No. 42710

Poland
and
Bulgaria

Agreement between the Government of the Republic of Poland and the Government of the Republic of Bulgaria on mutual protection and exchange of classified information. Warsaw, 7 April 2005

Entry into force: *16 March 2006 by notification, in accordance with article 12*

Authentic texts: *Bulgarian, English and Polish*

Registration with the Secretariat of the United Nations: *Poland, 12 May 2006*

Pologne
et
Bulgarie

Accord entre le Gouvernement de la République de Pologne et le Gouvernement de la République de Bulgarie relatif à la protection mutuelle et à l'échange de renseignements classifiés. Varsovie, 7 avril 2005

Entrée en vigueur : *16 mars 2006 par notification, conformément à l'article 12*

Textes authentiques : *bulgare, anglais et polonais*

Enregistrement auprès du Secrétariat des Nations Unies : *Pologne, 12 mai 2006*

[BULGARIAN TEXT — TEXTE BULGARE]

СПОРАЗУМЕНИЕ

между Правителството на Република Полша

и Правителството на Република България

за взаимна защита и обмен на

класифицирана информация

Правителството на Република Полша и правителството на Република България, наричани по-нататък "Договарящи страни",

Като целят да гарантират защитата на информацията, класифицирана в съответствие с националното законодателство на всяка от Договарящите страни и предоставена на другата Договаряща страна

Се договориха за следното:

Член 1

Определения

За целите на това Споразумение :

1) **"Класифицирана информация"** означава информацията, определена като такава съгласно националното законодателство, независимо от нейната форма, носител, начин на обективиране, създадена или в процес на създаване, която изисква защита срещу нерегламентиран достъп;
2) **"Нерегламентиран достъп до класифицирана информация"** означава всяка форма на разкриване на класифицирана информация, включително злоупотреба, увреждане, предоставяне, унищожаване, неправилно класифициране, както и всякакви други действия, водещи до нарушаване защитата й или до загуба на такава информация, както и всяко действие или бездействие, довело до узнаването й от лице, което няма съответното разрешение за това;
3) **"Разрешение за достъп"** означава документ, потвърждаващ че на лицето, на което е издаден, може да се предостави достъп до класифицирана информация в съответствие с националното законодателство на всяка от Договарящите страни;
4) **"Удостоверение за сигурност"** означава документ, потвърждаващ че на изпълнителя може да се предостави достъп до класифицирана информация във връзка с изпълнение на класифициран договор в съответствие с националното законодателство на всяка от Договарящите страни;
5) **"Класифициран договор/ Класифициран договор с подизпълнител"** означава споразумение между две или повече физически/юридически лица, което съдържа или предполага достъп до класифицирана информация;
6) **"Изпълнител/ подизпълнител"** означава физическо или юридическо лице, което има правоспособност да сключва договори или е страна по класифициран договор, попадащ под разпоредбите на това Споразумение;

7) **"Компетентен орган по сигурността"** означава орган, който в съответствие с националното законодателство на всяка от Договарящите страни, осъществява функции по защита на класифицираната информация, упражнява цялостен контрол в тази сфера, както и ръководи прилагането на това Споразумение, и е определен като такъв съгласно чл.3 пар.1 на това Споразумение;

8) **"Организационна единица"** означава всяка единица, която създава, обработва, предоставя, получава, съхранява, защитава и използва класифицирана информация в съответствие с националното законодателство на всяка от Договарящите страни и при спазване на разпоредбите на това Споразумение;

9) **"Трета страна"** означава държава или международна организация, която не е страна по това Споразумение или физическо/юридическо лице, което не притежава разрешение за достъп/удостоверение за сигурност, или на което е отказано такова разрешение/удостоверение след провеждане на съответната процедура по проучване в съответствие с националното законодателство на всяка от Договарящите страни и което не отговаря на принципа "необходимост да се знае".

Член 2

Нива на класификация за сигурност

1. Договарящите страни приемат, че следните нива на класификация за сигурност на информацията са еквивалентни и съответстват на нивата на класификация за сигурност, определени в националното законодателство на всяка от Договарящите страни.

За Република Полша	За Република България	Еквивалент на английски език
ŚCIŚLE TAJNE	СТРОГО СЕКРЕТНО	TOP SECRET
TAJNE	СЕКРЕТНО	SECRET
POUFNE	ПОВЕРИТЕЛНО	CONFIDENTIAL
ZASTRZEŻONE	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

2. Организационните единици се информират за всички случаи на промяна или премахване на нивото на класификация за сигурност на предоставената информация.

Член 3

Компетентни органи по сигурността

1. За целите на това Споразумение компетентни органи по сигурността са:
   а. За Република Полша: Ръководителят на Агенцията за вътрешна сигурност (цивилен) и ръководителят на Служба военна информация (военен);
   б. За Република България: Държавната комисия по сигурността на информацията.
2. Компетентните органи по сигурността се информират за действащото национално законодателство, регламентиращо защитата на класифицираната информация и обменят своите реквизити.
3. С цел постигане и поддържане на сходни стандарти за сигурност, компетентните органи по сигурността, си предоставят взаимно информация относно стандартите за сигурност, процедурите и практиките за защита на класифицираната информация, прилагани от всяка от Договарящите страни.
4. Компетентните органи по сигурността могат да подписват договорености по приложението на това Споразумение.

Член 4

Принципи на защита на класифицираната информация

1. В съответствие с това Споразумение и националното си законодателство, Договарящите страни предприемат съответните мерки за защита на класифицираната информация, която се предоставя или се създава в резултат на съвместни дейности или във връзка с изпълнение на класифициран договор.
2. Организационната единица-получател дава на класифицираната информация ниво на класификация за сигурност еквивалентно на определеното от Организационната единица - източник, в съответствие с принципите, залегнали в член 2 на това Споразумение.
3. Компетентните органи по сигурността взаимно се информират за настъпили промени в националното законодателство, които биха могли да повлияят върху защитата на класифицираната информация.
4. При настъпване на описаните в пар.3 промени Договарящите страни предприемат мерки, целящи извършване на съответни изменения на това Споразумение. Междувременно класифицираната информация се опазва в съответствие с клаузите на това Споразумение, доколкото няма други договорености в писмена форма.
5. Достъп до предоставена или създадена в съответствие с това Споразумение класифицирана информация се предоставя само на лица, които имат разрешение за достъп, издадено след провеждане на съответна процедура по проучване в съответствие с националното законодателство на всяка от Договарящите страни и при спазване на принципа "необходимост да се знае".
6. Организационната единица-получател не предоставя достъп до класифицирана информация на трета страна без предварителното съгласие на Организационната единица, която е определила нивото на класификация за сигурност.

7. Организационната единица-получател няма да използва класифицираната информация за цел различна от тази, за която е предоставена или създадена.

Член 5

Пренасяне на класифицирана информация

1. Класифицираната информация се пренася чрез дипломатически или военни куриери или по други начини, в съответствие с националното законодателство на всяка от Договарящите страни. Организационната единица-получател трябва писмено да потвърди, че е получила класифицираната информация.
2. Класифицираната информация се предава единствено чрез защитени телекомуникационни системи, мрежи или електромагнитни средства, които са сертифицирани в съответствие с националното законодателство на всяка от Договарящите страни.
3. Други средства за пренасяне на класифицирана информация могат да се използват, само ако са взаимно одобрени от Компетентните органи по сигурността.

Член 6

Превод, размножаване, унищожаване

1. Преводът и размножаването на класифицирана информация, маркирана с ниво на класификация ŚCIŚLE TAJNE/СТРОГО СЕКРЕТНО/TOP SECRET се извършва единствено след писмено разрешение на компетентния орган по сигурността на Договарящата страна-източник.
2. Всички преводи на класифицирана информация трябва да се извършват от лица, на които е издадено съответно разрешение за достъп. Тези преводи

носят съответен гриф за сигурност и подходяща анотация на езика, на който се преведени, в която се посочва, че преводът съдържа класифицирана информация на организационната единица - източник .

3. При размножаване на класифицирана информация, грифът за сигурност на оригинала също трябва да бъде размножен или отбелязан на всяко копие. Размножената информация се поставя под същия контрол като оригиналната информация. Броят на копията трябва да се ограничи до необходимия брой за официални цели.
4. Организационната единица - източник може изрично да забрани размножаването, видоизменянето или унищожаването на класифицирана информация чрез отбелязване върху съответния носител на класифицирана информация или чрез изпращане на последващо писмено уведомление. В този случай подлежащата на унищожаване класифицирана информация се изпраща обратно на Организационната единица – източник.
5. Класифицираната информация се унищожава или видоизменя по такъв начин, че да не може да бъде възстановена изцяло или отчасти. Класифицирана информация, маркирана с ниво на класификация ŚCIŚLE TAJNE/СТРОГО СЕКРЕТНО/TOP SECRET, не може да се унищожава или видоизменя. Такава класифицирана информация се връща на организационната единица – източник или на компетентния орган по сигурността в случай на ликвидация на организационната единица – източник.

Член 7

Класифицирани договори

1. В случай на сключване на класифициран договор с потенциален изпълнител, който пребивава, има седалище или регистрация на

територията на държавата на другата Договаряща страна, компетентният орган по сигурността на потенциалния изпълнител издава сертификат, удостоверяващ че на същия е издадено удостоверение за сигурност, отговарящо на изискуемото ниво на класификация за сигурност, както и че всички лица, чиито длъжности и задължения предполагат достъп до класифицирана информация, имат съответно разрешение за достъп.

2. Ако потенциалният изпълнител не отговаря на изискванията, посочени в пар.1, компетентният орган по сигурността, които следва да издаде сертификата, уведомява незабавно компетентния орган по сигурността на другата Договаряща страна, че при подаване на искане от нейна страна ще бъдат предприети необходимите действия за започване на процедури по проучване за издаване на удостоверение за сигурност и на разрешения за достъп.
3. Към всеки класифициран договор се прилага инструкция по сигурността. В инструкцията се указва класифицираната информация, предоставяна на или създавана от изпълнителя, определеното ниво на класификация на тази информация и различните фази на изпълнение на класифицирания договор. Копие от този документ се предоставя на компетентния орган по сигурността на всяка от Договарящите страни.
4. Класифицираният договор следва да съдържа минимални стандарти за защита на класифицираната информация, свързани с нейното създаване, предоставяне и ползване, реда за извършване на посещения и достъп до такава информация. Съдържанието на класифицирания договор следва да бъде в пълно съответствие с това Споразумение, както и с императивните разпоредби на националното законодателство на всяка от Договарящите страни.
5. Изискванията, указани в този член, се прилагат в цялост по отношение на под-изпълнителите и договорите с под-изпълнители.

Член 8

Посещения

1. Експертите по сигурността на класифицираната информация от компетентните органи по сигурността провеждат периодични срещи, на които да обсъждат мерките за защита на класифицираната информация.
2. На лица, извършващи посещение от територията на едната Договаряща страна на територията на другата Договаряща страна, се разрешава достъп до класифицирана информация в необходимия обем, както и достъп до местата, в които се създава, обработва или съхранява класифицирана информация, само след предварително получаване на писмено разрешение, издадено от компетентния орган по сигурността на съответната договаряща страна.
3. Разрешението по пар.2 се издава единствено на лица, притежаващи разрешение за достъп, издадено в съответствие с тяхното национално законодателство.
4. Исканията за посещения съдържат следната информация:
   а) цел на посещението, дати и програма на посещението;
   б) темите, съдържащи класифицирана информация, които ще се обсъждат и тяхното ниво на класификация за сигурност;
   в) име и фамилия на посетителя, дата и място на раждане, националност, номер на паспорт или на лична карта;
   г) заеманата от посетителя длъжност и наименование на организацията, която той представлява;
   д) сертификат за нивото на достъп на посетителя съобразно притежаваното от него разрешение за достъп;
   ж) наименование и адрес на обекта на посещение;
   з) име и фамилия и длъжност/длъжности на лицето/лицата, които ще бъдат посетени, ако са известни

5. Всяка Договаряща страна гарантира защитата на личните данни на лицата, които извършват посещение, в съответствие с националното си законодателство.

Член 9

Нарушаване на мерките за сигурност

1. В случай на нарушаване на мерките за сигурност в резултат на реален или възможен нерегламентиран достъп до класифицирана информация, създадена или получена в съответствие с разпоредбите на това Споразумение, компетентният орган по сигурността на Договарящата страна, на чиято територия е възникнало събитието, информира незабавно компетентния орган по сигурността на другата Договаряща страна и предприема необходимите мерки, целящи ограничаване до минимум на последиците от подобно нарушение.
2. В случаите, когато нарушаването на мерките за сигурност може да засегне защитата на класифицираната информация, създадена или предоставена в съответствие с разпоредбите на това Споразумение, Договарящата страна, на чиято територия е възникнало нарушението, предприема съответното разследване в съответствие с нейното национално законодателство.
3. Компетентния орган по сигурността на Договарящата страна, на чиято територия е възникнало нарушаването на мерките за сигурност, информира незабавно компетентния орган по сигурността на другата Договаряща страна за резултатите от разследването по пар.2.

Член 10

Разходи

Всяка Договаряща страна покрива своите разходи, възникнали във връзка с изпълнение на задълженията й по това Споразумение.

Член 11

Разрешаване на спорове

Всеки спор, свързан с тълкуването или приложението на това Споразумение, се решава чрез преговори между Договарящите страни, ако предварителните консултации между компетентните органи по сигурността са завършили без резултат.

Член 12

Заключителни разпоредби

1. Това Споразумение влиза в сила след изтичане на четиринадесет дни от датата на получаване на последната дипломатическа нота, потвърждаваща изпълнението на всички процедури, предвидени в националното законодателство на всяка от Договарящите страни.
2. Това Споразумение се сключва за неопределен период от време.
3. Всяка Договаряща страна може да денонсира това Споразумение с дипломатическа нота, изпратена до другата Договаряща страна. Денонсирането влиза в сила след изтичането на шест месеца, считано от датата на получаване на такава дипломатическа нота. Независимо от прекратяването на Споразумението, цялата класифицирана информация, предоставена по Споразумението, продължава да бъде защитавана съгласно горепосочените разпоредби, до момента в който една от Договарящите страни не освободи другата Договаряща страна от това задължение.
4. Това Споразумение може да бъде изменяно по взаимно съгласие на Договарящите страни, изразено в писмена форма. Измененията влизат в сила в съответствие с разпоредбата на пар.1.

Подписано във Варшава, на 7 април 2005 година, в два оригинални екземпляра, всеки от които на полски, български и английски език, като трите текста имат еднаква сила. В случай на различия при тълкуването, за меродавен се счита английският текст.

ЗА ПРАВИТЕЛСТВОТО НА РЕПУБЛИКА ПОЛША

ЗБИГНЕВ ГОШЧИНСКИ

Заместник директор на Агенцията по вътрешна сигурност

ЗА ПРАВИТЕЛСТВОТО НА РЕПУБЛИКА БЪЛГАРИЯ

ЦВЕТА МАРКОВА

Председател на Държавната комисия по сигурността на информацията

[ENGLISH TEXT — TEXTE ANGLAIS]

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

The Government of the Republic of Poland and the Government of the Republic of Bulgaria, hereinafter referred to as the "Contracting Parties",

Aiming to ensure the protection of all the information which has been classified pursuant to the internal legislation of each of the Contracting Parties and transferred to the other Contracting Party

Have agreed as follows:

Article 1. Definitions

For the purpose of this Agreement,

1) "Classified Information" means all legally defined information, irrespective of its form, carrier, manner of expression, either generated or in process of generation, which requires protection against unauthorised access;

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

3) "Personnel Security Clearance" means a document confirming that its holder may be granted access to Classified Information in accordance with the internal legislation of each of the Contracting Parties;

4) "Industrial Security Clearance" means a document confirming that the Contractor may be granted access to Classified Information in connection with a Classified Contract and in accordance with the internal legislation of each of the Contracting Parties;

5) "Classified Contract/Subcontract" means an agreement between two or more persons/legal entities which contains or provides for access to Classified Information;

6) "Contractor/Subcontractor" means a person or a legal entity possessing the legal capacity to conclude contracts or a party to a Classified Contract under the provisions of this Agreement;

7) "Competent Security Authority" means the authority which, in compliance with the internal legislation of each of the Contracting Parties, performs functions regarding the protection of Classified Information, exercises overall control in this sphere as well as conducts the implementation of this Agreement, and is determined as such in Article 3 Paragraph 1 of this Agreement;

8) "Organisational Unit" means an entity which generates, processes, transfers, receives, stores, protects and uses Classified Information in accordance with the internal legislation of each of the Contracting Parties and in compliance with this Agreement;

9) "Third Party" means a state or international organization which is not a Party to this Agreement or any person/legal entity who does not have a Personnel Security Clearance/Industrial Security Clearance or who was refused such a Clearance after conducting a vetting procedure in accordance with the internal legislation of each of the Contracting Parties and who does not have a need-to-know.

Article 2. Security Classification Levels

1. The Contracting Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the internal legislation of each of the Contracting Parties.

For the Republic of Poland	For the Republic of Bulgaria	Equivalent in English
ŚCIŚLE TAJNE	СТРОГО СЕКРЕТНО	TOP SECRET
TAJNE	СЕКРЕТНО	SECRET
POUFNE	ПОВЕРИТЕЛНО	CONFIDENTIAL
ZASTRZEŻONE	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

2. The Organisational Units shall inform each other of any case of change or removal of the security classification level of the transferred information.

Article 3. Competent Security Authorities

1. For the purpose of this Agreement, the Competent Security Authorities shall be:
   a. for the Republic of Poland: the Head of the Internal Security Agency (civilian) and the Head of the Military Information Services (military);
   b. for the Republic of Bulgaria: the State Commission on Information Security.

2. The Competent Security Authorities shall inform each other of their internal legislation in force regulating the protection of Classified Information and shall exchange their requisites.

3. In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall provide each other with information about the security standards, procedures and practices for protection of Classified Information applied by each of the Contracting Parties.

4. The Competent Security Authorities can sign executive arrangements with regard to the implementation of this Agreement.

Article 4. Principles of the Protection of Classified Information

1. In compliance with this Agreement and their internal legislation, the Contracting Parties shall implement appropriate measures for protection of Classified Information which is transferred or generated as a result of their mutual activities or in connection with a Classified Contract.

2. The Receiving Organisational Unit shall afford Classified Information a security classification level equivalent to that provided by the Originating Organisational Unit in accordance with the principle set forth in Article 2 of this Agreement;

3. The Competent Security Authorities shall inform each other about any changes in the internal legislation affecting the protection of Classified Information.

4. In the case referred to in Paragraph 3, the Contracting Parties shall undertake measures aimed at the introduction of appropriate changes to this Agreement.

Meanwhile, the Classified Information shall be protected according to the provisions of this Agreement, unless otherwise agreed in writing.

5. Access to Classified Information transferred or generated in accordance with this Agreement shall be granted only to persons who have a Personal Security Clearance, issued after conducting an appropriate vetting procedure in accordance to the internal legislation of each of the Contracting Parties and who have a need - to - know.

6. The Receiving Organisational Unit shall not allow access to the Classified Information to a Third Party without a prior consent of the Originating Organisational Unit who imposed the security classification.

7. The Receiving Organisational Unit shall not use the Classified Information for purposes other than those for which it was transferred or generated.

Article 5. Transfer of Classified Information

1. Classified Information shall be transferred by means of diplomatic or military couriers or by other means in accordance with the internal legislations of each of the Contracting Parties. The Receiving Organisational Unit shall confirm in writing the receipt of the Classified Information.

2. Classified Information shall be transmitted via protected telecommunication systems, networks or electromagnetic means which have been granted a certificate issued pursuant to the internal legislation of each of the Contacting Parties.

3. Other means of transfer of Classified Information may also be used if mutually approved by the Competent Security Authorities.

Article 6. Translation, reproduction, destruction

1. Classified Information marked with a classification level ŚCIŚLE TAJNE/СТРОГО СЕКРЕТНО/TOP SECRET shall be translated or copied only by written permission of the Competent Security Authority of the Originating Contracting Party.

2. All translations of Classified Information shall be made by persons who have appropriate Personnel Security Clearance. Such translation shall bear an appropriate security classification marking and a suitable annotation in the language of translation indicating that the translation contains Classified Information of the Originating Organisational Unit.

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

4. The Originating Organisational Unit may expressly prohibit reproduction, alteration or destruction of Classified Information by marking the relevant carrier or sending subsequent written notice. In such case, the Classified Information subject to destruction shall be returned to the Originating Organisational Unit.

5. Classified Information shall be destroyed or modified insofar as to forestall its reconstruction in whole or in part. Classified Information marked as ŚCIŚLE TAJNE/СТРОГО СЕКРЕТНО/TOP SECRET shall not be destroyed or modified. Instead it shall be returned to the Originating Organisational Unit or to the Competent Security Authority in case of liquidation of the Originating Organisational Unit.

Article 7. Classified Contracts

1. In case a Classified Contract with a potential Contractor residing or having its seat or registered in the territory of the State of the other Contracting Party is to be concluded, the Competent Security Authority for the potential Contractor shall issue a document certifying that it has been granted the Industrial Security Clearance corresponding to the required security classification level and that all of its personnel whose positions and duties require access to Classified Information have been granted the appropriate Personnel Security Clearance.

2. If the potential Contractor does not meet the requirements referred to in Paragraph 1, the Competent Security Authority which is to issue the certifying document, shall imme-

diately inform the Competent Security Authority of the other Contracting Party that, upon its request, necessary actions shall be taken to start the vetting procedures for issuance of Industrial Security Clearance and Personnel Security Clearances.

3. Each Classified Contract shall be accompanied by a security instruction. This instruction shall specify the Classified Information released to or generated by the Contractor, the classification level assigned to this information and the different phases of the execution of the Classified Contract. A copy of this document shall be submitted to the Competent Security Authority of each of the Contracting Parties.

4. The Classified Contract must contain minimum measures for protection of Classified Information regarding generation, transfer and usage of the Classified Information, visits procedures and access to such information. It must be in full conformity with this Agreement and the imperative provisions of the internal legislation of each of the Contracting Parties.

5. The requirements set forth in this Article shall also fully apply respectively to subcontracts and Subcontractors.

Article 8. Visits

1. Experts on Classified Information protection of the Competent Security Authorities shall hold regular meetings to discuss the measures for protection of Classified Information.

2. Persons arriving on a visit from the territory of one of the Contracting Parties to the territory of the other Contracting Party shall be allowed access to Classified Information to the necessary extent, as well as to the premises where Classified Information is generated, handled or stored, only after prior receipt a written permit issued by the Competent Security Authority of the respective Contracting Party.

3. The permit referred to in Paragraph 2, shall be granted exclusively to persons granted a Personnel Security Clearance pursuant to their internal legislation.

4. Requests for visits shall include information concerning:

a. purpose, date and programme of the visit;

b. issues relating to Classified Information that are to be discussed and level of their security classification;

c. name and surname of the proposed visitor, date and place of birth, nationality and passport number or identity card number;

d. position of the visitor together with the name of the institution or facility which he or she represents;

e. certification of the level of Personnel Security Clearance held by the visitor;

f. name and address of the facility to be visited;

g. name, surname and position(s) of the person(s) to be visited, if known.

5. Each Contracting Party shall guarantee the protection of personal data of the visitors, according to its internal legislation.

Article 9. Breach of Security Regulations

1. In case of a breach of security regulations resulting from unauthorized access or a risk of unauthorized access to Classified Information generated or transferred in accordance with this Agreement, the Competent Security Authority of the Contracting Party on whose territory such event occurred shall immediately inform the Competent Security Authority of the other Contracting Party and it shall take necessary measures aimed at minimizing effects of such breach.

2. In case of a breach of security regulations which might affect the protection of Classified Information generated or transferred in accordance with this Agreement, the Contracting Party on whose territory such breach occurred, shall take up appropriate investigation in compliance with its internal legislation.

3. The Competent Security Authority of the Contracting Party on whose territory the breach of security regulations occurred shall immediately inform the Competent Security Authority of the other Contracting Party of the result of the investigation referred to in Paragraph 2.

Article 10. Expenses

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

Article 11. Settlement of Disputes

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by way of negotiations between the Contracting Parties, if the prior consultations between Competent Security Authorities turn out to be ineffective.

Article 12. Final Provisions

1. This Agreement shall enter into force fourteen days after the receipt of the last diplomatic note confirming the fulfilment of all the procedures provided for by the internal legislation of each of the Contracting Parties.

2. This Agreement is concluded for an indefinite period of time.

3. Each of the Contracting Parties may denounce this Agreement by diplomatic note forwarded to the other Contracting Party. The denunciation shall enter into force six months after the date of receipt of such diplomatic note.

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 one of the Contracting Parties dispenses the other Contracting Party from this obligation.

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

Done at Warsaw on 7 April 2005 in two original copies, each in the Polish, Bulgarian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

For the Government of the Republic of Poland :

ZBIGNIEW GOSZCZYNSKI
Deputy Head of Internal Security Agency

For the Government of the Republic of Bulgaria :

CWETA MARKOWA
Chairperson of the State Commission on Information Security

[POLISH TEXT — TEXTE POLONAIS]

UMOWA

między Rządem Rzeczypospolitej Polskiej

a Rządem Republiki Bułgarii

w sprawie wzajemnej ochrony i wymiany

informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Republiki Bułgarii,

zwane dalej „Umawiającymi się Stronami",

mając na celu zapewnienie ochrony wszystkich informacji,

które zostały zaklasyfikowane jako informacje niejawne zgodnie z prawem

wewnętrznym każdej z Umawiających się Stron

i przekazane drugiej Umawiającej się Stronie,

uzgodniły, co następuje:

Artykuł 1

Definicje

Dla celów niniejszej Umowy:

1) **„informacja niejawna"** oznacza wszelką określoną prawem informację, niezależnie od formy, nośnika oraz sposobu wyrażenia, wytworzoną lub będącą w trakcie wytwarzania, która wymaga ochrony przed nieuprawnionym dostępem;
2) **„nieuprawniony dostęp do informacji niejawnych"** oznacza każdą formę ujawnienia informacji niejawnych, w tym niewłaściwe wykorzystanie, uszkodzenie, przekazanie, zniszczenie, niewłaściwe zaklasyfikowanie, a także wszelkie inne działania, których skutkiem jest naruszenie ochrony lub utrata takiej informacji, jak również inne działania lub zaniechania, których rezultatem jest zapoznanie się z takimi informacjami osoby nieuprawnionej;
3) **„poświadczenie bezpieczeństwa"** oznacza dokument potwierdzający, że jego posiadacz może uzyskać dostęp do informacji niejawnych, zgodnie z prawem wewnętrznym każdej z Umawiających się Stron;
4) **„świadectwo bezpieczeństwa przemysłowego"** oznacza dokument potwierdzający, że kontrahent może uzyskać dostęp do informacji niejawnych w związku z kontraktem niejawnym i zgodnie z prawem wewnętrznym każdej z Umawiających się Stron;
5) **„kontrakt niejawny/kontrakt zawarty z podwykonawcą"** oznacza umowę między dwoma lub więcej osobami fizycznymi lub prawnymi, która zawiera informacje niejawne lub wiąże się z dostępem do nich;
6) **„kontrahent/podwykonawca"** oznacza osobę fizyczną lub prawną, posiadającą zdolność prawną do zawierania kontraktów lub stronę kontraktu niejawnego zgodnie z postanowieniami niniejszej Umowy;
7) **„właściwy organ bezpieczeństwa"** oznacza organ, który zgodnie z prawem wewnętrznym każdej z Umawiających się Stron, wykonuje funkcje w zakresie ochrony informacji niejawnych, przeprowadza całościową kontrolę w tym

zakresie, jak również wykonuje niniejszą Umowę i jest określony w artykule 3 ustęp 1 niniejszej Umowy;

8) **„jednostka organizacyjna"** oznacza podmiot, który wytwarza, przetwarza, przekazuje, otrzymuje, przechowuje, chroni i wykorzystuje informacje niejawne zgodnie z prawem wewnętrznym każdej z Umawiających się Stron oraz na podstawie niniejszej Umowy;

9) **„strona trzecia"** oznacza państwo lub organizację międzynarodową, która nie jest stroną niniejszej Umowy lub jakąkolwiek osobę fizyczną bądź prawną, która nie posiada poświadczenia bezpieczeństwa lub świadectwa bezpieczeństwa przemysłowego albo której odmówiono takiego poświadczenia lub świadectwa, po przeprowadzeniu postępowania sprawdzającego, zgodnie z prawem wewnętrznym każdej z Umawiających się Stron oraz której zadania nie wymagają zapoznania się z informacjami niejawnymi.

Artykuł 2

Poziomy tajności

1. Umawiające się Strony uzgadniają, że poniższe poziomy tajności są równoważne i odpowiadają klauzulom tajności, określonym w prawie wewnętrznym każdej z Umawiających się Stron:

w Rzeczypospolitej Polskiej	w Republice Bułgarii	odpowiednik w języku angielskim
ŚCIŚLE TAJNE	СТРОГО СЕКРЕТНО	TOP SECRET
TAJNE	СЕКРЕТНО	SECRET
POUFNE	ПОВЕРИТЕЛНО	CONFIDENTIAL
ZASTRZEŻONE	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED

2. Jednostki organizacyjne powiadamiają się wzajemnie o każdym przypadku zmiany lub zniesienia poziomu tajności przekazywanych informacji.

Artykuł 3

Właściwe organy bezpieczeństwa

1. Właściwymi organami bezpieczeństwa, dla celów niniejszej Umowy są:
   a. w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego (w sferze cywilnej) i Szef Wojskowych Służb Informacyjnych (w sferze wojskowej);
   b. w Republice Bułgarii: Państwowa Komisja do spraw Bezpieczeństwa Informacji.
2. Właściwe organy bezpieczeństwa informują się wzajemnie o przepisach obowiązujących w ich Państwach, regulujących ochronę informacji niejawnych i wymieniają między sobą dane kontaktowe.
3. W celu osiągnięcia i utrzymania porównywalnych standardów bezpieczeństwa właściwe organy bezpieczeństwa przekazują sobie wzajemnie informacje o standardach bezpieczeństwa, procedurach i praktyce w zakresie ochrony informacji niejawnych, stosowanych przez każdą z Umawiających się Stron.
4. Właściwe organy bezpieczeństwa mogą podpisywać porozumienia wykonawcze w odniesieniu do wykonywania niniejszej Umowy.

Artykuł 4

Zasady ochrony informacji niejawnych

1. Zgodnie z niniejszą Umową i swoim prawem wewnętrznym, Umawiające się Strony wdrażają odpowiednie środki w celu ochrony informacji niejawnych, które są przekazywane lub wytwarzane w wyniku wspólnych działań lub w związku z kontraktem niejawnym.

2. Otrzymująca jednostka organizacyjna przyznaje informacjom niejawnym klauzulę tajności równoważną do przyznanej przez wytwarzającą jednostkę organizacyjną, zgodnie z zasadą określoną w artykule 2 niniejszej Umowy.
3. Właściwe organy bezpieczeństwa informują się wzajemnie o wszelkich zmianach w prawie wewnętrznym mających wpływ na ochronę informacji niejawnych.
4. W przypadku określonym w ustępie 3 Umawiające się Strony podejmują środki, mające na celu wprowadzenie właściwych zmian w niniejszej Umowie. W tym czasie informacje niejawne są chronione zgodnie z postanowieniami niniejszej Umowy, o ile nie uzgodniono inaczej na piśmie.
5. Informacje niejawne przekazywane lub wytwarzane zgodnie z niniejszą Umową są udostępniane jedynie osobom, które posiadają poświadczenie bezpieczeństwa, wydane po przeprowadzeniu właściwego postępowania sprawdzającego, zgodnie z prawem wewnętrznym każdej z Umawiających się Stron, oraz których zadania wymagają zapoznania się z nimi.
6. Otrzymująca jednostka organizacyjna nie udostępnia informacji niejawnych stronie trzeciej bez uprzedniej zgody wytwarzającej jednostki organizacyjnej, która przyznała klauzulę tajności.
7. Otrzymująca jednostka organizacyjna nie wykorzystuje informacji niejawnych dla innych celów niż te, dla których zostały przekazane lub wytworzone.

Artykuł 5

Przekazywanie informacji niejawnych

1. Informacje niejawne są przekazywane za pośrednictwem kurierów dyplomatycznych lub wojskowych bądź w inny sposób zgodnie z prawem wewnętrznym każdej z Umawiających się Stron. Otrzymująca jednostka organizacyjna potwierdza na piśmie fakt otrzymania informacji niejawnych.

2. Informacje niejawne powinny być przekazywane za pośrednictwem chronionych systemów telekomunikacyjnych, sieci lub środków wykorzystujących energię elektromagnetyczną, którym przyznano certyfikat wydany zgodnie z prawem wewnętrznym każdej z Umawiających się Stron.

3. Inne środki przekazywania informacji niejawnych mogą również być wykorzystane, jeżeli tak wspólnie zaakceptowały właściwe organy bezpieczeństwa.

Artykuł 6

Tłumaczenie, powielanie, niszczenie

1. Informacje niejawne oznaczone klauzulą ŚCIŚLE TAJNE/СТРОГО СЕКРЕТНО/TOP SECRET są tłumaczone lub kopiowane wyłącznie na podstawie pisemnego zezwolenia właściwych organów bezpieczeństwa wytwarzającej Umawiającej się Strony.
2. Wszelkie tłumaczenia informacji niejawnych są dokonywane przez osoby, które posiadają odpowiednie poświadczenie bezpieczeństwa. Takie tłumaczenia oznaczone są odpowiednią klauzulą tajności oraz właściwą adnotacją w języku, na który dokonano przekładu, że zawierają one informacje niejawne wytwarzającej jednostki organizacyjnej.
3. W przypadku powielania informacji niejawnych wszelkie oryginalnie naniesione oznaczenia bezpieczeństwa są również powielone lub nanoszone na każdej kopii. Powielone w ten sposób informacje niejawne podlegają takiej samej kontroli jak oryginalne informacje. Liczba kopii jest ograniczona do wymaganej dla celów służbowych.
4. Wytwarzająca jednostka organizacyjna może wyraźnie zakazać powielania, zmian oraz niszczenia informacji niejawnych poprzez oznaczanie odpowiednich nośników lub późniejsze przesłanie pisemnego zawiadomienia.

W takim przypadku, informacje podlegające zniszczeniu są zwracane wytwarzającej jednostce organizacyjnej.

5. Informacje niejawne są niszczone lub zmieniane w taki sposób, aby uniemożliwić ich całkowitą lub częściową rekonstrukcję. Informacje niejawne oznaczone jako ŚCIŚLE TAJNE/СТРОГО СЕКРЕТНО/TOP SECRET nie podlegają niszczeniu lub modyfikacjom. Zamiast tego, są one zwracane wytwarzającej jednostce organizacyjnej lub właściwym organom bezpieczeństwa, w przypadku likwidacji wytwarzającej jednostki organizacyjnej.

Artykuł 7

Kontrakty niejawne

1. W przypadku, gdy ma być zawarty kontrakt niejawny z potencjalnym kontrahentem, który zamieszkuje na stałe, ma siedzibę bądź jest zarejestrowany na terytorium Państwa drugiej Umawiającej się Strony, właściwy organ bezpieczeństwa dla potencjalnego kontrahenta wydaje dokument potwierdzający, że wydano mu świadectwo bezpieczeństwa przemysłowego odpowiadające wymaganemu poziomowi tajności oraz, że wszyscy jego pracownicy, których stanowiska i obowiązki wymagają dostępu do informacji niejawnych, posiadają stosowne poświadczenie bezpieczeństwa.
2. Jeżeli potencjalny kontrahent nie spełnia wymogów, o których mowa w ustępie 1, właściwy organ bezpieczeństwa, który ma wydać dokument potwierdzający, poinformuje niezwłocznie właściwy organ bezpieczeństwa drugiej Umawiającej się Strony o tym, że na jego wniosek zostaną podjęte niezbędne działania prowadzące do rozpoczęcia postępowania sprawdzającego w celu wydania świadectwa bezpieczeństwa przemysłowego lub poświadczeń bezpieczeństwa.

3. Do każdego kontraktu niejawnego dołączona jest instrukcja bezpieczeństwa. Instrukcja ta określa: informacje niejawne udostępnione lub wytwarzane przez kontrahenta, poziom klauzuli tajności przyznany tym informacjom oraz poszczególne etapy realizacji kontraktu niejawnego. Kopia tego dokumentu jest przekazywana właściwemu organowi bezpieczeństwa każdej z Umawiających się Stron.
4. Kontrakt niejawny musi zawierać minimalne środki ochrony informacji niejawnych, dotyczące wytwarzania, przekazywania i wykorzystywania informacji niejawnych, procedur wizyt oraz dostępu do takich informacji. Musi on być w pełni zgodny z niniejszą Umową, a także zasadniczymi przepisami prawa wewnętrznego każdej z Umawiających się Stron.
5. Wymagania określone w niniejszym artykule stosuje się odpowiednio zarówno do kontraktów zawieranych z podwykonawcą, jak i podwykonawców.

Artykuł 8

Wizyty

1. Eksperci w dziedzinie ochrony informacji niejawnych z właściwych organów bezpieczeństwa odbywają regularne spotkania w celu omawiania środków ochrony informacji niejawnych.
2. Osobom przybywającym z wizytą z terytorium jednej z Umawiających się Stron na terytorium drugiej Umawiającej się Strony zezwala się na dostęp w niezbędnym zakresie do informacji niejawnych, a także do obiektów, w których są wytwarzane, opracowywane lub przechowywane informacje niejawne, wyłącznie po uprzednim uzyskaniu pisemnego zezwolenia, wydanego przez właściwy organ bezpieczeństwa odpowiedniej Umawiającej się Strony.

3. Zezwolenie, o którym mowa w ustępie 2, jest udzielane jedynie osobom, którym wydano poświadczenie bezpieczeństwa zgodnie z ich prawem wewnętrznym.
4. Wnioski w sprawie wizyt zawierają informacje dotyczące:
   a. celu, terminu i programu wizyty;
   b. kwestii związanych z informacjami niejawnymi, które mają być omawiane oraz poziom ich klauzul tajności;
   c. imię i nazwisko osoby przybywającej z wizytą, datę i miejsce urodzenia, obywatelstwo, numer paszportu lub dowodu osobistego;
   d. stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą instytucji lub jednostki, którą reprezentuje;
   e. potwierdzenie poziomu poświadczenia bezpieczeństwa, jakie posiada osoba przybywająca z wizytą;
   f. nazwę i adres odwiedzanej jednostki;
   g. imię i nazwisko oraz stanowisko (stanowiska) służbowe osoby przyjmującej (osób przyjmujących), o ile są znane.
5. Każda z Umawiających się Stron gwarantuje ochronę danych osobowych osób przybywających z wizytą, zgodnie ze swoim prawem wewnętrznym.

Artykuł 9

Naruszenie przepisów dotyczących bezpieczeństwa

1. W przypadku naruszenia przepisów dotyczących bezpieczeństwa, którego skutkiem jest nieuprawniony dostęp lub ryzyko nieuprawnionego dostępu do informacji niejawnych wytworzonych lub przekazanych zgodnie z niniejszą Umową, właściwy organ bezpieczeństwa Umawiającej się Strony, na terytorium której takie zdarzenie miało miejsce, powiadamia niezwłocznie właściwy organ bezpieczeństwa drugiej Umawiającej się Strony i podejmuje

niezbędne środki mające na celu zminimalizowanie skutków takiego naruszenia.

2. W przypadku naruszenia przepisów dotyczących bezpieczeństwa, które mogłoby mieć wpływ na ochronę informacji niejawnych wytwarzanych lub przekazywanych zgodnie z niniejszą Umową, Umawiająca się Strona, na terytorium której takie naruszenie miało miejsce, podejmie odpowiednie czynności wyjaśniające zgodnie ze swoim prawem wewnętrznym.

3. Właściwy organ bezpieczeństwa Umawiającej się Strony, na terytorium której naruszenie przepisów dotyczących bezpieczeństwa miało miejsce, niezwłocznie powiadamia właściwy organ bezpieczeństwa drugiej Umawiającej się Strony o wyniku czynności wyjaśniających, o których mowa w ustępie 2.

Artykuł 10

Wydatki

Każda z Umawiających się Stron pokrywa swoje wydatki poniesione w związku z wykonywaniem zobowiązań na podstawie niniejszej Umowy.

Artykuł 11

Rozstrzyganie sporów

Wszelkie spory dotyczące interpretacji lub wykonywania niniejszej Umowy są rozstrzygane w drodze negocjacji między Umawiającymi się Stronami, jeżeli wcześniejsze konsultacje między właściwymi organami bezpieczeństwa okazały się nieskuteczne.

Artykuł 12

Postanowienia końcowe

1. Niniejsza Umowa wchodzi w życie po czternastu dniach od daty otrzymania ostatniej noty dyplomatycznej, potwierdzającej spełnienie wszelkich procedur przewidzianych prawem wewnętrznym każdej z Umawiających się Stron.
2. Niniejsza Umowa zawarta jest na czas nieokreślony.
3. Każda z Umawiających się Stron może wypowiedzieć niniejszą Umowę notą dyplomatyczną przesłaną do drugiej Umawiającej się Strony. Wypowiedzenie wchodzi w życie po sześciu miesiącach od daty otrzymania takiej noty dyplomatycznej. Niezależnie od wypowiedzenia niniejszej Umowy, wszystkie informacje niejawne przekazywane zgodnie z niniejszą Umową będą nadal chronione zgodnie z postanowieniami niniejszej Umowy, dopóki jedna z Umawiających się Stron nie zwolni drugiej Umawiającej się Strony z tego obowiązku.
4. Niniejsza Umowa może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wchodzą w życie zgodnie z postanowieniami ustępu 1.

Sporządzono w Warszawie, dnia 7 kwietnia 2005 roku w dwóch oryginalnych egzemplarzach, każdy w językach polskim, bułgarskim i angielskim, przy czym wszystkie teksty są jednakowo autentyczne. W razie rozbieżności przy interpretacji, tekst w języku angielskim uważany jest za rozstrzygający.

Z UPOWAŻNIENIA
RZĄDU RZECZYPOSPOLITEJ POLSKIEJ

ZBIGNIEW GOSZCZYŃSKI

Zastępca Szefa
Agencji Bezpieczeństwa Wewnętrznego

Z UPOWAŻNIENIA
RZĄDU REPUBLIKI BUŁGARII

CWETA MARKOWA

Przewodnicząca Państwowej Komisji
do spraw Bezpieczeństwa Informacji

[TRANSLATION - TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE DE POLOGNE ET LE GOUVERNEMENT DE LA RÉPUBLIQUE DE BULGARIE RELATIF À LA PROTECTION MUTUELLE ET À L'ÉCHANGE DE RENSEIGNEMENTS CLASSIFIÉS

Le Gouvernement de la République de Pologne et le Gouvernement de la République de Bulgarie (ci-après dénommés les "Parties contractantes"),

Visant à assurer la protection de toutes les informations classifiées au titre de la législation interne de chacune des Parties contractantes et transmises à l'autre Partie contractante, sont convenus des dispositions suivantes:

Article premier. Définitions

1) L'expression "informations classifiées" ou "renseignements classifiés" désigne tous les renseignements légalement définis, quels que soient leur forme, support, mode d'expression, générés ou en cours de création, qui nécessitent la protection contre l'accès non autorisé;

2) L'expression "accès non autorisé aux informations classifiées" désigne toute forme de divulgation de renseignements classifiés, notamment leur mauvaise utilisation, dégradation, présentation, destruction et classification incorrecte, ainsi que toutes autres actions se traduisant par une violation de la protection ou la perte de ces informations, de même que toutes actions ou inactions entraînant la divulgation de l'information à une personne non autorisée;

3) L'expression "habilitation de sécurité personnelle" désigne un document attestant que son titulaire est autorisé à accéder aux informations classifiées conformément à la législation interne de chacune des Parties contractantes;

4) L'expression "habilitation de sécurité industrielle" désigne un document attestant que l'entrepreneur est autorisé à accéder aux informations classifiées dans le cadre d'un contrat classifié et conformément à la législation interne de chacune des Parties contractantes;

5) "Contrat/contrat de sous-traitance classifié" désigne un accord entre deux ou plusieurs personnes/entités juridiques, reprenant ou prévoyant l'accès à des informations classifiées;

6) "Entrepreneur/sous-traitant" désigne une personne ou une entité juridique possédant la capacité légale de conclure des contrats ou une partie à un contrat classifié au titre du présent contrat;

7) L'expression "Autorité compétente en matière de sécurité" désigne l'organisme qui, conformément à la législation nationale de chacune des Parties contractantes, remplit des fonctions relatives à la protection des informations classifiées, exerce un contrôle général dans ce domaine, procède à la mise en oeuvre du présent Accord et est défini en tant que tel au paragraphe 1 de l'article 3 du présent Accord;

8) "Unité organisationnelle" désigne l'entité qui génère, traite, transmet, reçoit, sauvegarde, protège et utilise les renseignements classifiés conformément à la législation interne de chacune des Parties contractantes et en conformité avec le présent Accord;

9) "Tierce Partie " désigne un État ou une organisation internationale qui n'est pas partie au présent Accord et toute personne/entité juridique ne possédant pas d'habilitation de sécurité personnelle/industrielle ou à qui cette habilitation a été refusée après une procédure de validation conforme à la législation nationale de chacune des Parties contractantes et qui n'a pas de besoin de savoir.

Article 2. Classifications de sécurité

1. Les Parties contractantes conviennent que les classifications de sécurité suivantes sont équivalentes et correspondent aux classifications de sécurité précisées dans la législation interne de chacune des Parties contractantes.

Pour la République de Pologne	**Pour la République de Bulgarie**	**Equivalence en anglais**
SCISLE TAJNE	СТРОГО СЕКРЕТНО	TOP SECRET (SECRET DÉFENSE)
TAJNE	СЕКРЕТНО	SECRET
POUFNE	ПОВЕРИТЕЛНО	CONFIDENTIAL (CONFIDENTIEL)
ZASTRZEŻONE	ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED (RESTREINT)

2. Les unités organisationnelles s'informeront mutuellement de tout changement ou suppression de niveau de classification de sécurité des informations transmises.

Article 3. Autorités compétentes en matière de sécurité

1. Aux fins du présent Accord, les Autorités compétentes en matière de sécurité sont:
   a. Pour la République de Pologne: le Chef de l'Organisme de sécurité interne (organisme civil) et le Chef des Services d'intelligence militaire (organisme militaire);
   b. Pour la République de Bulgarie: la Commission de sécurité des informations.

2. Les Autorités compétentes s'informent réciproquement de la législation nationale en vigueur réglementant la protection des renseignements classifiés et échangent les informations nécessaires.

3. En vue d'atteindre et de maintenir des niveaux comparables de sécurité, les Autorités compétentes se fournissent mutuellement des renseignements sur les niveaux de sécurité, les procédures et pratiques pour protéger les informations classifiées dans chacune des Parties contractantes.

4. Les Autorités compétentes peuvent conclure des arrangements pour l'exécution du présent Accord.

Article 4. Principes de protection des informations classifiées

1. Conformément au présent Accord et à leur législation nationale, les Parties contractantes prennent les mesures nécessaires pour protéger les informations classifiées transmises ou générées dans le cadre de leurs activités mutuelles ou en rapport avec un contrat classifié.

2. L'unité organisationnelle destinataire attribue aux informations classifiées, une classification de sécurité de niveau équivalent à celui de l'entité organisationnelle d'origine, conformément au principe énoncé à l'article 2 du présent Accord;

3. Les Autorités compétentes s'informent mutuellement de tout changement survenu dans leur législation nationale affectant la protection des informations classifiées.

4. Dans les cas visés au paragraphe 3, les Parties contractantes prennent des mesures nécessaires pour introduire les changements appropriés dans le présent Accord. Dans l'intervalle, les informations classifiées sont protégées conformément aux dispositions du présent Accord, sauf accord contraire écrit.

5. L'accès aux informations classifiées transmises ou générées au titre du présent Accord sera accordé uniquement aux personnes titulaires d'une habilitation de sécurité personnelle, délivrée après une procédure de validation appropriée conforme à la législation nationale de chacune des Parties contractantes, et qui ont besoin de savoir.

6. L'unité organisationnelle destinataire n'autorise pas l'accès aux informations classifiées à une tierce Partie sans autorisation préalable de l'unité organisationnelle d'origine, qui prescrit la classification de sécurité.

7. L'unité organisationnelle destinataire n'utilise pas les informations classifiées à d'autres fins que celles pour lesquelles elles ont été transmises ou générées.

Article 5. Transmission d'informations classifiées

1. Les informations classifiées sont transmises par valise diplomatique ou militaire, ou d'autres moyens, conformément aux législations nationales de chacune des Parties contractantes. L'unité organisationnelle destinataire confirme par écrit la réception des informations classifiées.

2. Les informations classifiées sont transmises par des systèmes de télécommunication protégés, réseaux ou autres moyens électromagnétiques, certifiés conformément à la législation nationale de chacune des Parties contractantes.

3. D'autres moyens de transfert d'informations classifiées peuvent être utilisés également, après accord mutuel entre les autorités compétentes en matière de sécurité.

Article 6. Traduction, reproduction, destruction

1. Les informations classifiées portant la classification SCISLE TAJNE/СТРОГО ЕКРЕТНО/TOP SECRET peuvent être traduites ou copiées uniquement avec la permission écrite de l'Autorité compétente en matière de sécurité de la Partie contractante d'origine.

2. Toutes les traductions d'informations classifiées sont faites par des personnes ayant l'habilitation de sécurité personnelle appropriée. Ces traductions reproduisent la classification de sécurité appropriée ainsi que les annotations voulues dans la langue de la traduction, précisant que la traduction en question contient des informations classifiées de l'unité organisationnelle d'origine.

3. Lorsque les informations classifiées sont reproduites, tous les marquages de sécurité d'origine le sont également ou ils sont indiqués sur chaque exemplaire. Ces informations classifiées reproduites font l'objet du même contrôle que l'information originale. Le nombre de copies est limité à celui nécessaire à des fins officielles.

4. L'unité organisationnelle d'origine peut interdire expressément la reproduction, l'altération ou la destruction d'informations classifiées en marquant le support concerné ou en envoyant une notification ultérieure. Dans ce cas, les informations classifiées qui doivent être détruites sont renvoyées à l'unité organisationnelle d'origine.

5. Les informations classifiées sont détruites ou modifiées de manière à empêcher toute reconstruction totale ou partielle. Les informations classifiées marquées SCISLE TAJNE/СТРОГО ЕКРЕТНО/TOP SECRET ne sont pas détruites ni modifiées. En revanche, elles sont renvoyées à l'unité organisationnelle d'origine ou à l'Autorité compétente en matière de sécurité en cas de liquidation de l'unité organisationnelle d'origine.

Article 7. Contrats classifiés

1. Si un contrat classifié doit être conclu avec un entrepreneur potentiel résidant, ayant son siège ou constitué dans l'État de l'autre Partie contractante, l'Autorité compétente en matière de sécurité de l'entrepreneur potentiel délivre un document certifiant qu'il a reçu l'habilitation de sécurité industrielle correspondant à la classification requise et que tout son personnel dont les fonctions et les tâches nécessitent d'accéder aux informations classifiées est titulaire de l'habilitation de sécurité personnelle appropriée.

2. Si l'entrepreneur potentiel ne remplit pas les exigences visées au paragraphe 1, l'Autorité compétente en matière de sécurité qui doit délivrer le document de certification, avertit immédiatement l'Autorité compétente de l'autre Partie contractante que, à sa demande, les mesures nécessaires seront prises immédiatement pour entamer les procédures de validation en vue de délivrer l'habilitation industrielle et l'habilitation personnelle.

3. Chaque contrat classifié sera accompagné d'une instruction de sécurité, précisant les informations classifiées communiquées à ou générées par l'entrepreneur, le niveau de classification attribué à ces informations et les différentes phases d'exécution du contrat classifié. Une copie de ce document sera remise à l'Autorité compétente en matière de sécurité de chacune des Parties contractantes.

4. Le contrat classifié doit contenir des mesures minimales de protection concernant la génération, la transmission et l'usage des informations classifiées, les procédures de visite et d'accès à ces informations. Il doit être en totale conformité avec le présent Accord, ainsi que les dispositions contraignantes de la législation nationale de chacune des Parties contractantes.

5. Les exigences énoncées dans le présent article s'appliquent intégralement aux contrats de sous-traitance et aux sous-traitants aussi.

Article 8. Visites

1. Les experts en protection des informations classifiées des Autorités compétentes en matière de sécurité se réuniront régulièrement pour examiner les mesures de protection des informations classifiées.

2. Les personnes de l'une des Parties contractantes en visite sur le territoire de l'autre Partie contractante sont autorisées à accéder aux informations classifiées dans la mesure nécessaire, ainsi qu'aux locaux où les informations classifiées sont générées, traitées ou stockées, après réception préalable d'une autorisation écrite délivrée par l'Autorité compétente en matière de sécurité de la Partie contractante concernée.

3. L'autorisation visée au paragraphe 2 sera délivrée exclusivement aux personnes titulaires d'une habilitation de sécurité personnelle conformément à leur législation nationale.

4. Les demandes de visite contiendront les informations suivantes:

a. Objet, date et programme de la visite;

b. Questions relatives aux informations classifiées qui doivent être abordées et niveau de classification de sécurité;

c. Nom et prénom du visiteur proposé, date et lieu de naissance, nationalité et numéro de passeport ou de carte d'identité;

d. Fonction du visiteur et nom de l'institution ou organisme qu'il ou elle représente;

e. Certification du niveau de l'habilitation de sécurité personnelle délivrée au visiteur;

f. Nom et adresse des installations à visiter;

g. Nom, prénom et fonction(s) de la (des) personne(s) à visiter, si elle(s) est (sont) connue(s).

5. Chaque Partie contractante garantit la protection des données à caractère personnel des visiteurs, conformément à sa législation nationale.

Article 9. Infractions aux réglementations de sécurité

1. En cas d'infraction aux réglementations de sécurité résultant d'un accès non autorisé ou d'un risque d'accès non autorisé à des informations classifiées générées ou transférées au titre du présent Accord, l'Autorité compétente en matière de sécurité de la Partie contractante sur le territoire de laquelle le cas se produit informe immédiatement l'Autorité compétente de l'autre Partie contractante et prend les mesures nécessaires en vue de réduire les effets de cette infraction.

2. En cas d'infraction aux réglementations de sécurité pouvant affecter la protection des informations classifiées générées ou transférées en vertu du présent Accord, la Partie contractante sur le territoire de laquelle l'infraction se produit mène une enquête appropriée conformément à sa législation nationale.

3. L'Autorité compétente en matière de sécurité de la Partie contractante sur le territoire de laquelle l'infraction a lieu, informe immédiatement l'Autorité compétente de l'autre Partie contractante du résultat de l'enquête visée au paragraphe 2.

Article 10. Dépenses

Chaque Partie contractante prend en charge ses dépenses encourues dans le cadre de la mise en oeuvre de ses obligations au titre du présent Accord.

Article 11. Règlement des litiges

Tout litige concernant l'interprétation ou la mise en application du présent Accord sera résolu par voie de négociation entre les Parties contractantes si les consultations entre les Autorités compétentes s'avèrent inefficaces.

Article 12. Dispositions finales

1. Le présent Accord entrera en vigueur quatorze jours après la réception de la dernière note diplomatique confirmant l'accomplissement de toutes les formalités prévues par la législation nationale de chacune des Parties contractantes.

2. Le présent Accord est conclu pour une durée indéterminée.

3. Chacune des Parties contractantes peut dénoncer le présent Accord par une note diplomatique transmise à l'autre Partie contractante. La dénonciation entrera en vigueur six mois après la date de réception de cette note diplomatique. Nonobstant la dénonciation du présent Accord, toutes les informations classifiées transmises en vertu de celui-ci continuent d'être protégées conformément aux dispositions énoncées dans les présentes, jusqu'à ce que l'une des Parties contractantes dispense l'autre de cette obligation.

4. Le présent Accord peut être modifié par consentement mutuel écrit des deux Parties contractantes. Ces amendements entreront en vigueur conformément aux dispositions du paragraphe 1.

Fait à Varsovie le 7 avril 2005, en deux originaux, chacun en langues polonaise, bulgare et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, le texte anglais prévaudra.

Pour le Gouvernement de la République de Pologne :

ZBIGNIEW GOSZCZYNSKI
Chef adjoint de l'Agence de sécurité interne

Pour le Gouvernement de la République de Bulgarie :

CWETA MARKOWA
Président de la Commission d'État sur la sécurité de l'information