

Väljaandja:
Akti liik:
Teksti liik:
Jõustumise kp:
Avaldamismärge:

Vabariigi Valitsus
välisleping
algtekst
02.08.2006
RT II 2006, 17, 46

Eesti Vabariigi valitsuse ja Albaania Vabariigi Ministrite Nõukogu salastatud teabe vastastikuse kaitse kokkulepe

[“Eesti Vabariigi valitsuse ja Albaania Vabariigi ministrite nõukogu salastatud teabe vastastikuse kaitse kokkuleppe” eelnõu heakskiitmine](#)

[Teadaanne välislepingu jõustumise kohta](#)

Koostatud 29. märtsil 2006 Tallinnas, jõustus 2. augustil 2006

Eesti Vabariigi valitsus ja Albaania Vabariigi ministrite nõukogu (edaspidi *pooled*),

kavatsedes tagada vastastikuse kaitse kogu salastatud teabele, mis on koostatud või salastatud ühe poole riigis ja edastatud teise poole riigile,

soovides kehtestada salastatud teabe vastastikuse kaitse korda, mida kohaldatakse kõigile poolte vahel sõlmitavatele koostöökokkulepetele ning poolte füüsiliste ja juriidiliste isikute lepingutele, milles nähakse ette vahetada salastatud teavet,

on kokku leppinud järgmises.

Artikkel 1. Mõisted

Kokkuleppes kasutatakse järgmisi mõisteid.

- 1) *Salastatud teave*– dokument või materjal, mida selle vormist, laadist või edastusviisist olenemata tuleb riikliku julgeoleku huvides ja poolte riigisiseste õigusaktide kohaselt kaitsta julgeolekunõuete rikkumise, hävitamise, avalikustamise, kadumise, loata juurdepääsu või muul viisil ohtusattumise eest.
- 2) *Vastuvõttev pool*– pool, kellele edastatakse salastatud teavet.
- 3) *Päritolupool* –pool, kellelt salastatud teave pärineb.
- 4) *Riigi julgeoleku volitatud esindaja*– riigiorgan, kes poole riigisiseste õigusaktide kohaselt vastutab salastatud teabe kaitsmise ja kokkuleppe täitmise eest.
- 5) *Lepinglane*– füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid.
- 6) *Salastatud leping*– kahe või enama lepinglase kokkulepe, millega määratakse kindlaks poolte õigused ja kohustused ning mis sisaldab salastatud teavet või on sellega seotud.
- 7) *Kolmas isik*– rahvusvaheline organisatsioon või kolmas riik (ka selle füüsilised ja juriidilised isikud), kes ei ole kokkuleppe pool.
- 8) *Külastaja*– ühe poole ametlik esindaja, kellel on vaja külastada teise poole ehitisi, milles tegeldakse salastatud teabega.
- 9) *Füüsilise isiku juurdepääsuluba*– dokument, mille riigi julgeoleku volitatud esindaja väljastab kooskõlas riigisiseste õigusaktidega oma kodanikule juurdepääsuks salastatud teabele.
- 10) *Juriidilise isiku juurdepääsuluba*– dokument, mille riigi julgeoleku volitatud esindaja väljastab kooskõlas riigisiseste õigusaktidega, ja mis tõendab, et juriidiline isik on reaalselt ja organisatoorselt võimeline kasutama ja hoidma salastatud teavet.
- 11) *Põhjendatud teadmismvajadus*– ametiülesannetega seotud juurdepääsuvajadus salastatud teabele.

Artikkel 2. Salastatuse tasemed

1. Poolte salastatuse tasemed ja salastusmärged vastavad üksteisele järgmiselt:

Eesti Vabariigis	Albaania Vabariigis	Ingliskeelne vaste
TÄIESTI SALAJANE	TEPER SEKRET	TOP SECRET
SALAJANE	SEKRET	SECRET
KONFIDENTSIAALNE	KONFIDENCIAL	CONFIDENTIAL
PIIRATUD	–	RESTRICTED

2. Eestis tasemel PIIRATUD salastatud teavet kaitstakse Albaanias kui teavet, mis on salastatud tasemel KONFIDENCIAL.

Artikkel 3. Riigi julgeoleku volitatud esindajad

1. Kummagi poole riigi julgeoleku volitatud esindajad on järgmised:

Eesti Vabariigi valitsus:
– Kaitseministeeriumi julgeolekuosakond

Albaania Vabariigi ministrite nõukogu:
– salastatud teabe kaitse direktoraat.

2. Riigi julgeoleku volitatud esindajad esitavad teineteisele oma ametlikud rekvisiidid.

3. Võrreldavate kaitstuse tasemete saavutamiseks ja säilitamiseks annavad riigi julgeoleku volitatud esindajad teineteisele taotluse korral teavet salastatud teabe kaitse normide, korra ja tavade kohta oma riigis.

Artikkel 4. Julgeolekupõhimõtted

1. Juurdepääs salastatud teabele võimaldatakse üksnes põhjendatud teadmismvajadusega isikutele, kellel on nõuetekohane füüsilise isiku juurdepääsuluba.

2. Vastuvõttev pool:

a) määrab salastatud teabele kokkuleppe artikli 2 kohaselt omakeelse salastatuse taseme ning tagab salastatud teabele samasuguse kaitse nagu oma samaväärsel tasemel salastatud teabele;

b) kasutab salastatud teavet üksnes ettenähtud otstarbel;

c) ei edasta salastatud teavet kolmandale isikule ilma päritolupoole kirjaliku loata;

d) austab salastatud teabega seotud intellektuaalse omandi õigusi ja ärisaladusi.

Artikkel 5. Salastatud teabe edastamine

1. Salastatud teavet edastatakse üldjuhul diplomaatiliste, sõjaväe- ja muude kulleritega, kelle poolte julgeoleku volitatud esindajad on heaks kiitnud. Vastuvõttev pool kinnitab salastatud teabe kättesaamist.

2. Suure koguse salastatud teabe edastamisel lepivad poolte julgeoleku volitatud esindajad iga kord eraldi kokku transpordivahendites, marsruudis ning julgeolekumeetmetes.

3. Salastatud teavet võib edastada kaugsidesüsteemide ja -võrkude kaudu, mis on kaitstud ja kummagi poole riigisisese õiguse kohaselt akrediteeritud.

4. Riigi julgeoleku volitatud esindajad võivad erijuhtudel leppida kokku teistes teabe edastusviisides, mis tagavad teabe kaitstuse.

5. Poolte julgeolekuasutused võivad operatiiv- või luureteavet omavahel vahetada otse riigisisese õiguse kohaselt.

Artikkel 6. Salastatud teabe märgistamine

1. Vastuvõttev pool teeb saadud salastatud teabele salastusmärke artikli 2 kohaselt.

2. Saadud salastatud teabe koopiad ja tõlked märgistatakse ja neid töödeldakse võrdselt originaalidega.

3. Teabe tähistamise nõuded kehtivad ka salastatud lepingute alusel loodud salastatud teabe kohta.

4. Kummagi poole riigi julgeoleku volitatud esindaja võib päritolupoole pädeva asutuse taotlusel muuta salastatuse taset või salastatuse kustutada. Päritolupoole riigi julgeoleku volitatud esindaja teavitab vastuvõtva poole riigi julgeoleku volitatud esindajat teabe salastatuse taseme muutmisest või salastatuse kustutamisest.

Artikkel 7. Hävitamine

1. Salastatud teave hävitatakse nii, et selle osaline või täielik taastamine on võimatu.

2. Tasemel TÄIESTI SALAJANE / TEPER SEKRET / TOP SECRET salastatud teavet ei hävitata. See tagastatakse päritolupoole riigi julgeoleku volitatud esindajale.

3. Kriisiolukorras, kui kokkuleppe alusel koostatud või edastatud salastatud teavet ei ole võimalik kaitsta ega tagastada, hävitatakse salastatud teave viivitamata. Vastuvõttev pool teatab salastatud teabe hävitamisest päritolupoole riigi julgeoleku volitatud esindajale võimalikult kiiresti.

Artikkel 8. Paljundused ja tõlked

1. Tasemel TÄIESTI SALAJANE / TEPER SEKRET / TOP SECRET salastatud teavet võib paljundada ja tõlkida üksnes päritolupoole riigi julgeoleku volitatud esindaja kirjalikul loal.

2. Kõik salastatud teabe paljundused märgistatakse originaali salastusmärkega. Paljundusi kaitstakse võrdselt originaalidega. Paljundusi tehakse üksnes ametlikuks otstarbeks vajalikul hulgal.

3. Salastatud teavet tohivad tõlkida ainult nõuetekohase juurdepääsulooga isikud. Tõlkele märgitakse originaali salastatuse tase ning sihtkeelne märges selle kohta, et tõlge sisaldab päritolupoole salastatud teavet.

Artikkel 9. Külastused

1. Riigi julgeoleku volitatud esindajate ametnikud võivad üksteist külastada, et arutada salastatud teabe kaitse korda.

2. Kui külastajad vajavad juurdepääsu salastatud teabele või ehitisele, kus salastatud teavet koostatakse, töödeldakse või hoitakse, tuleb külastuseks eelnevalt hankida vastuvõtva poole riigi julgeoleku volitatud esindaja luba.

3. Riigi julgeoleku volitatud esindajad töötavad välja ja kooskõlastavad omavahel külastuste korra.

4. Pool tagab külastajate isikuandmete kaitsmise riigisiseste õigusaktide kohaselt.

Artikkel 10. Salastatud lepingud

1. Pool, kes soovib sõlmida salastatud lepingut teise poole territooriumil asuva lepinglasega, taotleb teise poole riigi julgeoleku volitatud esindajalt kinnitust selle kohta, et lepinglasel on nõuetekohane juurdepääsuluba.

2. Riigi julgeoleku volitatud esindaja on kohustatud tagama, et kogu salastatud teave, mida edastatakse teise poole lepinglasele või koostatakse seoses salastatud lepinguga, on märgistatud võrdväärse omakeelse salastatuse tasemega. Lepinglase riigi julgeoleku volitatud esindaja taotluse korral esitab teise poole riigi julgeoleku volitatud esindaja julgeolekunõuete loetelu.

3. Taotluse korral esitab teise poole riigi julgeoleku volitatud esindaja lepinglase riigi julgeoleku volitatud esindajale teate ka selle kohta, et lepinglane kohustub täitma salastatud teabe kaitset käsitlevaid riigisiseseid õigusakte.

4. Lepinglase riigi julgeoleku volitatud esindaja kinnitab kirjalikult taotletud julgeolekunõuete loetelu kättesaamist ning edastab loetelu lepinglasele.

5. Pooled tagavad, et salastatud leping sõlmitakse või töö selle salastatud osadega algab alles pärast seda, kui lepinglane on rakendanud julgeolekumeetmed.

6. Kui riigi julgeoleku volitatud esindaja kiidab heaks salastatud alltöövõtulepingu, kohaldatakse ka selle suhtes käesolevat artiklit.

Artikkel 11. Salastatud teabe kaitse nõuete rikkumine

1. Salastatud teabe kaitse nõuete rikkumise korral, mille tulemusel teiselt poolt saadud salastatud teave satub ohtu või tekib sellekohane kahtlus, teatab selle poole riigi julgeoleku volitatud esindaja, kelle territooriumil salastatud teave ohtu sattus, teise poole riigi julgeoleku volitatud esindajale võimalikult kiiresti juhtunust ning viib läbi nõuetekohase uurimise. Teine pool võtab vajaduse korral uurimisest osa.

2. Kui salastatud teave satub ohtu kolmandas riigis, võtab lõikes 1 nimetatud meetmeid teavet edastanud poole riigi julgeoleku volitatud esindaja.

3. Teisele poolele teatatakse uurimise tulemustest ning edastatakse lõpparuanne juhtunu põhjuste ja kahju ulatuse kohta.

Artikkel 12. Kulud

Kumbki pool kannab enda kokkuleppe täitmise seotud kulud.

Artikkel 13. Lõppsätted

1. Kokkuleppe jõustub päeval, mil poolte diplomaatiliste kanalite kaudu laekub viimane kirjalik teade selle kohta, et nende riigisisestest õigusaktides kokkuleppe jõustumiseks ettenähtud nõuded on täidetud.

2. Kokkuleppe sõlmitakse määramata ajaks. Pool võib kokkuleppe lõpetada, teatades sellest teisele poolele kirjalikult kuus kuud ette.

3. Kokkuleppe lõpetamisest olenemata kaitstakse kokkuleppe alusel saadud salastatud teavet kokkuleppe kohaselt edasi, kuni päritolupool vabastab vastuvõtva poole sellest kohustusest.

4. Pool teatab teisele poolele viivitamata oma riigisiseste õigusaktide muudatustest, mis võivad mõjutada salastatud teabe kaitstmist kokkuleppe kohaselt. Sellisel juhul peavad pooled teineteisega nõu, et arutada kokkuleppe võimalikku muutmist. Seni kaitstakse salastatud teavet kokkuleppe kohaselt, välja arvatud juhul, kui päritolupool esitab kirjaliku taotluse toimida teisiti.

5. Poolte kirjalikul nõusolekul võib kokkuleppet muuta. Muudatused jõustuvad lõike 1 kohaselt.

6. Kokkuleppe tõlgendamise või kohaldamisega seotud vaidlused lahendatakse poolte nõupidamise teel, kasutamata välisvahendajate abi.

Koostatud 29. märtsil 2006 Tallinnas kahes eksemplaris eesti, albaania ja inglise keeles; kõik tekstid on autentsed. Tõlgenduserinevuste korral lähtutakse ingliskeelsest tekstist.

Eesti Vabariigi valitsuse nimel
Urmas PAET

Albaania Vabariigi ministrite nõukogu nimel
Besnik MUSTAJAJ

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA AND THE COUNCIL OF MINISTERS OF THE REPUBLIC OF ALBANIA ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Estonia and the Council of Ministers of the Republic of Albania (here in after referred to as “the Parties”),

Intending to ensure mutual protection of all classified information, which has been produced or classified in the State of one Party and transmitted to the State of the other Party,

Desiring to establish the rules of the mutual protection of classified information, which shall extend to all cooperation agreements to be concluded between the Parties and the contracts to be awarded between the individuals and legal entities of the States of the Parties, which provide for the exchange of classified information,

have agreed as follows:

Article 1. Definitions

For the purpose of this Agreement:

(1) “Classified Information” means any document or material, regardless of its form, nature or method of transmission, which, in the interests of national security and in accordance with the national laws and regulations of the Parties, require protection against breach, destruction, disclosure, loss, access by any unauthorised person or any other kind of compromise.

(2) “Receiving Party” means the Party to which the Classified Information is transmitted.

(3) “Originating Party” means the Party initiating the Classified Information.

(4) “National Security Authority” means a public entity, which, in compliance with national laws and regulations, is responsible for the protection of Classified Information and for the implementation of this Agreement.

(5) “Contractor” means an individual or a legal entity possessing the legal capacity to undertake contracts.

(6) “Classified Contract” means an agreement between two or more Contractors creating and defining enforceable rights and obligations between them, which contains or involves Classified Information.

(7) “Third Party” means an international organization or a third state (including its individuals or legal entities) that is not a Party to this Agreement.

(8) “Visitor” means an official representative of one Party who needs to visit facilities of the other Party, engaged in activities involving Classified Information.

(9) “Personnel Security Clearance” means the document granted by National Security Authority to a citizen of a Party for access to Classified Information, in accordance with national laws and regulations.

(10) “Facility Security Clearance” means the document granted by National Security Authority proving that a legal entity has the physical and organizational capability to use and deposit Classified Information, in accordance with national laws and regulations.

(11) “Need-to-know” means the necessity to have access to Classified Information in connection with official duties.

Article 2. Security Classification levels

1. The equivalents of security classification levels and classification markings of the Parties are:

In the Republic of Estonia:	In the Republic of Albania:	English equivalent:
TÄIESTI SALAJANE	TEPER SEKRET	TOP SECRET
SALAJANE	SEKRET	SECRET
KONFIDENTSIAALNE	KONFIDENCIAL	CONFIDENTIAL
PIIRATUD	–	RESTRICTED

2. Estonian Classified Information marked as “PIIRATUD” shall be protected in Albania as Classified Information marked as “KONFIDENCIAL”.

Article 3. National Security Authorities

1. The National Security Authorities of the Parties are the following:

For the Government of the Republic of Estonia:

– Security Department of the Ministry of Defence of the Republic of Estonia

For the Council of Ministers of the Republic of Albania:

– Classified Information Security Directorate

2. The National Security Authorities will provide each other with their official requisites.

3. In order to achieve and maintain comparable standards of security, the National Security Authorities will, on request, provide each other with information about the security standards, procedures and practices for safeguarding Classified Information in their States.

Article 4. Security Principles

1. Access to Classified Information shall be limited to those persons who have a “need-to-know” and hold a Personnel Security Clearance of an appropriate level.

2. The Receiving Party shall:

(a) afford Classified Information a security classification level equivalent to that stipulated in Article 2 of this Agreement and consequently provide a protection, equivalent to the national Classified Information with the corresponding security classification level;

(b) not use Classified Information for other purpose than it was provided for;

(c) not release Classified Information to a third Party without a prior written consent of the Originating Party;

(d) respect the intellectual property rights and trade secrets that are involved in Classified Information;

Article 5. Transmission of Classified Information

1. Classified Information shall be transmitted normally by means of diplomatic, military and other courier services approved by the National Security Authorities. The Receiving Party shall confirm the receipt of Classified Information.

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

3. Classified Information may be transmitted by protected telecommunication systems and networks, which have been certified according to the national laws and regulations of either Party.

4. National Security Authorities of the Parties may, in special cases, adopt other mode of transmitting the Classified Information, which assures its protection.

5. 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. Marking of Classified Information

1. The Receiving Party shall mark the received Classified Information with the corresponding classification marking pursuant to Article 2.

2. Copies and translations of the received Classified Information shall be marked and handled in the same manner as originals.

3. The marking requirements shall also apply to Classified Information generated in connection with a Classified Contract.

4. Classification level may be changed or removed by a competent authority of either Party on the request of the competent authority of the Originating Party. The competent authority of the Originating Party shall notify the competent authority of the Receiving Party of the changes or declassification.

Article 7. Destruction

1. Classified Information shall be destroyed in such a manner as to avoid its partial or total reconstruction.

2. Information marked as TÄIESTI SALAJANE / TEPER SEKRET / TOP SECRET shall not be destroyed. It shall be returned to the National Security Authority of the Originating Party.

3. In case of crisis situation, which 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 National Security Authority of the Originating Party about the destruction of Classified Information as soon as possible.

Article 8. Reproduction and Translation

1. Information marked as TÄIESTI SALAJANE / TEPER SEKRET / TOP SECRET may be translated and copied only on the written permission of the National Security Authority of the Originating Party.

2. All reproduced copies of Classified Information shall be marked with the original classification marking. Such reproduced information shall be protected as the original information. The number of copies shall be restricted to that required for official purposes.

3. All translations of classified information shall be made by individuals with a Personnel Security Clearance of an appropriate level. The translation shall be marked with the original classification marking and shall bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originating Party.

Article 9. Visits

1. Security experts of the National Security Authorities may periodically visit each other in order to discuss the procedures for the protection of Classified Information.

2. The prior approval of the National Security Authority of the host Party is required in respect of visitors if access to Classified Information or to facilities developing, handling or storing Classified Information is necessary.

3. The procedures related to visits shall be developed and agreed between National Security Authorities.

4. Each Party shall guarantee the protection of personal data of the visitors according to the national laws and regulations.

Article 10. Classified Contracts

1. A Party that considers concluding a Classified Contract with a Contractor residing in the territory of the State of the other Party shall obtain an assurance from the National Security Authority of the other Party that the proposed Contractor has a security clearance of an appropriate level.
2. The National Security Authority is responsible for ensuring that all Classified Information, which has been either released to the Contractor of the other Party or generated in connection with a Classified Contract, has been marked with an equivalent security classification level. By request of the National Security Authority of the Contractor, the National Security Authority of the other Party shall provide a security requirements list.
3. The National Security Authority of the other Party shall, on request, also provide the National Security Authority of the Contractor with a notification stating that the Contractor has undertaken to observe the national laws and regulations on the protection of Classified Information.
4. The National Security Authority of the Contractor shall confirm in writing the receipt of the requested security requirements list and forward the list to the Contractor.
5. The Parties shall ensure that a Classified Contract is concluded, or eventually, work on classified parts begins only after the Contractor has implemented security measures.
6. Should the National Security Authority approve a classified subcontract, this Article shall apply accordingly.

Article 11. Breach of Security

1. In case of a breach of security that results in a certain or suspected compromise of Classified Information, received from the other Party, the National Security Authority in whose state the compromise occurred shall inform the National Security Authority of the other Party as soon as possible and carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation.
2. In case of compromise that occurs in a state different from the Parties the National Security Authority of the transmitting Party shall take the actions as of paragraph 1 of this Article.
3. The other Party shall be informed of the results of the investigation and shall receive the final statement as to the reasons of the event and the extent of the damage.

Article 12. Expenses

Each Party shall cover its own expenses arising from the implementation of this Agreement.

Article 13. Final Provisions

1. This Agreement shall enter into force on the date of receipt of the last written notification by which the Parties inform each other through diplomatic channels that the requirements of the national laws and regulations for its entry into force have been fulfilled.
2. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party giving the other Party 6 (six) months prior written notice.
3. Notwithstanding the termination of this Agreement, all Classified Information provided 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. Each Party shall promptly notify the other Party of any amendments to its laws and regulations that would affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult to consider possible amendments to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless requested otherwise in writing by the Originating Party.
5. This Agreement may be amended on the basis of written consent of both Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.
6. Any dispute related to the interpretation or the application of this Agreement shall be settled by consultation between the Parties, without recourse to outside jurisdiction.

Done in Tallinn on 29 March 2006 in two original copies, each in Estonian, Albanian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text will prevail.

For the Government of the Republic of Estonia

Urmas PAET

**For the Council of Ministers of the Republic of
Albania**

Besnik MUSTAFAJ