Sveriges internationella överenskommelser

ISSN 1102-3716

Utgiven av Utrikesdepartementet

SÖ 2008: 2

Nr 2
Avtal med Bulgarien om ömsesidigt skydd och utbyte av hemliga uppgifter
Stockholm den 9 oktober 2007

Regeringen beslutade den 13 september 2007 att ingå avtalet. Avtalet trädde i kraft den 10 januari 2008.

Den på bulgariska avfattade texten finns tillgänglig på Utrikesdepartementets enhet för folkrätt, mänskliga rättigheter och traktaträtt (FMR)

SÖ 2008: 2

Avtal mellan Konungariket Sveriges regering och Republiken Bulgariens regering om ömsesidigt skydd och utbyte av hemliga uppgifter

Konungariket Sveriges regering och Republiken Bulgariens regering, i det som följer kallade "parterna",

med insikt om att det i gott samarbete också kan behöva utbytas hemliga uppgifter mellan parterna,

i syfte att skapa ett regelverk som reglerar det ömsesidiga skyddet av hemliga uppgifter och som är tillämpbart i alla framtida samarbetsavtal som kommer att implementeras mellan parterna och säkerhetsskyddsavtal i vilka uppgifter förekommer eller berörs;

har överenskommit följande:

ARTIKEL 1

DEFINITIONER

I detta avtal avser:

(1) **"Hemliga uppgifter"** – information oavsett form, slag eller överföringsmetod som har färdigtställts eller som är under färdigställande och som har placerats i informationssäkerhetsklass och som med hänsyn till rikets säkerhet, i enlighet med parternas nationella lagar och föreskrifter, skall skyddas.

(2) **"Informationssäkerhetsklass"** – den kategorisering, som enligt nationella lagar och föreskrifter, anger de hemliga uppgifternas känslighet och den behörighetsnivå som krävs för att få tillgång till dem och den grad av skydd som parterna skall tillse samt de nivåer enligt vilka uppgifterna skall märkas.

(3) **"Säkerhetsklarering"** – ett positivt beslut efter registerkontroll i syfte att utfärda försäkran om en fysisk eller juridisk persons lojalitet och pålitlighet och att övriga säkerhetshänsyn tagits i enlighet med nationella lagar och föreskrifter. Ett sådant beslut gör det möjligt att ge en fysisk eller juridisk person behörighet att hantera hemliga uppgifter på en viss nivå.

(4) **"Upprättande part"** – den part, inbegripet statliga eller privata organisationer under dess jurisdiktion, som delger hemliga uppgifter till den andra parten.

(5) **"Mottagande part"** – den part, inbegripet statliga eller privata organisationer under dess jurisdiktion, som mottar hemliga uppgifter från upprättande part.

(6) **"Behörig säkerhetsmyndighet"** – nationell säkerhetsmyndighet, som i enlighet med respektive parts nationella lagar och föreskrifter tillser efterlevnad av statens avsikter vad gäller skydd av hemliga uppgifter och som utövar tillsynen inom detta område samt andra behöriga myndigheter med ansvar för genomförandet av detta avtal. Dessa myndigheter finns förtecknade i avtalets artikel 3.

(7) **"Kontraktspart"** – fysisk eller juridisk person med rättslig förmåga att ingå avtal.

(8) **"Säkerhetsskyddsavtal"** – ett avtal mellan två eller flera avtalsparter vilket innehåller eller medför tillgång till hemliga uppgifter.

(9) **"Behovsprincipen"** – endast den som har behov av hemliga uppgifter för sitt arbete i den verksamhet där de hemliga uppgifterna förkommer.

(10) **"Tredje part"** – avser en stat eller internationell organisation som inte är part i avtalet.

(11) **"Säkerhetsöverträdelse"** – en handling eller en försummelse som bryter mot nationella lagar och föreskrifter som leder eller kan leda till obehörigt röjande, missbruk, skada, förstörande eller förlust av hemliga uppgifter, eller misstanke om att så har skett.

ARTIKEL 2

INFORMATIONSSÄKERHETSKLASSER

(1) Parterna överenskommer om att följande informationssäkerhetsklasser är likvärdiga och motsvarar de informationssäkerhetsklasser som anges i parternas respektive nationella lagar och föreskrifter:

för Konungariket Sverige: Försvarsmyndigheter	för Konungariket Sverige: andra myndigheter	Motsvarande nivå på engelska	för Republiken Bulgarien
HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	TOP SECRET	СТРОГО СЕКРЕТНО
HEMLIG/SECRET	HEMLIG	SECRET	СЕКРЕТНО
HEMLIG/CONFIDENTIAL	–	CONFIDENTIAL	ПОВЕРИТЕЛНО
HEMLIG/RESTRICTED	–	RESTRICTED	ЗА СЛУЖЕБНО ПОЛЗВАНЕ

(2) Information från Konungariket Sverige som endast bär beteckningen "HEMLIG" skall behandlas som "СЕКРЕТНО" i Republiken Bulgarien om annat inte har begärts av upprättande part.

(3) Hemliga uppgifter från Republiken Bulgarien med beteckningen för informationssäkerhetsklass "ЗА СЛУЖЕБНО ПОЛЗВАНЕ" eller "ПОВЕРИТЕЛНО", skall ges skydd på nivån "HEMLIG" av andra svenska myndigheter än försvarsmyndigheter om annat inte begärts av upprättande part.

(4) Upprättande part skall utan dröjsmål meddela mottagande part om ändringar beträffande informationssäkerhetsklass på de hemliga uppgifter som delgivits.

ARTIKEL 3

BEHÖRIGA SÄKERHETSMYNDIGHETER OCH SÄKERHETSSAMARBETE

(1) Parternas nationella säkerhetsmyndigheter är:

för Konungariket Sverige:

– Den militära säkerhetstjänsten

för Republiken Bulgarien:

– Den statliga kommissionen för informationssäkerhet

(2) Parternas nationella säkerhetsmyndigheter skall förse varandra med kontaktuppgifter till behöriga säkerhetsmyndigheter.

(3) De behöriga säkerhetsmyndigheterna skall informera varandra om nu gällande nationella lagar och föreskrifter för reglering av skydd av hemliga uppgifter.

(4) På anmodan skall behöriga säkerhetsmyndigheter, inom ramen för nationella lagar och föreskrifter bistå varandra med att genomföra säkerhetsklareringar.

(5) I syfte att säkerställa ett nära samarbete i implementeringen av detta avtal kan behöriga säkerhetsmyndigheter samråda på förfrågan från någon av parterna.

(6) Parternas säkerhetstjänster (inklusive de nationella underrättelsetjänsterna) får utbyta operativ information och underrättelseinformation direkt med varandra i enlighet med nationella lagar och föreskrifter.

ARTIKEL 4

NATIONELLA ÅTGÄRDER

(1) I enlighet med nationella lagar och föreskrifter skall parterna vidta alla nödvändiga åtgärder till skydd för de hemliga uppgifter som upprättats gemensam eller utbyts, direkt eller indirekt, genom detta avtal. Det skall säkerställas att dessa hemliga uppgifter ges likvärdigt skydd med nationella hemliga uppgifter i motsvarande informationssäkerhetsklass.

(2) Mottagande part skall vidta alla rättsliga åtgärder för att förhindra att hemliga uppgifter som har delgivits, röjs eller används för andra ändamål än vad som har angivits av upprättande part.

(3) I enlighet med dess nationella lagar och föreskrifter, får mottagande part delge hemliga uppgifter till tredje part endast under förutsättning att uttryckligt skriftligt godkännande från upprättande part har lämnats.

(4) Behörighet att ta del av hemliga uppgifter skall endast ges till personer som har erhållit vederbörlig säkerhetsklarering, har fått information om säkerhetsskydd av hemliga uppgifter och i enlighet med behovsprincipen.

(5) Parterna skall ömsesidigt erkänna respektive parts intyg om säkerhetsklarering och informera varandra om efterföljande ändringar sker i dessa.

(6) Upprättande part skall:

a) säkerställa att delgivna hemliga uppgifter är märkta med rätt nationell beteckning för informationssäkerhetsklass i enlighet med artikel 2,

b) informera mottagande part om villkor för delgivning eller begränsningar i användningen av de hemliga uppgifterna, när det är tillämpligt,

c) informera mottagande part om efterföljande ändringar av informationssäkerhetsklassningen av delgivna hemliga uppgifter.

(7) Mottagande part skall:

a) åsätta hemliga uppgifter den informationssäkerhetsklass som motsvarar den som upprättande part angivit,

b) säkerställa att klassningen inte ändras, utom i de fall skriftligt tillstånd har lämnats av upprättande part.

(8) Parterna skall i god tid informera varandra om ändringar i de nationella lagar och föreskrifter som påverkar skyddet av hemliga uppgifter. I sådana

fall skall parterna informera varandra i enlighet med stycke 3 i artikel 3, i syfte att diskutera möjliga ändringar av avtalet. Under tiden skall de hemliga uppgifterna skyddas i enlighet med avtalets föreskrifter, om annat inte skriftligen har överenskommits.

ARTIKEL 5

FÖRMEDLING AV HEMLIGA UPPGIFTER

(1) Hemliga uppgifter skall förmedlas via diplomatkurir eller militär kurir eller på annat sätt som uppfyller de krav som ställs genom parternas nationella lagar och föreskrifter. Mottagande part skall skriftligen bekräfta mottagande av hemliga uppgifter.

(2) Hemliga uppgifter får förmedlas via skyddade telekommunikationssystem, nätverk eller med andra elektromagnetiska överföringsmetoder som godkänts av behöriga säkerhetsmyndigheter och där vederbörligt intyg om godkännande i enlighet med endera partens nationella lagar och föreskrifter finns.

(3) Andra godkända sätt för förmedling av hemliga uppgifter får endast användas efter överenskommelse mellan behöriga säkerhetsmyndigheter.

ARTIKEL 6

ÖVERSÄTTNING, KOPIERING OCH FÖRSTÖRING

(1) Hemliga uppgifter med informationssäkerhetsklass "СТРОГО СЕКРЕТНО" / "HEMLIG/TOP SECRET" / "HEMLIG av synnerlig betydelse för rikets säkerhet" får endast översättas eller återges efter skriftligt medgivande från upprättande parts behöriga säkerhetsmyndighet.

(2) Översättningar av hemliga uppgifter skall märkas med motsvarande informationssäkerhetsklass som originalet.

(3) När hemliga uppgifter kopieras skall beteckning för informationssäkerhetsklass också kopieras eller återges på varje kopia. Antalet kopior skall begränsas till vad som är nödvändigt för tjänsteutövning.

(4) Upprättande part kan uttryckligen förbjuda kopiering, förändring eller förstöring av hemliga uppgifter genom att märka försändelsen med hemliga uppgifter eller genom efterföljande skriftligt meddelande. Om förstöring av hemliga uppgifter är förbjuden, skall dessa ges skydd i enlighet med den informationssäkerhetsklass de tillhör eller återsändas till upprättande part.

(5) I nödfall, där det är omöjligt att skydda eller att återsända hemliga uppgifter som har framställts eller förmedlats under detta avtal, skall de hemliga uppgifterna omedelbart förstöras. Mottagande part skall meddela upprättande parts behöriga säkerhetsmyndighet om förstöringen så snart som möjligt.

ARTIKEL 7

SÄKERHETSSKYDDSAVTAL

(1) Säkerhetsskyddsavtal skall slutas och genomföras i enlighet med varje parts nationella lagar och föreskrifter. På förfrågan från behörig säkerhetsmyndighet skall parterna tillhandahålla uppgifter om huruvida en föreslagen kontraktspart har intyg om säkerhetsklarering för angiven informationssäkerhetsklass. Om den föreslagna kontraktsparten saknar intyg om säker-

hetsklarering kan endera parternas behöriga säkerhetsmyndigheter begära att kontraktsparten säkerhetsklareras.

(2) Säkerhetsskyddsavtal skall innehålla riktlinjer för gällande säkerhetskrav och informationssäkerhetsklassning av varje del av det hemliga kontraktet. Upprättande part skall i riktlinjerna ange vilka hemliga uppgifter som kommer att delges till, eller framställas av, mottagande part.

(3) Kontrakt slutna med kontraktsparter som rör hemliga uppgifter på nivån "ЗА СЛУЖЕБНО ПОЛЗВАНЕ" / "HEMLIG/RESTRICTED" skall innehålla en för syftet relevant bestämmelse som anger en minsta nivå för åtgärder att tillämpas för skydd av hemliga uppgifter av detta slag. Säkerhetsklarering krävs inte för sådana kontrakt.

ARTIKEL 8

BESÖK

(1) Besökare kan endast ges förhandstillstånd från berörd behörig säkerhetsmyndighet i värdlandet om de är behöriga att ta del av hemliga uppgifter i enlighet med egna nationella lagar och föreskrifter och om de har behov av att ta del av hemliga uppgifter eller behörighet till anläggningar där hemliga uppgifter upprättas, hanteras eller lagras.

(2) Förfaranden för besök skall överenskommas mellan parternas berörda behöriga säkerhetsmyndigheter.

(3) Förfrågan om besök skall innehålla följande information:

a) besökarens namn, födelsedatum och -plats, pass- eller ID-kortsnummer,

b) besökarens nationalitet,

c) besökarens befattning eller titel och namn på den organisation som han eller hon företräder,

d) säkerhetsklarering för besökaren på rätt nivå,

e) syfte och planerad(e) tidpunkt(er) för besök,

f) namn på de organisationer och anläggningar som besöksförfrågan gäller.

(4) Parternas behöriga säkerhetsmyndigheter får överenskomma om att listor upprättas över behöriga personer för återkommande besök. Dessa listor kan göras giltiga för en inledande period på tolv månader. När dessa listor har godkänts av parternas behöriga säkerhetsmyndigheter, skall villkoren för de enskilda besöken beslutas direkt mellan de organisationer som skall besökas av dessa personer, i enlighet med de villkor och förutsättningar som överenskommits.

ARTIKEL 9

SÄKERHETSÖVERTRÄDELSER

(1) I händelse av säkerhetsöverträdelse skall mottagande parts nationella säkerhetsmyndighet informera upprättande parts nationella säkerhetsmyndighet snarast möjligt och inleda vederbörlig utredning. Den andra parten skall, om så krävs, samarbeta i utredningen.

(2) Upprättande part skall alltid informeras om utredningsresultatet och skall tillsändas den slutliga rapporten om skälen bakom och omfattningen av den skada som förorsakats samt om vilka åtgärder som har vidtagits.

ARTIKEL 10

KOSTNADER

Varje part skall bära sina kostnader för genomförandet av sina åtaganden på grund av detta avtal.

ARTIKEL 11

SLUTBESTÄMMELSER

(1) Detta avtal löper på obestämd tid och träder i kraft på första dagen efter mottagande av det sista meddelandet där parterna informerar varandra om att nödvändiga nationella åtgärder för ikraftträdande vidtagits.

(2) Detta avtal får ändras efter skriftligt medgivande från båda parterna. Sådana ändringar skall träda i kraft i enlighet med första stycket i denna artikel.

(3) Varje part kan häva detta avtal genom skriftligt meddelande till den andra parten. Hävandet träder i kraft sex månader efter mottagande av sådant meddelande. Om avtalet hävs skall alla hemliga uppgifter som förmedlats i enlighet med detta avtal skyddas i enlighet med vad som här föreskrivs, till dess upprättande part befriar mottagande part från detta åtagande.

(4) Tvist om tolkning eller tillämpning av detta avtal skall lösas i vänskapligt samförstånd mellan parterna utan inblandning av annan jurisdiktion.

Undertecknat i Stockholm den 9 oktober 2007 i två original, vardera på språken svenska, bulgariska och engelska, där varje text äger lika giltighet. Vid tolkningsskillnader skall den engelska texten äga företräde.

Å Konungariket Sveriges regerings vägnar
Sten Tolgfors

Å Republiken Bulgariens regerings vägnar
Tsveta Markova

Agreement between the Government of the Kingdom of Sweden and the Government of the Republic of Bulgaria on mutual protection and exchange of Classified Information

The Government of the Kingdom of Sweden and the Government of the Republic of Bulgaria, hereinafter referred to as the "Parties",

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

Desiring to create a set of rules regulating the mutual protection of Classified Information applicable to any future co-operation agreements and classified contracts, which will be implemented between the Parties, containing or involving Classified Information,

Have agreed as follows:

ARTICLE 1

DEFINITIONS

For the purpose of this Agreement:

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

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

(3) **"Security Clearance"** means a positive determination stemming from a vetting procedure that shall ascertain loyalty and trustworthiness of an individual or legal entity as well as other security aspects in accordance with national laws and regulations. Such determination enables to grant the individual or the legal entity access to Classified Information and allow them to handle Classified Information on a certain level

(4) **"Originating Party"** means the Party, including any public or private entities under its jurisdiction, which releases Classified Information to the other Party.

(5) **"Receiving Party"** means the Party, including any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party.

(6) **"Competent Security Authority"** means the National Security Authority, which in compliance with the national laws and regulations of the respective Party performs the State policy for the protection of Classified Information and exercises overall control in this sphere, as well as other competent authorities with responsibilities concerning the implementation of this Agreement. Such authorities are listed in Article 3 of this Agreement.

(7) **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude contracts.

(8) **"Classified Contract"** means a contract between two or more Contractors, which contains or provides for access to Classified Information.

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

(10) **"Third Party"** means a state or an international organisation, which is not a Party to this Agreement.

(11) **"Breach of security"** means an act or an omission contrary to the national laws and regulations, which results or may result in an unauthorised disclosure, misuse, damage, destruction or loss of Classified Information, or suspicion thereof.

ARTICLE 2

SECURITY CLASSIFICATION LEVELS

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

For the Kingdom of Sweden Defense Authorities	For the Kingdom of Sweden Other Authorities	Equivalent in English	For the Republic of Bulgaria
HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	TOP SECRET	СТРОГО СЕКРЕТНО
HEMLIG/SECRET	HEMLIG	SECRET	СЕКРЕТНО
HEMLIG/CONFIDENTIAL	–	CONFIDENTIAL	ПОВЕРИТЕЛНО
HEMLIG/RESTRICTED	–	RESTRICTED	ЗА СЛУЖЕБНО ПОЛЗВАНЕ

(2) Information from the Kingdom of Sweden bearing the sole marking of "HEMLIG" shall be treated as "СЕКРЕТНО" in the Republic of Bulgaria unless otherwise requested by the Originating Party.

(3) Classified Information of the Republic of Bulgaria, marked with the Security classification level "ЗА СЛУЖЕБНО ПОЛЗВАНЕ" or "ПОВЕРИТЕЛНО", shall be protected by other authorities than the defence authorities of the Kingdom of Sweden as "HEMLIG" unless otherwise requested by the Originating Party.

(4) The Originating Party shall without delay notify the Receiving Party of any changes to the Security classification level of released Classified Information.

ARTICLE 3

COMPETENT SECURITY AUTHORITIES AND SECURITY CO-OPERATION

(1) The National Security Authorities of the Parties are:

For the Kingdom of Sweden:

– Military Security Service

For the Republic of Bulgaria:

– State Commission on Information Security.

(2) The National Security Authorities of the Parties shall provide each other with information and contact data of the Competent Security Authorities.

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

(4) On request, the Competent Security Authorities shall, within the limits set up by their national laws and regulations, assist each other in carrying out Security Clearance procedures.

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

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

ARTICLE 4

NATIONAL MEASURES

(1) In compliance with their national laws and regulations, the Parties shall implement all appropriate measures for protection of Classified Information, which is commonly generated or exchanged either directly or indirectly under this Agreement. The same level of protection shall be ensured for such Classified Information as it is provided for the national Classified Information, with the corresponding Security classification level.

(2) The Receiving Party shall take all lawful steps to prevent the disclosure or use of Classified Information released, except for the purposes and within limitations stated by the Originating Party.

(3) Subject to its national laws and regulations, the Receiving Party may release Classified Information requested by a Third Party only with an explicit written approval of the Originating Party.

(4) Access to Classified Information shall be granted only to those individuals who have been issued an appropriate Security Clearance, briefed on Classified Information protection and in accordance with the "Need to know principle".

(5) The Parties shall mutually recognise their respective certificates of Security Clearances and inform each other about any subsequent changes in them.

(6) The Originating Party shall:

a) ensure that released Classified Information is marked with an appropriate national security classification marking according to Article 2;

b) inform the Receiving Party of any conditions of release or limitations on the use of the Classified Information, as applicable;

c) inform the Receiving Party of any subsequent changes in the Security classification level of released Classified Information.

(7) The Receiving Party shall:

a) grant Classified Information a Security classification level equivalent to that provided by the Originating Party;

b) ensure that security classifications are not altered, except if authorised in writing by the Originating Party.

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

ARTICLE 5

TRANSFER OF CLASSIFIED INFORMATION

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

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

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

ARTICLE 6

TRANSLATION, REPRODUCTION AND DESTRUCTION

(1) Classified Information with a Security classification level “HEMLIG/ TOP SECRET” / ”HEMLIG av synnerlig betydelse för rikets säkerhet” / “СТРОГО СЕКРЕТНО” shall be translated or reproduced only by written permission of the relevant Competent Security Authority of the Originating Party.

(2) All translations of Classified Information shall bear a security classification marking equal to the original.

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

(4) The Originating Party may expressly prohibit reproduction, alteration or destruction of Classified Information by marking the relevant carrier of Classified Information or sending subsequent written notice. If destruction of the Classified Information is prohibited, it shall be protected according to its Security classification level or returned to the Originating Party.

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

ARTICLE 7

CLASSIFIED CONTRACTS

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

(2) A Classified Contract shall contain guidelines on the security requirements and on the Security classification level of any element of the Classified Contract. In these guidelines the Originating Party shall specify which Classified Information will be released to or generated by the Receiving Party.

(3) Contracts placed with Contractors involving Classified Information at "HEMLIG/RESTRICTED" / "ЗА СЛУЖЕБНО ПОЛЗВАНЕ" level will contain an appropriate clause identifying the minimum measures to be applied for the protection of such Classified Information. Security Clearance for such contracts is not necessary.

ARTICLE 8

VISITS

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

(2) Visiting procedures shall be agreed between the relevant Competent Security Authorities of the Parties.

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

a) name of the visitor, date and place of birth, passport (ID card) number;

b) citizenship of the visitor;

c) position or title of the visitor and name of the organisation he/she represents;

d) Security Clearance of the visitor of appropriate classification level;

e) purpose and planned date(s) of the visit(s);

f) names of organisations and facilities requested to be visited.

(4) The Competent Security Authorities of the Parties may agree to establish lists of authorised persons to make recurring visits. Those lists may be valid for an initial period of twelve months. Once those lists have been approved by the Competent Security Authorities of the Parties, the terms of the specific visits shall be directly arranged with the appropriate authorities of the organisations to be visited by those persons, in accordance with the terms and conditions agreed upon.

ARTICLE 9

BREACH OF SECURITY

(1) In case of a Breach of security, the National Security Authority of the Receiving Party shall inform the National Security Authority of the Originating Party as soon as possible and shall initiate the appropriate investigation. The other Party shall, if required, co-operate in the investigation.

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

ARTICLE 10

EXPENSES

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

ARTICLE 11

FINAL PROVISIONS

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

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

(3) Each Party may terminate this Agreement by written notice forwarded to the other Party. The termination shall enter into force six months after the date of receipt of the notification. Notwithstanding the termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

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

Done at Stockholm on 9th October 2007 in two original copies, each in the Swedish, Bulgarian and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English language text shall prevail.

For the Government of the Kingdom of Sweden
Sten Tolgfors

For the Government of the Republic of Bulgaria
Tsveta Markova

Edita Stockholm 2008