No. 42271

Estonia
and
Czech Repnblic

Security Agreemeut ou protectiou of classified iuformatiou betweeu the Goverumeut of the Republic of Estouia aud the Government of the Czech Republic (with auuex). Talliuu, 29 July 2003

Eutry iuto force: *22 November 2003 by notification, in accordance with article 13*

Authentic texts: *Czech, English and Estonian*

Registratiou with the Secretariat of the United Natious: *Estonia, 13 January 2006*

Estonie
et
Répnbliqne tchèqne

Accord de sécurité relatif à la protectiou des iuformations classifiées eutre le Gouvernement de la République d'Estouie et le Gouvernement de la République tchèque (avec aunexe). Talliun, 29 juillet 2003

Entrée eu vigueur : *22 novembre 2003 par notification, conformément à l'article 13*

Textes autheutiques : *tchèque, anglais et estonien*

Euregistremeut auprès du Secrétariat des Natious Uuies : *Estonie, 13 janvier 2006*

[CZECH TEXT — TEXTE TCHÈQUE]

BEZPEČNOSTNÍ DOHODA

O VZÁJEMNÉ OCHRANĚ UTAJOVANÝCH SKUTEČNOSTÍ

mezi

VLÁDOU ESTONSKÉ REPUBLIKY

a

VLÁDOU ČESKÉ REPUBLIKY

Vláda Estonské republiky a vláda České republiky (dále jen „smluvní strany“) se v zájmu ochrany utajovaných skutečností předaných přímo či prostřednictvím veřejných nebo soukromých subjektů, jež nakládají s utajovanými skutečnostmi států smluvních stran, dohodly takto:

ČLÁNEK 1
ROZSAH PLATNOSTI

1. Tato Dohoda stanoví základní zásady pro všechny kontrakty či dohody, které mohou být v budoucnu uzavřeny mezi smluvními stranami, veřejnými či soukromými subjekty států smluvních stran, a které se budou týkat následujících oblastí:

    a) spolupráce států smluvních stran v otázkách národní obrany, bezpečnosti a vojenských záležitostí.
    b) spolupráce, prodeje vybavení a know-how, výměny informací, podniků se společnou majetkovou účastí, kontraktů či jiných vztahů mezi veřejnými subjekty, soukromými společnostmi a/nebo fyzickými osobami států smluvních stran v oblastech týkajících se národní obrany, bezpečnosti a vojenských záležitostí.

2. Tato Dohoda se nevztahuje na přímou spolupráci zpravodajských služeb států smluvních stran a předávání informací zpravodajského charakteru.

3. Tato Dohoda nesmí být žádnou ze smluvních stran využita jako nástroj k získání utajovaných skutečností, které druhá ze smluvních stran obdržela od třetí strany.

ČLÁNEK 2
DEFINICE POJMŮ

Pro účely této Dohody:

Utajovanými skutečnostmi se rozumí

a) vše, co je utajováno, ať již se jedná o ústní sdělení utajovaného obsahu, o elektromagnetický přenos utajované zprávy či o „materiál" ve smyslu definice v části b) tohoto odstavce,

b) „materiál" zahrnuje „dokumenty" ve smyslu definice v části c) tohoto odstavce a rovněž všechny součásti strojů, vybavení, zbraní či zbraňových systémů ať již vyrobených či v procesu výroby,

c) „dokumentem" se rozumí všechny formy zaznamenané informace bez ohledu na charakter záznamového média.

Kontraktem se rozumí smlouva mezi dvěma či více kontrahenty, která zakládá a vymezuje vynutitelná práva a povinnosti mezi nimi.

Utajovaným kontraktem se rozumí kontrakt, který obsahuje utajované skutečnosti.

Kontrahentem se rozumí fyzická nebo právnická osoba, která je právně způsobilá uzavřít kontrakt.

Porušením bezpečnosti utajovaných skutečností se rozumí čin nebo opomenutí v rozporu s vnitrostátními bezpečnostními právními předpisy, jehož důsledkem může být ohrožení nebo vyzrazení utajovaných skutečností.

Vyzrazením se rozumí zpřístupnění utajovaných skutečností, ať už zčásti nebo jako celku, osobám, subjektům či státům, které nemají příslušnou bezpečnostní prověrku či oprávnění k přístupu k těmto skutečnostem, popřípadě i jen vystavení utajovaných skutečností riziku takového zpřístupnění.

Bezpečnostním osvědčením a potvrzením se rozumí pozitivní rozhodnutí založené na vyšetřovacím procesu, jehož cílem je ověřit loajalitu a důvěryhodnost osoby nebo subjektu jakož i jiné bezpečnostní aspekty v souladu s vnitrostátními právními předpisy. Toto rozhodnutí umožňuje povolit takové osobě či subjektu přístup k

utajovaným skutečnostem daného stupně utajení a umožnit jim nakládání s nimi bez bezpečnostního rizika.

Potřeba být obeznámen znamená, že přístup k utajovaným skutečnostem smí být povolen pouze osobě, která má prokazatelnou potřebu se s nimi seznámit v souvislosti se svými oficiálními úkoly, v jejichž rámci byla utajovaná skutečnost předána přijímající smluvní straně.

ČLÁNEK 3
BEZPEČNOSTNÍ OCHRANA

1. V souladu s vnitrostátními právními předpisy a zvyklostmi musí obě smluvní strany podniknout příslušné kroky k zajištění ochrany utajovaných skutečností, které budou předány, obdrženy, vytvořeny či vzniknou při vývoji v rámci dohod či vztahů mezi smluvními stranami či subjekty jejich států. Smluvní strany musí poskytnout všem těmto předaným, vytvořeným či vzniklým utajovaným skutečnostem stejný stupeň bezpečnostní ochrany jaký je poskytován vlastním utajovaným skutečnostem srovnatelného stupně utajení v souladu s článkem 5 této Dohody.

2. Přístup k utajovaným skutečnostem a do prostor či zařízení, kde probíhají utajované činnosti či v nichž jsou uchovávány utajované skutečnosti, smí být povolen pouze osobám, kterým bylo vydáno příslušné bezpečnostní osvědčení a které v souvislosti se svým postavením či pracovními úkoly mají „potřebu být obeznámeny".

3. Každá ze smluvních stran musí provádět dohled nad dodržováním vnitrostátních právních předpisů a metodiky u orgánů, úřadů a zařízení ve své jurisdikci, které mají v držení, vyvíjejí, vytvářejí a/nebo používají utajované skutečnosti druhé smluvní strany. Dohledem se, kromě jiného, rozumí i inspekční návštěvy.

4. Před vydáním bezpečnostního osvědčení osoby či bezpečnostního potvrzení organizace budou příslušné úřady států smluvních stran, na základě žádosti a s přihlédnutím k vlastním vnitrostátním právním předpisům, spolupracovat během procesu prověřování svých občanů či zařízení zdržujících se nebo umístěných na území druhého státu. Za tímto účelem mohou být mezi kompetentními bezpečnostními úřady dohodnuta specifická opatření.

5. Smluvní strany budou uznávat bezpečnostní osvědčení osob a bezpečnostní potvrzení organizací vydaná v souladu s vnitrostátními právními předpisy druhého státu. Srovnatelnost bezpečnostních osvědčení a potvrzení se řídí článkem 5 této Dohody.

6. Kompetentní bezpečnostní úřady se budou navzájem informovat o změnách vzájemně uznaných bezpečnostních osvědčení osob a bezpečnostních potvrzení organizací, zejména o případech jejich odebrání či snížení jejich stupně utajení.

ČLÁNEK 4
ZPŘÍSTUPŇOVÁNÍ SKUTEČNOSTÍ

1. Smluvní strany nesmí zpřístupnit utajované skutečnosti přijaté podle této Dohody třetím stranám nebo občanům jiných států bez předchozího písemného souhlasu smluvní strany původce utajované skutečnosti. Utajované skutečnosti předané jednou smluvní stranou druhé smí být použity pouze pro stanovené účely.

2. V případě, že jedna ze smluvních stran a/nebo orgány či subjekty z jejího státu zapojené do aktivit vyjmenovaných v článku 1 zadají utajovaný kontrakt, který bude realizován na území státu druhé smluvní strany, převezme tato druhá smluvní strana, na území jejíhož státu budou aktivity na základě kontraktu probíhat, odpovědnost za nakládání s těmito utajovanými skutečnostmi v souladu se svými vnitrostátními požadavky a právními předpisy.

3. Dříve než budou kontrahentu nebo budoucímu kontrahentu ze státu přijímající smluvní strany předány jakékoliv utajované skutečnosti obdržené od druhé ze smluvních stran, přijímající smluvní strana podnikne následující opatření:

   a) zabezpečí, že takový kontrahent nebo budoucí kontrahent a jeho zařízení mají schopnost patřičným způsobem zajistit ochranu utajovaných skutečností.
   b) zabezpečí, aby kontrahent před přístupem k utajovaným skutečnostem absolvoval bezpečnostní prověrku odpovídajícího stupně utajení.
   c) zabezpečí, aby všechny osoby, které vzhledem ke svým pracovním úkolům mají potřebu přístupu k utajovaným skutečnostem, absolvovaly bezpečnostní prověrku pro odpovídající stupeň utajení.
   d) zabezpečí, aby všechny osoby, které mají přístup k utajovaným skutečnostem, podstoupily bezpečnostní školení o svých povinnostech při ochraně utajovaných skutečností a aby tento fakt písemně potvrdily.

ČLÁNEK 5
STUPNĚ UTAJENÍ

1. Utajovaným skutečnostem musí být přidělen jeden z následujících srovnatelných stupňů utajení:

ESTONSKÁ REPUBLIKA	ČESKÁ REPUBLIKA	ANGLICKÝ EKVIVALEN
TÄIESTI SALAJANE	PŘÍSNĚ TAJNÉ	TOP SECRET
SALAJANE	TAJNÉ	SECRET
KONFIDENTSIAALNE	DŮVĚRNÉ	CONFIDENTIAL
PIIRATUD	VYHRAZENÉ	RESTRICTED

2. Přijímající smluvní strana ani žádný ze subjektů jejího státu nesmí snížit ani zrušit stupeň utajení přijaté utajované skutečnosti bez předchozího písemného

souhlasu smluvní strany původce utajované skutečnosti. Smluvní strana původce bude poskytovat přijímající smluvní straně informace o jakýchkoliv změnách týkajících se stupňů utajení předaných skutečností.

3. Přijímající smluvní strana musí označit přijaté utajované skutečnosti vlastním srovnatelným stupněm utajení. Překlady a reprodukce musí být označeny stejným stupněm utajení jako původní utajované skutečnosti.

ČLÁNEK 6
KOMPETENTNÍ BEZPEČNOSTNÍ ÚŘADY

1. Kompetentními bezpečnostními úřady, odpovědnými za provádění a dohled nad všemi aspekty této Dohody jsou:

V Estonské republice:
Národní bezpečnostní úřad
Oddělení bezpečnosti
Ministerstvo obrany
Estonská republika
Sakala Str. 1
15094 Tallinn
ESTONSKO

V České republice:
Národní bezpečnostní úřad
P.O. Box 49
150 06 Praha 56
ČESKÁ REPUBLIKA

2. Oba kompetentní bezpečnostní úřady, každý v jurisdikci svého vlastního státu, musí zajistit v souladu s vlastními vnitrostátními právními předpisy náležitou ochranu utajovaných skutečností předaných dle této Dohody.

3. Každý z kompetentních bezpečnostních úřadů musí poskytnout na základě žádosti druhému kompetentnímu bezpečnostnímu úřadu informace týkající se vlastní bezpečnostní organizace a postupů, aby bylo možné porovnat a udržet stejné bezpečnostní standardy, a musí umožnit návštěvy pověřených zástupců druhé smluvní strany ve svém státě.

ČLÁNEK 7
NÁVŠTĚVY

1. Návštěvy prostor, ve kterých utajované skutečnosti vznikají, ve kterých je s nimi nakládáno či ve kterých jsou uloženy, případně prostor, kde probíhají utajované projekty, smí být povoleny návštěvníkům ze státu druhé smluvní strany pouze v případech, kdy bylo předem získáno písemné povolení kompetentního bezpečnostního úřadu státu přijímající smluvní strany. Takové povolení bude uděleno pouze osobám, kterým bylo vydáno příslušné bezpečnostní osvědčení a které splňují podmínku „potřeby být obeznámeny".

2. Kompetentní bezpečnostní úřad vysílající smluvní strany uvědomí kompetentní bezpečnostní úřad státu přijímající smluvní strany o očekávaných návštěvnících nejméně tři týdny před plánovanou návštěvou, a to v souladu s postupy uvedenými v Příloze této Dohody. Tato Příloha je nedílnou součástí Dohody. Postupy spojené s návštěvami specifikované v Příloze mohou být upraveny na základě písemného souhlasu obou kompetentních bezpečnostních úřadů.

ČLÁNEK 8
KONTRAKTY

1. Kompetentní bezpečnostní úřad státu jedné ze smluvních stran, který má v úmyslu uzavřít utajovaný kontrakt s kontrahentem na území státu druhé

smluvní strany či který má v úmyslu zmocnit některého z vlastních kontrahentů k tomu, aby v rámci utajovaného projektu zadal utajovaný kontrakt na území státu druhé smluvní strany, musí předem obdržet od kompetentního bezpečnostního úřadu státu druhé smluvní strany písemné ujištění o tom, že navrhovaný kontrahent je držitelem bezpečnostního osvědčení či potvrzení odpovídajícího stupně a disponuje prostředky pro nakládání s utajovanými skutečnostmi stejného stupně a pro jejich ukládání.

2. Každý utajovaný kontrakt mezi subjekty států smluvních stran a/nebo soukromými subjekty nebo fyzickými osobami by měl obsahovat patřičnou bezpečnostní přílohu zpracovanou podle ustanovení této Dohody a popisující utajované součásti kontraktu včetně seznamu stupňů utajení jim přiřazených.

3. Jména sub-kontrahentů ucházejících se o utajované subkontrakty musí být kontrahentem předem předložena ke schválení kompetentnímu bezpečnostnímu úřadu. Pokud bude schválen, musí sub-kontrahent splnit stejné bezpečnostní požadavky jako kontrahent.

4. Oznámení o jakémkoliv utajovaném projektu, dohodě, kontraktu nebo subkontraktu musí být předem zasláno kompetentnímu bezpečnostnímu úřadu toho státu, kde bude práce probíhat.

5. Dvě kopie bezpečnostní přílohy jakéhokoliv utajovaného kontraktu musí být zaslány kompetentnímu bezpečnostnímu úřadu toho státu, v němž bude práce probíhat.

ČLÁNEK 9
PŘEDÁVÁNÍ A PŘENOS

1. Utajované skutečnosti budou mezi smluvními stranami obvykle předávány prostřednictvím diplomatických cest.

2. Předávání utajovaných skutečností může probíhat rovněž prostřednictvím zástupců oficiálně jmenovaných úřady států obou smluvních stran. V případě potřeby mohou být takto pověřeni i zástupci soukromých subjektů zapojených do konkrétních projektů.

3. Předávání objemných předmětů či velkého množství utajovaných skutečností organizované případ od případu musí být schváleno oběma kompetentními bezpečnostními úřady.

4. Je možné použít další schválené způsoby předávání utajovaných skutečností, pokud je schválí oba kompetentní bezpečnostní úřady.

ČLÁNEK 10
PORUŠENÍ BEZPEČNOSTI

V případě porušení bezpečnosti utajovaných skutečností, které vyústí ve vyzrazení utajovaných skutečností předaných druhou smluvní stranou či touto stranou vytvořených, či pokud se bude jednat o otázky společných zájmů, kompetentní bezpečnostní úřad státu, na jehož území k vyzrazení dojde, musí bez zbytečného odkladu vyrozumět kompetentní bezpečnostní úřad státu druhé smluvní strany a podniknout příslušná opatření k patřičnému vyšetření takového incidentu. Druhá smluvní strana musí v případě potřeby při vyšetřování spolupracovat. V každém případě však musí být kompetentní bezpečnostní úřad druhé smluvní strany vyrozuměn o výsledcích vyšetřování a musí obdržet závěrečnou zprávu o příčinách a rozsahu porušení bezpečnosti.

ČLÁNEK 11
VÝDAJE

Výdaje, které smluvní straně vzniknou v souvislosti s touto Dohodou, zejména s prováděním bezpečnostních opatření zde uvedených, musí být hrazeny touto smluvní stranou.

ČLÁNEK 12
ŘEŠENÍ SPORŮ

Jakýkoliv spor týkající se výkladu či provádění této Dohody musí být řešen jednáním mezi kompetentními úřady obou států. Nebude-li možné takto dosáhnout urovnání, spor musí být řešen jednáním mezi patřičně pověřenými zástupci smluvních stran, a nesmí být předložen k vyřešení žádnému vnitrostátnímu či mezinárodnímu soudu ani jiné třetí straně.

ČLÁNEK 13
ZÁVĚREČNÁ USTANOVENÍ

1. Tato Dohoda se uzavírá na dobu neurčitou. Tato Dohoda podléhá schválení v souladu s vnitrostátními právními předpisy států obou smluvních stran a vstoupí v platnost třicet dnů poté, kdy bylo doručeno poslední z písemných oznámení informujících, že byly splněny nezbytné právní podmínky pro vstup této Dohody v platnost.

2. Platnost Dohody může každá ze smluvních stran kdykoliv ukončit písemnou výpovědí. V takovém případě bude platnost Dohody ukončena šest měsíců od data, kdy byla výpověď obdržena.

3. Změny této Dohody lze kdykoliv provést na základě písemného souhlasu obou smluvních stran. Takovéto změny vstoupí v platnost v souladu s ustanovením odstavce 1 tohoto článku.

4. V případě ukončení platnosti Dohody musí být utajované skutečnosti a předměty předané podle ustanovení této Dohody navráceny bez zbytečného odkladu druhé smluvní straně. Ostatní utajované skutečnosti a/nebo předměty musí být chráněny v souladu s ustanoveními této Dohody.

Dáno v Tallinn dne 29.07.2003 ve dvou původních vyhotoveních, každé v jazyce estonském, českém a anglickém. V případě rozdílností ve výkladu je rozhodující znění Dohody v jazyce anglickém.

Za vládu Estonské republiky	Za vládu České republiky

Příloha k Bezpečnostní dohodě o vzájemné ochraně utajovaných skutečností mezi vládou Estonské republiky a vládou České republiky

Požadavky pro návštěvy

1. Přístup k utajovaným skutečnostem a do prostor či zařízení, v nichž probíhají práce na utajovaných činnostech, kde je nakládáno s utajovanými skutečnostmi či kde jsou tyto uchovávány, smí být smluvní stranou povolen osobám ze státu druhé smluvní strany, jen pokud takové osoby splňují následující předpoklady:

    a) bylo jim kompetentním bezpečnostním úřadem či jiným kompetentním vládním orgánem vysílající smluvní strany vydáno příslušné bezpečnostní osvědčení a byly v souladu s vnitrostátními právními předpisy hostitelského státu určeny ke styku či k seznámení se s utajovanými skutečnostmi;
    b) byly oprávněny kompetentním bezpečnostním úřadem či jiným kompetentním vládním orgánem příslušného státu vykonat vyžadovanou návštěvu či návštěvy.

2. Kompetentní bezpečnostní úřad žádající smluvní strany musí uvědomit v souladu s ustanoveními této Přílohy o plánované návštěvě kompetentní bezpečnostní úřad přijímající smluvní strany a zajistit, aby tento bezpečnostní úřad obdržel žádost o návštěvu nejpozději tři týdny před vlastním uskutečněním této návštěvy či návštěv.

3. Žádost o povolení návštěvy musí obsahovat následující údaje:

    a) Jméno a příjmení, datum a místo narození návštěvníka, jeho státní příslušnost, název jeho zaměstnavatele a rovněž číslo cestovního pasu nebo jiného dokladu totožnosti návštěvníka
    b) Certifikát o bezpečnostním prověření návštěvníka a jeho platnost.
    c) Cíl a účel návštěvy nebo návštěv.

d) Předpokládané datum a délka návštěvy nebo návštěv.

e) Identifikaci styčné osoby v objektu/zařízení, jež je cílem návštěvy, předchozí kontakty a jakékoliv další informace, které mohou přispět k určení toho, zda je návštěva nebo návštěvy odůvodněné.

4. Žádosti o návštěvu budou předávány:

a) Prostřednictvím Zastupitelského úřadu Estonské republiky v Praze v případech žádostí o návštěvy estonských občanů v České republice.

b) Prostřednictvím Zastupitelského úřadu České republiky v Tallinnu v případech žádostí o návštěvy českých občanů v Estonské republice.

c) Dalšími způsoby, pokud budou schváleny oběma kompetentními bezpečnostními úřady.

5. Platnost povolení k návštěvě nesmí přesáhnout dvanáct měsíců.

[ENGLISH TEXT — TEXTE ANGLAIS]

SECURITY AGREEMENT ON PROTECTION OF CLASSIFIED INFORMATION BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA AND THE GOVERNMENT OF THE CZECH REPUBLIC

The Government of the Republic of Estonia and the Government of the Czeeh Republic, hereafter referred to as the Parties, in order to safeguard the classificd information transmitted directly or through public entities or private eompanies that deal with classified information of the States of the Parties havc agrccd on thc following:

Article 1. Applicability

1. This Agreement shall form the basis of any contract or agreement that may be concluded in the future between the Parties or public cntitics and/or private eompanies of the States of the Parties concerning the following subjccts:

a) Co-operation between the States of thc two Partics conccrning national defence, security and military issues,

b) Co-operation, sales of equipment and know-how, exehange of information, joint ventures, contracts or any other relations bctwccn public cntitics, privatc companics and/or natural persons of the States of the Parties conccrning national defenee, seeurity and military issues.

2. This Agreement does not cover dirct co-opcration bctwccn intclligenee services of both Parties and exchange of intelligenee information.

3. This Agreement shall not be invoked by either Party in order to obtain elassified information that the other Party has receivcd from a third party.

Article 2. Definitions

For the purpose of this Agreement:

Classified information means

a) any classified item, either an oral communication of classificd contcnts or electromagnetic transmission of a classified messagc, or "matcrial" as dcfincd in b) bclow,

b) the term "material" includes "documcnt" as dcfincd in c) bclow, and any item of machinery, equipment, weapon or weapon-systcms cithcr manufactured or in the process of manufacture,

c) the term "document" means any form of rccordcd information rcgardlcss of the type of recording media.

Contract means an agreement betwecn two or morc contraetors ereating and defining enforceable rights and obligations between the contractors.

Classified contract means a contract which contains or involves elassified information.

Contractor means a natural person or a legal entity possessing the legal capability to undertake contracts.

Breach of secnrity of classified information means an act or an omission contrary to national legal security regulations, the result of which may endanger or compromise classified information.

Secnrity compromise means that classified information is compromised because knowledge of it has passed, in the whole or in part, to persons or entities or states without appropriate security clearance or authority to have such access, or that it has been subjected to the risk of such passing.

Secnrity clearance means a positive determination stemming from an investigative procedure that shall ascertain the loyalty and trustworthiness of a person or entity as well as other security aspects in accordance with the national legal regulations. Such determination enables that person or entity to be granted access and permission to handle classified information on a certain level without security risk.

"Need-to-know" means that access to classified information may only be granted to a person who has a verified need to know such information in connection with his official duties, within the framework of which the information was released to the receiving Party.

Article 3. Security Protection

1. In accordance with their national laws, legal regulations and practice, both Parties shall take appropriate measures to protect classified information, which is transmitted, received, produced or developed as a result of any agreement or relation between the Parties or entities of their States. The Parties shall afford to all transmitted, produced or developed classified information the same degree of security protection as is provided to their own classified information of the equivalent level of classification, as defined in Article 5 of this Agreement.

2. Access to classified information and to locations and facilities where classified activities are performed or where classified information is stored, shall be limited only to those persons who have been granted appropriate security clearance and who, due to their functions or employment, have a "need-to-know".

3. Each Party shall supervise the observance of national security laws, legal regulations and practice by the agencies, offices and facilities within their jurisdiction that possess, develop, produce and/or use classified information of the other Party, inter alia by means of review visits.

4. On request, the relevant Authorities of the States of the Parties, taking into account their national legal regulations, will assist each other during the vetting procedures of their citizens or facilities living or located in the territory of the other State, preceding the issue of the Personnel Security Clearance and the Facility Security Clearance. In this respect, specific arrangements may be agreed on between the Competent Security Authorities.

5. The Parties shall recognise the Personnel and Facility Security Clearance issued in accordance with national laws and legal regulations of the other State. The equivalence of the security clearances shall be in compliance with Article 5 of this Agreement.

6. The Competent Security Authorities shall inform each other about changes of mutually recognised Personnel and Facility Security Clearances, particularly in cases of their withdrawal or downgrading.

Article 4. Disclosure of Classified Information

1. The Parties shall not disclose classified information received under this Agreement to third parties or citizens of other states without the prior written consent of the originating Party. Classified information transmitted from one Party to the other Party shall be used for the specified purpose only.

2. In the event that either Party and/or agencies or entities from its State, concerned with the subjects set out in Article 1, award a classified contract to be performed within the territory of the State of the other Party, then the Party of the State in which the contracted performance is taking place, shall assume responsibility for protection of such classified information in accordance with its own national standards and legal regulations.

3. Prior to any release of classified information received from the other Party to contractors or prospective contractors from the State of the receiving Party, the receiving Party shall:

a) Ensure that such contractors or prospective contractors and their facilities have the capability to protect the classified information adequately;

b) Ensure that each contractor has undergone a security check of a corresponding level before having access to classified information;

c) Ensure that all persons who, because of their duties, require access to classified information have undergone a security check of a corresponding security level;

d) Ensure that all persons having access to classified information have been appropriately security briefed about their responsibilities to protect classified information and have confirmed this in writing.

Article 5. Security Classifications

1. Classified information shall be assigned one of the following equivalent security classification levels:

ESTONIAN	CZECH	ENGLISH
TÄIESTI SALAJANE	PŘÍSNĚ TAJNÉ	TOP SECRET
SALAJANE	TAJNÉ	SECRET
KONFIDENTSIAALNE	DŮVĚRNÉ	CONFIDENTIAL
PIIRATUD	VYHRAZENÉ	RESTRICTED

2. The receiving Party and/or entities from its State shall neither downgrade the classification nor declassify the received classified information without the prior written consent of the originating Party. The originating Party shall inform the receiving Party of any changes in security classification of the transmitted information.

3. The receiving Party shall mark the received classified information with its own equivalent security classification. Translations and reproductions shall be marked with the same security classification as the originals.

Article 6. Competent Security Authorities

1. The Competent Security Authorities responsible for the implementation and supervision of all aspects of this Agreement are:

In the Repnblic of Estonia:

National Security Authority

Department of Security

Ministry of Defence

Republic of Estonia

Sakala Str. 1

15094 Tallinn

ESTONIA

In the Czech Republic:

National Security Authority

P.O. Box 49

150 06 Prague 56

CZECH REPUBLIC

2. Both Competent Security Authorities, each within the jurisdiction of its own State, shall ensure appropriate protection of classified information transmitted according to this Agreement in compliance with their national legal regulations.

3. Each Competent Security Authority shall, on request, pass to the other Competent Security Authority information about its security organisation and procedures to make it possible to compare and maintain the same security standards and shall enable visits to its state by certified officials of the other Party.

Article 7. Visits

1. Visits to premises where classified information is developed, handled or stored or where classified projects are carried out, shall only be granted to visitors from the State of the other Party in case that prior written permission from the Competent Security Authority of the State of the host Party has been obtained. Such permission shall only be granted to persons who have been granted appropriate security clearance and have a "need-to-know".

2. The Competent Security Authority of the State of the sending Party shall notify the Competent Security Authority of the State of the host Party of expected visitors at least three weeks prior to the planned visit, in accordance with the procedures defined in the Annex to this Agreement. This Annex forms an integral part to this Agreement. Visit procedures as defined in the Annex can be changed on the basis of written consent of both Competent Security Authorities.

Article 8. Contracts

1. The Competent Security Authority of the State of one Party, wishing to place a classified contract with a contractor in the State of the other Party, or wishing to authorise one of its own contractors to place a classified contract in the State of the other Party within a classified project, shall obtain a prior written assurance from the Competent Security Authority of the State of the other Party that the proposed contractor holds security clearance of an appropriate level and has the suitable facilities to handle and store classified information of the same level.

2. Every classified contract between entities of the States of the Parties and/or private companies and/or natural persons should contain an appropriate security section identifying classified aspects of the contract and a list of security classifications allocated to them, based on the terms of this Agreement.

3. Names of the subcontractors interested in classified subcontracts shall be submitted in advance by the contractor to the Competent Security Authority for approval. If approved, the subcontractor must fulfil the same security obligations as the contractor.

4. Notification of any classified project, agreement, contract or subcontract shall be forwarded in advance to the Competent Security Authority of the State where the work is to be performed.

5. Two copies of the security section of any classified contract shall be forwarded to the Competent Security Authority of the State where the work is to be performed.

Article 9. Communications and Transmissions

1. Classified information shall normally be transmitted between the Parties through the diplomatic channels.

2. Transmission of classified information can also take plaee through representatives officially appointed by the authorities of the States of both Parties. Sueh authorisation may, when required, be given to representatives of private entities engaged in specifie projeets.

3. Delivery of large items or quantities of classified information arranged on a ease by case basis shall be approved by both Competent Seeurity Authorities.

4. Other means of transmission of classified information may bc used if approved by both Competent Security Authorities.

Article 10. Breach of Security

In case of a breach of security concerning classifiеd information originating or received from the other Party that results in a security compromise or if eommon interests are involved, the Competent Security Authority of the State where the eompromise oeeurs shall inform the Competent Security Authority of the State of the other Party as soon as possible and take appropriate action to ensure that such an ineident is propcrly invcstigatcd. Thc other Party shall, if required, co-operate in the investigation. In any ease, the Competent Security Authority of the State of the other Party shall be informcd of thc rcsults of thc investigation and shall receive a final statement on the rcasons and cxtcnt of thc sccurity violation.

Article 11. Expenses

Expenses incurred to a Party with respect to this Agreement, in partieular eoneerning the implementation of security measures set herein, shall bc covcrcd by thc sclf-same Party.

Article 12. Settlement of Disputes

Any dispute regarding the interpretation or applieation of this Agreement shall be resolved by consultations between the Competent Sccurity Authorities of the Statcs or, in the case that such a settlement is impossible to reach, bctwccn duly authorisеd representatives of the Parties, and shall not be referred to any national or international tribunal or third party for settlement.

Article 13. Final Provisions

1. This Agreement is concluded for an indefinitc pcriod. This Agreement is subjcct to approval in accordance with the national legal rcgulations of thc Statcs of both Partics and shall enter into force thirty days after the last written notifieation has been reecived indicating that the necessary legal conditions for this Agrccmcnt to cntcr into forcc havc bccn fulfilled.

2. This Agreement may be terminated at any time by either Party with a written notification. In such a case the Agreement expires six months after reeeipt of this notification.

3. Amendments to the prcscnt Agreement may be made at any timc with thc conscnt of both Parties in written form. Such amendments shall enter into foree in aeeordanec with paragraph 1 of this Article.

4. In the event of termination, elassified information and/or items transmitted under the terms of this Agreement shall be returned to the othcr Party as soon as possiblc. Rcmaining classified information and/or items shall be proteeted in aeeordanee with the provisions of this Agreement.

Done in Tallinn on 29.07.2003 in two originals in the Estonian, Czcch and English languages. In the case of differcnt intcrprctations thc English version of thc Agrccmcnt shall prevail.

On behalf of the Govcrnmcnt of thc Rcpublie of Estonia:

HERMAN SIMM

On behalf of thc Govcrnmcnt of thc Czcch Rcpublic:

VLADISLAV LABUDEK

ANNEX TO THE SECURITY AGREEMENT ON PROTECTION OF CLASSIFIED INFORMATION BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA AND THE GOVERNMENT OF THE CZECH REPUBLIC

Visit Requiremeuts

1. Access to classified information and to establishments and facilities where classified activities are performed or where classified information is stored or handled, shall be allowed by one Party to visitors from the other Party only if they have been:

a) granted appropriate security clearance by the Competent Security Authority or other competent government authority of the sending Party and authorised to receive or to have access to classified information in accordance with the national legal regulations of their State;

b) authorised by the Competent Security Authority or other competent government authority of the respective State to perform the required visit or visits.

2. The Competent Security Authority of the sending Party shall notify the Competent Security Authority of the receiving Party of the planned visit in accordance with the provisions of this Annex, and shall ensure that the latter receives the visit request at least three weeks before the visit or visits take place.

3. The visit request shall include:

a) Visitor's first and last name, place and date of birth, nationality, name of employer, passport number or number of another identity document of the visitor;

b) Visitor's Personnel Security Clearance Certificate and its validity;

c) Object and purpose of the visit or visits;

d) Expected date and duration of the requested visit or visits;

e) Point of contact at the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;

4. The request shall be submitted:

a) Through the Estonian Embassy in Prague for visit requests of Estonian citizens to the Czech Republic;

b) Through the Czech Embassy in Tallinn for visit requests of Czech citizens to the Republic of Estonia;

c) Other procedures may be used if approved by both Competent Security Authorities.

5. The validity of visit authorisation shall not exceed twelve months.

[ESTONIAN TEXT — TEXTE ESTONIEN]

EESTI VABARIIGI VALITSUSE
JA
TŠEHHI VABARIIGI VALITSUSE
VAHELINE
SALASTATUD TEABE KAITSE KOKKULEPE

Eesti Vabariigi valitsus ja Tšehhi Vabariigi valitsus, edaspidi *lepingupooled*, soovides kaitsta salastatud teavet, mida lepingupooled vahetavad nii otsekanalite kui ka salastatud teabega tegelevate riigiasutuste ning eraõiguslike juriidiliste isikute ja avalik-õiguslike juriidiliste isikute kaudu, on kokku leppinud järgmises.

ARTIKKEL 1
KOHALDAMISALA

1. Käesoleva kokkuleppe alusel sõlmivad lepingupooled ja nende riigiasutused ning eraõiguslikud juriidilised isikud ja avalik-õiguslikud juriidilised isikud lepinguid ja kokkuleppeid järgmistes valdkondades:

    a) lepingupoolte koostöö riigikaitse-, julgeoleku- ja sõjandusküsimustes;
    b) lepingupoolte riigiasutuste, era- ja avalik-õiguslike juriidiliste isikute ja eraisikute koostöö; seadmete ja oskusteabe müük; teabevahetus; ühisürituste korraldamine ja lepingute sõlmimine ning muu koostöö riigikaitse, julgeoleku ja sõjanduse valdkonnas.

2. Kokkulepe ei reguleeri lepingupoolte julgeoleku- ja luureteenistuste teabevahetust.

3. Kokkuleppe alusel ei või lepingupool teiselt lepingupoolelt saada salastatud teavet, mille on edastanud kolmas isik.

ARTIKKEL 2
MÕISTED

Käesolevas kokkuleppes on mõistetel järgmine tähendus:

salastatud teave

a) suuliselt või elektrooniliselt edastatud andmed või punktis b määratletud materjal;

b) *materjalina* käsitatakse punktis c määratletud dokumenti ning valmis või tootmisjärgus masinat, seadet, relva või relvasüsteemi;

c) mis tahes salvestisekandjal olevat teavet sisaldav dokument;

leping on lepinglaste kokkulepe, milles nähakse ette lepinguosaliste õigused ja kohustused;

salastatud leping on salastatud teavet sisaldav või selle teabega sisu poolest seotud kokkulepe;

lepinglane on füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid;

salastatud teabe kaitse nõuete rikkumine on riigi julgeolekut käsitlevate õigusaktidega vastuolus olev tegu või tegevusetus, mille tõttu võib salastatud teave ohtu sattuda;

teabeleke on olukord, kus salastatud teave või selle osa on muutunud või võib muutuda kättesaadavaks isikule, asutusele või ettevõttele või riigile, kellel ei ole teabele juurdepääsu luba või volitust;

juurdepääsuluba on julgeolekukontrolli tulemusel antud õigus, mis kooskõlas riigi õigusaktidega kinnitab füüsilise või juriidilise isiku usaldusväärsust ning teisi julgeolekuaspekte. Nimetatud luba võimaldab ilma julgeolekut ohustamata anda füüsilisele või juriidilisele isikule õiguse saada ja kasutada kindla salastatuse tasemega teavet;

teadmisvajadus on isiku põhjendatud tarvidus saada salastatud teavet ametikohustuste täitmiseks; lepingupool võimaldab teavet saada teabe edastaja seatud tingimustel.

ARTIKKEL 3
SALASTATUD TEABE KAITSE

1. Lepingupool rakendab oma õigusaktide ja õiguspraktika kohaseid abinõusid, et kaitsta salastatud teavet, mida tema asutused või ettevõtted edastavad või saavad või loovad kokkuleppeid sõlmides ja muul viisil suheldes. Lepingupool kohaldab edastatud, saadud ja loodud teabele samu salastatuse taseme nõudeid, mis kehtivad tema salastatud teabe kohta artikli 5 järgi.

2. Isikule võimaldatakse saada salastatud teavet ja ta lubatakse rajatisele või muusse kohta, kus tehakse salastatud toiminguid või säilitatakse salastatud teavet, kui tal on asjakohane juurdepääsuluba ning kui tal on teadmisvajadus oma kohustuste või tööülesannete täitmiseks.

3. Lepingupool tagab kontrollkäike tehes ja muul viisil, et tema jurisdiktsiooni all olevad asutused ja ettevõtted, kes saavad, valdavad, töötlevad või kasutavad teise lepingupoole salastatud teavet, järgiksid riigi julgeolekut käsitlevaid õigusakte ja selle valdkonna õiguspraktikat.

4. Kui lepingupoole kodanik elab teise lepingupoole territooriumil või kui sellel territooriumil paikneb lepingupoole rajatis, osutab lepingupoole pädev asutus teise lepingupoole pädevale asutusele oma õigusaktide alusel abi, mis võimaldab sellel asutusel kontrollida füüsilise või juriidilise isiku usaldusväärsust ning kontrolli tulemuste põhjal väljastada juurdepääsuloa. Abi andmise kohta võivad pädevad asutused sõlmida eraldi kokkuleppe.

5. Lepingupool tunnustab füüsilise ja juriidilise isiku juurdepääsuluba, mis on väljastatud teise lepingupoole õigusaktide alusel. Juurdepääsulubade tasemed peavad olema kooskõlas artikliga 5.

6. Pädevad asutused edastavad teineteisele teabe, mis käsitleb vastastikku tunnustatud füüsilise ja juriidilise isiku juurdepääsulubade tühistamist või nende tasemete alandamist või nimetatud lubades tehtud teisi muudatusi.

ARTIKKEL 4
TEABE AVALIKUSTAMINE

1. Lepingupool ei avalikusta käesoleva kokkuleppe alusel saadud salastatud teavet kolmandale riigile ega selle kodanikule ilma teabe edastanud poole kirjaliku nõusolekuta. Ühelt lepingupoolelt teisele edastatud salastatud teavet kasutatakse kindlaksmääratud eesmärgil.

2. Kui lepingupool või artiklis 1 nimetatud valdkonnas tegutsev lepingupoole asutus või ettevõte esitab salastatud lepingu, mis tuleb täita teise lepingupoole territooriumil, vastutab teine lepingupool salastatud teabe kaitse eest kooskõlas oma õigusaktidega.

3. Lepingupool võib teiselt poolelt saadud salastatud teabe edastada oma riigis tegutsevale lepinglasele, kui ta tagab, et:

    a) lepinglase käsutuses olevad vahendid võimaldavad salastatud teavet nõuetekohaselt kaitsta;
    b) enne salastatud teabele juurdepääsu võimaldamist on lepinglasele kohaldatud asjakohase taseme julgeolekukontrolli nõudeid;
    c) salastatud teabele oma kohustuste tõttu juurdepääsu vajavale isiku suhtes on läbi viidud asjakohane julgeolekukontroll;
    d) isikule, kellel on juurdepääs salastatud teabele, on asjakohaselt selgitatud kohustust kaitsta salastatud teavet ja et isik on seda kirjalikult kinnitanud.

ARTIKKEL 5
SALASTATUSE TASEMED

1. Salastatud teave märgistatakse ühega järgmistest üksteisele vastavatest salastatuse tasemete märgetest:

EESTI KEELES	TŠEHHI KEELES	INGLISE KEELES
TÄIESTI SALAJANE	PRISNE TAJNÉ	TOP SECRET
SALAJANE	TAJNÉ	SECRET
KONFIDENTSIAALNE	DŮVERNÉ	CONFIDENTIAL
PIIRATUD	VYHRAZENÉ	RESTRICTED

2. Salastatud teabe vastuvõtnud lepingupool või lepingupoole asutus või ettevõte ei või teabe salastatuse taset muuta ega teavet avalikustada ilma teabe edastanud lepingupoole kirjaliku nõusolekuta. Teabe edastanud lepingupool teatab teabe vastuvõtnud lepingupoolele teabe salastatuse taseme kõigist muudatustest.

3. Teabe vastuvõtnud lepingupool märgistab salastatud teabe võrdväärse salastatuse taseme märkega. Tõlge ja koopia tähistatakse sama salastatuse taseme märgisega kui originaal.

ARTIKKEL 6
PÄDEVAD ASUTUSED

1. Käesoleva kokkuleppe rakendamise ja järelevalve eest vastutavad pädevad asutused on:

Eesti Vabariigis:
Riigi julgeoleku volitatud esindaja
Riigisaladuse kaitse osakond
Kaitseministeerium
Eesti Vabariik
Sakala 1
15094 Tallinn
EESTI

Tšehhi Vabariigis:
Riiklik Julgeolekuamet
Pk 49
150 06 Praha 56
TŠEHHI VABARIIK

2. Lepingupoole pädev asutus tagab kokkuleppe alusel edastatava salastatud teabe kaitse kooskõlas oma õigusaktidega.

3. Salastatuse standardite võrdlemise huvides edastab lepingupoole pädev asutus teise poole pädevale asutusele teavet oma julgeolekukorralduse ja tegevuse kohta ning võimaldab teise lepingupoole pädevatel ametnikel külastada oma riiki.

ARTIKKEL 7
KÜLASTUSED

1. Lepingupool lubab teise lepingupoole esindajal külastada salastatud teabe tootmise, töötlemise või hoidmise või salastatud projektis ettenähtud ülesannete täitmise kohta oma pädeva julgeolekuasutuse kirjalikul nõusolekul. Luba antakse isikule, kellel on asjakohane juurdepääsuluba ja kellel on teadmisvajadus.

2. Saatjariigi pädev asutus teatab kooskõlas käesoleva kokkuleppe lisas ettenähtud menetluskorraga vastuvõtjariigi pädevale asutusele külastusest vähemalt kolm nädalat ette. Nimetatud lisa on kokkuleppe lahutamatu osa. Lisas käsitletud külastuse korda võib muuta lepingupoolte pädevate asutuste kirjalikul nõusolekul.

ARTIKKEL 8
LEPINGUD

1. Kui lepingupoole pädev asutus kavatseb teise lepingupoole lepinglasega sõlmida salastatud lepingu või kui ta soovib salastatud projektis ettenähtud ülesande täitmiseks volitada oma riigi lepinglase sõlmima lepingu teise lepingupoole riigis, peab ta saama teise lepingupoole pädevalt asutuselt kirjaliku kinnituse, et lepinglasel on asjaomase tasemega juurdepääsuluba ning et lepinglasel on vahendid, mis võimaldavad selle salastatuse tasemega teavet töödelda ja säilitada.

2. Lepingupoolte asutuste ja eraettevõtete vahelises salastatud lepingus on soovitatav käsitleda salastatavat teavet ja käesoleva kokkuleppe alusel selle teabe kohta kehtestatavaid salastatuse tasemeid asjakohases jaotises.

3. Kui isikud soovivad sõlmida salastatud all-lepingu, teatab lepinglane nende nimed pädevale asutusele sellelt heakskiidu saamiseks. Kui all-leping on heaks kiidetud, täidab all-lepinglane samu julgeolekunõudeid kui lepinglane.

4. Lepingupoole pädev asutus saadab salastatud projekti koostamise kohta või kokkuleppe, lepingu või all-lepingu sõlmimise kohta teate selle lepingupoole pädevale asutusele, kus leping täidetakse.

5. Lepingupoole pädev asutus saadab salastatud lepingus julgeolekut käsitleva jaotise kaks koopiat selle lepingupoole pädevale asutusele, kus leping täidetakse.

ARTIKKEL 9

SIDEKANALID JA TEABE EDASTAMINE

1. Üldjuhul vahetavad lepingupooled salastatud teavet diplomaatiliste kanalite kaudu.

2. Lepingupooled võivad salastatud teavet edastada ka oma asutuste esindajate kaudu. Vajaduse korral võib teavet edastama volitada projektis osaleva eraõigusliku juriidilise isiku esindaja.

3. Kui lepingupool kavatseb edastada salastatud teavet suures koguses, teatab ta sellest teisele lepingupoolele ette ja teabe edastamise peavad heaks kiitma mõlema lepingupoole pädevad asutused.

4. Salastatud teabe võib edastada muul viisil, kui lepingupoolte pädevad asutused on selle heaks kiitnud.

ARTIKKEL 10

JULGEOLEKUNÕUETE RIKKUMINE

Kui lepingupool on rikkunud teiselt lepingupoolelt saadud salastatud teabe kaitse nõudeid ja seetõttu tekitanud teabelekke või muul viisil kahjustanud ühiseid huve, teatab lepingupoole pädev asutus sellest teise lepingupoole asutusele võimalikult kiiresti ning tagab, et juhtumit uuritakse. Lepingupoole taotluse korral teeb teine lepingupool temaga uurimiskoostööd. Lepingupool teavitab teise lepingupoole pädevat asutust uurimistulemustest ja edastab talle kokkuvõtte teabelekke põhjustest ja ulatusest.

ARTIKKEL 11
KULUD

Kokkuleppes ettenähtud julgeolekuabinõude rakendamise kulud ja muud kokkuleppe täitmise kulud kannab see lepingupool, kellel on kulud tekkinud.

ARTIKKEL 12
VAIDLUSTE LAHENDAMINE

Lepingupooled lahendavad kokkuleppe tõlgendamise või kohaldamise vaidluse oma pädevate asutuste konsultatsioonide teel või kui kokkuleppele sel viisil ei jõuta, siis lepingupoolte volitatud esindajate läbirääkimiste teel; vaidlust ei anta lahendada lepingupoole kohtule, rahvusvahelisele kohtule ega kolmandale isikule.

ARTIKKEL 13
LÕPPSÄTTED

1. Kokkuleppe sõlmitakse määramata ajaks. Lepingupooled kiidavad kokkuleppe heaks oma õigusaktide kohaselt ja kokkulepe jõustub selleks vajalike tingimuste täitmist kinnitava hilisema kirjaliku teate saamisest arvates kolmekümne päeva pärast.

2. Lepingupool võib kokkuleppe lõpetada kirjaliku teatega. Sellisel juhul lõpeb lepingu kehtivus teate saamisest arvates kuue kuu pärast.

3. Kokkulepet võib muuta lepingupoolte kirjalikul nõusolekul. Muudatus jõustub kooskõlas lõikega 1.

4. Kui kokkulepe lõpetatakse, tagastatakse selle alusel edastatud salastatud teave või

4. Kui kokkulepe lõpetatakse, tagastatakse selle alusel edastatud salastatud teave või ese teisele lepingupoolele võimalikult kiiresti. Muud salastatud teavet või e et kaitstakse kooskõlas kokkuleppega.

Koostatud Tallinnas 29.07.2003 kahes eksemplaris eesti, tšehhi ja inglise keeles. Tõlgendamiserisuste korral võetakse aluseks ingliskeelne tekst.

Eesti Vabariigi
valitsuse nimel

Tšehhi Vabariigi
valitsuse nimel

Eesti Vabariigi valitsuse ja Tšehhi Vabariigi valitsuse vahelise salastatud teabe kaitse kokkuleppe **lisa**

Külastusnõuded

1. Lepingupool võimaldab teise lepingupoole külastajal pääseda salastatud toiminguid tegevasse või salastatud teavet säilitavasse või töötlevasse asutusse või ehitisse juhul, kui:

    a) teise lepingupoole pädev asutus või muu pädev valitsusasutus on andnud sellele isikule asjakohase juurdepääsuloa ning isik on volitatud saama salastatud teavet kooskõlas oma riigi õigusaktidega;
    b) isiku on volitanud külastusel osalema tema riigi pädev asutus või muu pädev valitsusasutus.

2. Külastuse kavandanud lepingupoole pädev asutus teavitab teise lepingupoole pädevat asutust külastusest käesolevas lisas sätestatud korras ja tagab, et nimetatud asutus saab külastustaotluse kätte vähemalt kolm nädalat enne visiiti.

3. Külastustaotluses esitatakse järgmised andmed:

    a) külastaja ees- ja perekonnanimi, sünniaeg ja -koht, kodakondsus ning isiku tööandja nimi ja passi või muu isikut tõendava dokumendi number;
    b) isiku juurdepääsuloa andmed;
    c) külastuse objekt ja eesmärk;
    d) külastuse alguse kuupäev ja külastuse kestus;
    e) andmed kontaktisiku ja varasema suhtluse kohta ning muu teave, mille alusel on võimalik otsustada, kas külastus on põhjendatud.

4. Taotlus esitatakse:

   a) Tšehhi saatkonna kaudu Tallinnas, kui Eesti Vabariiki soovib külastada Tšehhi kodanik;

   b) Eesti saatkonna kaudu Prahas, kui Tšehhi Vabariiki soovib külastada Eesti kodanik;

   c) lepingupoolte pädevate asutuste kokkuleppel võib kasutada ka muid võimalusi.

5. Külastusluba kehtib kuni kaksteist kuud.

[TRANSLATION - TRADUCTION]

ACCORD DE SÉCURITÉ RELATIF À LA PROTECTION DES INFORMATIONS CLASSIFIÉES ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE D'ESTONIE ET LE GOUVERNEMENT DE LA RÉPUBLIQUE TCHÈQUE

Le Gouvernement de la République d'Estonie et le Gouvernement de la République tchèque, ci après dénommés les "Parties", soucieux de protéger la sécurité des informations classifiées qui sont transmises soit directement soit par le truchement d'organismes publics ou d'entreprises privées qui traitent des informations classifiées des États des Parties, conviennent comme suit :

Article premier. Champ d'application

1. Le présent Accord vise à régir tout contrat, marché ou accord qui pourrait être conclu entre les Parties ou entre des organismes publics ou des entreprises privées de leurs États respectifs dans les domaines ci-après :

a) Collaboration entre les États respectifs des deux Parties dans les domaines de la défense nationale, de la sécurité ou des affaires militaires;

b) Collaboration, cessions de matériel et de technologie, échanges d'informations, coentreprises, contrats, marchés et toutes autres relations entre des organismes publies, des entreprises privées ou des personnes physiques des États respectifs des Parties, qui ont rapport à la défense nationale, à la sécurité ou aux affaires militaires;

2. Le présent Accord ne s'applique pas à la collaboration directe entre les services de renseignement des Parties ni aux échanges d'informations issues d'activités de renseignement.

3. Aucune des Parties ne peut invoquer le présent Accord pour obtenir des informations classifiées que l'autre Partie a reçues d'un tiers.

Article 2. Définitions

Aux fins du présent Accord, les termes et expressions ci après s'entendent comme suit :

"informations classifiées" :

a) Tout objet classé, qu'il s'agisse d'une communication orale ou visuelle au contenu classé ou de la transmission électromagnétique d'un message classé, ou d'un des "matériels" définis en b) ci dessous :

b) "matériel" : tout "document" défini en c) ci dessous, ainsi que tout constituant de machine, d'équipement, d'arme ou de système d'armement, que sa fabrication soit aehevée ou en cours;

c) "document" : toute information enregistrée, quel qu'en soit la forme ou le support;

"contrat" : tout accord entre au moins deux parties, qui crée ou définit des droits et obligations exécutoires entre celles ci;

"contrat classé" : contrat qui contient ou qui a rapport à des informations classés;

"contractant" : personne physique ou morale ayant la eapaeité juridique d'exécuter un contrat ou un marché;

"infraction à la sécurité" : tout acte ou omission contraire aux règlements nationaux en matière de sécurité, qui risque de compromettre des informations classifiées;

"compromission de la sécurité" : le fait que des informations classifiées soient compromises soit parce qu'elles sont divulguées, en tout ou en partie, à des personnes, entités ou pays démunis de l'habilitation de sécurité ou du pouvoir néeessaire pour y accéder, soit parce qu'elles ont risqué d'être ainsi de divulguées;

"habilitation de sécurité" : décision, prise après enquête, attestant en conformité avee les lois et règlements nationaux de la loyauté et de la fiabilité d'une personne physique ou morale ainsi que de divers aspects relatifs à la sécurité. Cette constatation habilite ladite personne physique ou morale à avoir accès à des informations classifiées à une certaine cote de sécurité et à les manipuler sans risquer d'en eompromettre la séeurité;

"accès sélectif" : autorisation d'accéder à des informations elassifiées, qui n'est aeeordée qu'après avoir vériflé que le demandeur a besoin d'en connaître du fait de ses fonctions officielles dans le cadre desquelles ces informations ont été eommuniquées à la Partie destinataire.

Article 3. Protection de la sécurité

1. Chacune des deux Parties prend, dans le cadre de son droit interne, toutes les mesures voulues pour protéger les informations classifiées qui sont transmises, reçues, produites ou élaborées à raison de tous accords ou relations entre les Parties ou des organismes de leurs États respectifs. Les Parties accordent à la sécurité de toutes les informations ainsi transmises, reçues, produites ou élaborées la même proteetion que celle que reçoivent leurs propres informations classifiées sous une cote de séeurité équivalente telle que définie à l'article 5 du présent Accord.

2. Seules peuvent avoir accès aux informations classifiées, ainsi qu'aux sites et établissements où s'accomplissent des activités classifiées et où sont eonservées des informations classifiées, les personnes ayant besoin d'en eonnaître du fait de leurs fonctions ou activités officielles et auxquelles a été délivrée une habilitation de sécurité autorisant l'aeeès séleetif.

3. Chaque Partie veille avec la plus grande vigilanee, notamment par des visites de contrôle, à ce que ses organismes, ses administrations et ses établissements qui détiennent, élaborent, produisent ou exploitent les informations classifiées de l'autre Partie respectent sa législation, de ses règles et ses pratiques nationales en matière de sécurité.

4. Les Autorités compétentes des États des Parties se prêtent assistanee, sur simple demande et compte dûment tenu de leurs lois et règlements nationaux, aux fins des enquêtes visant à habiliter leurs citoyens et leurs établissements, vivant ou situés dans le territoire de l'autre État, et à leur attribuer une "cote de séeurité - personnel" (PSC) ou une "eote de sécurité - établissement" (FSC).

5. Chacune des Parties reconnaît les habilitations PSC et FSC attribuées en eonformité avec les lois et règlements nationaux de l'autre État. L'article 5 du présent Accord établit l'équivalence des cotes de sécurité des deux États.

6. Les Autorités compétentes en matière de sécurité se communiqucnt mutucllement les modifications apportées aux habilitation PSC et FSC délivrées en réciprocitc, notamment en cas de révocation ou de retrait.

Article 4. Divulgation d'informations classifiées

1. Les Parties ne doivent divulguer à des tiers ou à des citoyens d'autres États aueune information classifiée reçue sous l'empire du présent Accord, sauf le consentement préalable de la Partie d'origine. Les informations classifiées qui sont transmises d'une Partie à l'autre doivent être employées exclusivement aux fins prescrites.

2. Lorsque l'une des Parties ou un de ses organismes publics chargé de questions visées à l'article premier adjuge un contrat ou marché classé afin que celui ci soit exéeuté dans le territoire de l'État de l'autre Partie, cette dernière se porte responsable dc la protcction dcs informations classifiées communiquées, produites ou élaborées titre dudit eontrat ou marché, comme en disposent ses propres lois et règlements nationaux.

3. Avant de communiquer aux contractants adjudicataires ou soumissionnaires de son État des informations classifiées reçues de l'autre Partie, la Partie destinatairc s'assurc que :

a) Les contractants adjudicataires ou soumissionnaires et leurs établissements possèdent les capacités voulues pour protéger adéquatement la sécurité de ces informations elassifiées;

b) Chaque contractant a fait l'objet d'une enquête à la cote de sécuritc vouluc avant d'avoir accès à ces informations classifiées;

c) Les personnes dont les fonctions nécessitent l'accès à ces informations classifiécs ont fait l'objet d'une enquête à la cote de sécurité correspondante;

d) Toutes les personnes ayant accès à ces informations classifiées ont ctć informécs dc leurs responsabilités en matière de protection des informations classifiées et en ont attcstć par écrit.

Article 5. Cotes de sécurité

1. Les classifications de sécurité employées par les Parties sont articulécs sclon lcs équivalences suivantes :

ESTONIAN	CZECH	FRANÇAIS
TÄIESTI SALAJANE	PRISNE TAJNE	(TRÈS SECRET)
SALAJANE	TAJNE	(SECRET)
KONFIDENTSIAALNE	DŮVĚRNÉ	CONFIDENTIEL
PIIRATUD	VYHRAZENÉ	(DIFFUSION RESTREINTE)

2. La Partie destinataire et (ou) ses organismes publics ne peuvent ni abaisser la cote de sécurité ni déclassifier les informations classifiées qu'ils reçoivent, sans avoir reçu par écrit le consentement préalable de la Partie d'origine. La Partie d'origine tient la Partie destinataire au courant de toute modification apportée à la cote de sécurité des informations classifiées qu'elle lui a communiquées.

3. La Partie destinataire appose sur les informations classifiées qu'elle reçoit ses propres marques conformément aux équivalences définies au paragraphe 1. Les traductions et reproductions doivent être revêtues de marques identiques à la cote de sécurité des originaux.

Article 6. Autorités compétentes

1. Les Autorités compétentes chargées d'élaborer, de mettre en oeuvre et de superviser le présent Mémorandum d'accord dans sous aspects sont :

En Répnbliqne d'Estonie :

Autorité nationale de la sécurité

Département de la sécurité

Ministère de la défense

Sakala Str. 1

15094 Tallinn (Estonie)

En Répnbliqne tchèqne :

Autorité nationale de la sécurité

B.P. 49

150 06 Prague 56 (République tchèque)

2. Les Autorités compétentes assurent, chacune dans le ressort de son État et en conformité avec ses lois et règlements nationaux, la protection adéquate des informations classifiées qui sont communiquées en application du présent Accord.

3. Chaque Autorité compétente met l'autre au courant, sur simple demande, de son organisation et de ses procédures en matière de sécurité, afin de permettre de comparer et de maintenir les mêmes normes de sécurité, et elle autorise les agents officiels de cette autre Partie de visiter son État.

Article 7 - Visites

1. Seuls sont admis à visiter les locaux ou installations où sont élaborées, traitées ou conservées des informations classifiées, ou les établissements où sont exécutés des projets classés, les visiteurs de l'État de l'autre Partie qui ont obtenu au préalable l'autorisation écrite de l'Autorité compétente de l'État de la Partie d'accueil. L'autorisation n'est accordée qu'aux personnes à qui a été délivrée une habilitation de sécurité autorisant l'accès sélectif à raison de leur besoin d'en connaître.

2. L'Autorité compétente de l'État de la Partie d'origine annonce à l'Autorité compétente de l'État de la Partie d'accueil la venue de visiteurs avec un préavis d'au moins trois semaines et en conformité avec les procédures définies à l'annexe au présent Accord, dont elle est partie intégrante. Les procédures énoncées en annexe peuvent être modifiées par écrit du commun accord des deux Autorités compétentes.

Article 8 - Contrats

1. L'Autorité compétente de l'État d'une Partie qui souhaite adjuger un contrat classé à un contractant dans l'État de l'autre Partie, ou autoriser un des propres contractants à adjuger un contrat classé dans l'État de l'autre Partie au titre d'un projet classé, doit obtenir au préalable de l'Autorité compétente de l'État de l'autre Partie, par écrit, l'assurance que l'adjudicataire envisagé est habilité à la cote de sécurité voulue et dispose des installations appropriées pour traiter et conserver des informations classifiées à la même cote.

2. Tout contrat classé entre des organismes publics des États des Parties et (ou) des entreprises privées et (ou) des personnes physiques doit contenir une section distincte concernant la sécurité, qui définit les aspects classés du contrat, ainsi qu'une liste des cotes de sécurité qui leur sont attribuées comme en dispose le présent Accord.

3. L'adjudicataire doit présenter à l'approbation préalable de l'Autorité compétente une liste des sous traitants qui souhaitent exécuter des tranches du contrat classé. Chaque sous traitant ainsi approuvé doit satisfaire, en matière de sécurité, aux mêmes obligations que l'adjudicataire principal.

4. Tout projet, accord, contrat, ou sous contrat doit d'abord être notifié à l'Autorité compétente de l'État où il est prévu d'exécuter les travaux.

5. Le texte de la section "sécurité" de tout contrat classé doit être transmis en double exemplaire à l'Autorité compétente de l'État où il est prévu d'exécuter les travaux.

Article 9 - Communication et transmission d'informations classifiées

1. Les informations classifiées sont normalement transmises entre les Parties par la voie diplomatique.

2. Les informations classifiées peuvent aussi être transmises par le truchement de représentants officiels nommés par l'État de chacune des Parties. Au besoin, l'autorisation de ce faire peut être donnée aux représentants d'entités privées qui participent à un projet spécifique.

3. Si les informations ou objets classés à transférer sont particulièrement volumineux ou nombreux, les Autorités compétentes en approuvent la livraison au cas par cas.

4. Toute autre voie de transmission peut être employée du commun accord des deux Autorités compétentes.

Article 10 - Infraction à la sécurité

Lorsqu'une se produit une infraction qui compromet la sécurité d'informations classifiées provenant ou reçues d'une autre Partie, ou lorsque des intérêts communs sont en jeu, l'Autorité compétente de l'État où l'infraction est commise doit en informer au plus tôt l'Autorité compétente de l'État de l'autre Partie et prendre les mesures voulues pour assurer que l'incident est dûment enquêté. L'autre Partie collabore à l'enquête sur simple demande. L'Autorité compétente de l'État de l'autre Partie est en tout cas être tenue au courant des résultats de l'enquête et reçoit un exposé définitif des motifs et de l'étendue de l'infraction.

Article 11 - Dépenses

Chacune des Parties a la charge de toutes les dépenses qu'elle engage aux fins de la mise en oeuvre des mesures de sécurité prescrites par les présentes.

Article 12 - Règlement des différends

Tout différend concernant l'interprétation ou l'application du présent Accord doit être réglé par voie de consultations entre les Autorités compétentes des États ou, s'il est impossible de parvenir ainsi à un règlement, entre des représentants dûment autorisés des Parties, sans qu'aucune instance juridictionnelle nationale ou internationale ni aucune tierce partie ne puisse en être saisie.

Article 13 - Dispositions finales

1. Le présent Accord est conclu pour une période indéfinie. Il est sujet à approbation en conformité avec les lois et règlements de l'une et l'autre des Parties et il entrera en vigueur 30 jours après la réception de la dernière notification attestant que sont satisfaites les conditions juridiques prescrites pour son entrée en vigueur.

2. L'une ou l'autre des Parties peut dénoncer le présent Accord par une notification écrite, auquel cas celui ci expirera six mois après la réception de ladite notification.

3. Le présent Accord peut être modifié à tout moment du commun accord écrit des deux Parties. La modification entre alors en vigueur comme en dispose le paragraphe 1 du présent article.

4. En cas de dénonciation, chacune des Parties doit restituer dès que possible à l'autre Partie les informations et (ou) objets classés. Les autres informations et (ou) objets classés doivent être protégés comme en dispose le présent Accord.

Fait à Tallinn le 29 juillet 2003 en double exemplaire en estonien, en tchèque et en anglais. En case de divergence d'interprétation, l'anglais l'emporte.

Au nom du Gouvernement de la République d'Estonie :

HERMAN SIMM

Au nom du Gouvernement de la République tchèque :

VLADISLAV LABUDEK

ANNEXE À L'ACCORD DE SÉCURITÉ ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE D'ESTONIE ET LE GOUVERNEMENT DE LA RÉPUBLIQUE TCHÈQUE RELATIF À LA PROTECTION DES INFORMATIONS CLASSIFIÉES

Règles applicables aux visites

1. Chacune des Parties autorise l'accès de visiteurs de l'autre Partie aux informations classifiées, ainsi qu'aux sites et établissements où s'accomplissent des activités classifiées et où sont conservées des informations classifiées, exclusivement si ces visiteurs ont reçu :

a) Une habilitation de sécurité à la cote appropriée, délivrée par l'Autorité compétente ou par une autre autorité publique compétente, ainsi que l'autorisation nécessaire pour recevoir ou consulter des informations classifiées en conformité avec les lois et règlements nationaux de cet État;

b) L'autorisation de procéder à la ou aux visites nécessaires, délivrée par l'Autorité compétente ou par une autre autorité publique.

2. L'Autorité compétente de la Partie qui délègue le visiteur notifie la visite prévue à l'Autorité compétente de la Partie d'accueil comme en dispose la présente annexe et elle veille à ce que la demande soit reçue avec un préavis d'au moins trois semaines.

3. La demande d'autorisation de visite doit comprendre les renseignements suivants :

a) Nom et prénoms, date et lieu de naissance, nationalité, employeur, numéro de passeport ou autre pièce d'identité du visiteur;

b) Attestation de l'habilitation PSC du visiteur, avec mention de sa date de péremption;

c) Objet et finalité de la ou des visites;

d) Date(s) et durée(s) prévues de la ou des visites;

e) Point de contact dans l'établissement ou l'installation à visiter, contacts antérieurs et tout autre renseignement voulu pour justifier la ou les visites;

4. La demande doit être présentée :

a) À l'ambassade d'Estonie à Prague pour les visites en République tchèque de citoyens estoniens;

b) À l'ambassade de la République tchèque à Tallinn pour les visites en Estonie de citoyens tchèques;

c) Selon toute autre procédure approuvée par l'une et l'autre des deux Autorités compétentes.

5. L'autorisation de visite est valable pour une période d'au plus 12 mois.