in accordance with the national law of the Parties. The National Security Authorities shall inform each other about the systems to be used.
3. Information classified as PIIRATUD / ZASTRZEŻONE / RESTRICTED may be transmitted also through authorised carriers in accordance with the national law of the Originating Party.
4. The National Security Authorities of the Parties may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure.
5. If necessary, the security and police services of the Parties may exchange Classified Information directly.
6. The Recipient Party shall confirm in writing the receipt of Classified Information.

ARTICLE 9
REPRODUCTION OR TRANSLATION OF CLASSIFIED INFORMATION

1. Reproduction or translation of Classified Information shall be conducted pursuant to the national law of each of the Parties. Reproduced or translated information shall be placed under the same protection as the original information. The number of copies or translations shall be reduced to that required for official purposes.
2. Information classified as TÄIESTI SALAJANE / ŚCIŚLE TAJNE / TOP SECRET shall be reproduced or translated only after obtaining a prior written consent issued by the Originating Party.

ARTICLE 10
DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Information shall be destroyed in accordance with the national law of the Recipient Party in such a manner as to eliminate its partial or total reconstruction.
2. Information classified as TÄIESTI SALAJANE / ŚCIŚLE TAJNE / TOP SECRET shall not be destroyed, it shall be returned to the Originating Party.
3. In case of exceptional circumstances in which it is impossible to protect or return Classified Information referred to in paragraph 2, it shall be destroyed immediately. The National Security Authority of the Recipient Party shall inform the National Security Authority of the Originating Party about this destruction as soon as possible.

ARTICLE 11
VISITS

1. Visits involving access to Classified Information shall be subject to prior permission of the National Security Authority of the host Party.
2. The National Security Authority of the visiting Party shall apply with a request for a visit to the National Security Authority of the host Party at least 30 days prior to the planned visit referred to in paragraph 1, and in urgent cases in shorter time.
3. The request referred to in paragraph 2 shall include the date, signature and official seal of the National Security Authority of the visiting Party as well as the following information:
 - 1) purpose of the visit, including the highest security classification level of Classified Information involved;
 - 2) date and program of the visit;
 - 3) name and surname of the visitor, his date and place of birth, nationality and passport or other official identification document's number;
 - 4) position of the visitor together with the name of the entity which he represents;

5) level and the validity date of Personnel Security Clearance held by the visitor;

6) name and address of the entity to be visited;

7) name, surname and position of the person to be visited.

4. The National Security Authorities of the Parties may agree to establish lists of persons authorised to make recurring visits connected with the implementation of a specific project, program or Classified Contract. The lists shall contain the data specified in paragraph 3 and are valid for a period of 12 months. Once such lists have been approved by the National Security Authorities of the Parties, the dates of the visits shall be arranged directly between visiting and hosting entities, in accordance with the conditions agreed upon.

5. Visits involving access to information classified as PIIRATUD / ZASTRZEŻONE / RESTRICTED are arranged directly between authorised visiting and hosting entities.

6. The Parties shall ensure, pursuant to their national law, the protection of the personal data of the persons arriving on a visit involving access to Classified Information.

ARTICLE 12

BREACH OF SECURITY

1. Information on every Breach of Security or a suspicion of a Breach of Security concerning Classified Information of the Originating Party or Classified Information generated as a result of cooperation of the Parties shall be immediately reported to the National Security Authority of the other Party.

2. Every Breach of Security or a suspicion of a Breach of Security shall be investigated pursuant to the national law of the Party in the territory of the state of which it has occurred. The National Security Authority of one Party shall inform the National Security Authority of the other Party in writing about the circumstances of the breach and the outcome of the investigation.

3. The National Security Authorities of the Parties shall cooperate in the investigations referred to in paragraph 2, upon the request of one of them.

ARTICLE 13
LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use English or their official languages, in case of which the translation into the official language of the other Party or English shall be attached.

ARTICLE 14
EXPENSES

Each Party shall cover its expenses resulting from the implementation of the provisions of this Agreement.

ARTICLE 15
CONSULTATIONS

1. The National Security Authorities of the Parties shall notify each other of any amendments to their national law on the protection of Classified Information concerning the implementation of this Agreement.
2. The National Security Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions of this Agreement.
3. In order to ensure effective cooperation resulting from the provisions of this Agreement, and in the scope of authority acknowledged by the national law of their Parties, the National Security Authorities may, if necessary, conclude written detailed technical or organisational arrangements.

ARTICLE 16
SETTLEMENT OF DISPUTES

1. Any disputes concerning the implementation of this Agreement shall be settled by direct negotiations between the National Security Authorities of the Parties.

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

ARTICLE 17
RELATION TO PREVIOUS AGREEMENTS

Upon entry into force of this Agreement, the *Agreement between the Government of the Republic of Poland and the Government of the Republic of Estonia on Mutual Protection of Classified Information*, done in Warsaw on 12 May 2003, shall terminate. Previously exchanged Classified Information shall be protected in accordance with the provisions of this Agreement.

ARTICLE 18
FINAL PROVISIONS

1. This Agreement shall enter into force after the completion of the national procedures of each of the Parties, which shall be confirmed by an exchange of notes. The Agreement shall enter into force on the first day of the second month following the receipt of the latter note.

2. This Agreement may be amended on the basis of mutual written consent of both Parties. Such amendments shall enter into force in accordance with the provisions of paragraph 1.

3. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party by giving written notice to the other Party. In such case, this Agreement shall expire after six months following the receipt of the termination notice.

4. In case of termination, Classified Information exchanged or generated on the basis of this Agreement shall be protected in accordance with the provisions thereof.

Done at Warsaw on the 27th of November, 2018 in two original copies, each in the Estonian, Polish and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF
THE REPUBLIC OF ESTONIA

Martin Roger

FOR THE GOVERNMENT OF
THE REPUBLIC OF POLAND

Piotr Pogonowski