1228

UMOWA

między Rzecząpospolitą Polską a Republiką Portugalską o wzajemnej ochronie informacji niejawnych,

podpisana w Lizbonie dnia 2 sierpnia 2007 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 2 sierpnia 2007 r. w Lizbonie została podpisana Umowa między Rzecząpospolitą Polską a Republiką Portugalską o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między Rzecząpospolitą Polską

a Republiką Portugalską

o wzajemnej ochronie informacji

niejawnych

Rzeczpospolita Polska oraz Republika Portugalska

zwane dalej „Stronami",

Mając na uwadze zagwarantowanie wzajemnej ochrony wszelkich informacji, którym, zgodnie z prawem wewnętrznym każdej ze Stron, nadano klauzule tajności oraz które zostały przekazane drugiej Stronie przez właściwe organy lub upoważnione do tego osoby;

Pragnąc stworzyć system regulacji w zakresie wzajemnej ochrony informacji niejawnych wymienianych pomiędzy Stronami,

uzgodniły, co następuje:

ARTYKUŁ 1
PRZEDMIOT UMOWY

Niniejsza Umowa określa zasady bezpieczeństwa mające zastosowanie w przypadku kontraktów, których realizacja wiąże się z przekazywaniem informacji niejawnych. Dotyczy to zarówno kontraktów, które zostały podpisane, jak i kontraktów, których podpisanie przez właściwe krajowe organy Stron lub podmioty do tego uprawnione jest planowane.

ARTYKUŁ 2
ZAKRES OBOWIĄZYWANIA

Niniejsza Umowa określa procedury ochrony informacji niejawnych wymienianych między Stronami.

ARTYKUŁ 3
DEFINICJE

W rozumieniu niniejszej Umowy:

a) „Informacje niejawne" oznaczają informacje, dokumenty i materiały, niezależnie od ich formy, rodzaju oraz nośnika, które, zgodnie z nadaną im klauzulą tajności, wymagają ochrony przed nieuprawnionym ujawnieniem;

b) „Krajowa władza bezpieczeństwa" oznacza organ odpowiedzialny za wprowadzanie w życie postanowień oraz nadzór nad niniejszą Umową;

c) „Strona przekazująca" oznacza Stronę, która przekazuje lub przesyła informacje niejawne drugiej Stronie;

d) „Strona otrzymująca" oznacza Stronę, której informacje niejawne są przekazywane lub przesyłane przez Stronę przekazującą;

e) „Strona trzecia" oznacza organizację międzynarodową lub państwo, które nie jest Stroną niniejszej Umowy;

f) „Kontrakt niejawny" oznacza umowę tworzącą oraz definiującą wzajemne prawa i obowiązki między dwoma lub więcej kontrahentami w przypadku, gdy umowa zawiera lub wiąże się z dostępem do informacji niejawnych;

g) „Kontrahent" oznacza osobę fizyczną lub osobę prawną posiadającą zdolność prawną do zawierania kontraktów;

h) „Poświadczenie bezpieczeństwa" oznacza oświadczenie wydane przez krajową władzę bezpieczeństwa lub inny właściwy organ stwierdzające, że osoba fizyczna jest uprawniona do dostępu do informacji niejawnych, zgodnie z prawem wewnętrznym każdej ze Stron;

i) „Świadectwo bezpieczeństwa przemysłowego" oznacza oświadczenie wydane przez krajową władzę bezpieczeństwa lub inny uprawniony organ stwierdzające, że, z punktu widzenia ochrony informacji niejawnych, dany przedsiębiorca posiada fizyczne i organizacyjne zdolności przechowywania oraz korzystania z tych informacji, zgodnie z prawem wewnętrznym każdej ze Stron;

j) „Zasada ograniczonego dostępu" oznacza, że dostęp do informacji niejawnych mogą uzyskać tylko te osoby, które posiadają potwierdzoną potrzebę dostępu, potrzebę uzyskania wiedzy na dany temat lub potrzebę posiadania takich informacji, w celu wykonania swoich zadań służbowych lub zawodowych;

k) „Instrukcja bezpieczeństwa przemysłowego" oznacza zbiór wymogów bezpieczeństwa odnoszących się do konkretnego projektu, których celem jest ujednolicenie procedur w zakresie bezpieczeństwa;

l) „Wytyczne w zakresie nadawania klauzul tajności w ramach projektu" oznaczają część instrukcji bezpieczeństwa projektu wskazującą, które elementy projektu są klasyfikowane oraz określającą klauzule tajności.

ARTYKUŁ 4
ODPOWIEDZIALNE ORGANY

1. Krajowymi władzami bezpieczeństwa są:

W Rzeczypospolitej Polskiej:

- w sferze cywilnej

Szef Agencji Bezpieczeństwa Wewnętrznego

ul. Rakowiecka 2A

00-993 Warszawa

Polska

- w sferze wojskowej

Szef Służby Kontrwywiadu Wojskowego

ul. Oczki 1

02-007 Warszawa

Polska

W Republice Portugalskiej:

Autoridade Nacional de Segurança

Presidência do Conselho de Ministros

Av. Ilha da Madeira, 1

1400-204 Lisboa

Portugal

2. Strony będą się informować, drogą dyplomatyczną, o jakichkolwiek zmianach danych przedstawionych w ustępie 1 niniejszego artykułu.

ARTYKUŁ 5
KLAUZULE TAJNOŚCI I ICH ODPOWIEDNIKI

Strony uzgodniły, iż poniższe klauzule tajności są równorzędne i zgodne z klauzulami tajności przewidzianymi w prawie wewnętrznym każdej ze Stron:

RZECZPOSPOLITA POLSKA	REPUBLIKA PORTUGALSKA	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	MUITO SECRETO	TOP SECRET
TAJNE	SECRETO	SECRET
POUFNE	CONFIDENCIAL	CONFIDENTIAL
ZASTRZEŻONE	RESERVADO	RESTRICTED

ARTYKUŁ 6
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Każda ze Stron zapewnia, że wszystkie podmioty spełniają warunki niezbędne do ochrony informacji niejawnych przekazywanych zgodnie z postanowieniami niniejszej Umowy lub wytwarzanych albo przetwarzanych w związku z kontraktem niejawnym lub innymi formami kontaktu między Stronami.
2. Strony zapewniają wszystkim przekazywanym, wytwarzanym lub przetwarzanym informacjom niejawnym taką samą ochronę, jaka obowiązuje w stosunku do ich własnych informacji niejawnych objętych równorzędną klauzulą tajności, zgodnie z odpowiednikami określonymi w artykule 5 niniejszej Umowy.
3. Dostęp do informacji niejawnych będzie ograniczony do osób, które, w celu wykonania swoich obowiązków, uzyskały zezwolenie na dostęp do informacji niejawnych zgodnie z zasadą ograniczonego dostępu.

posiadają poświadczenie bezpieczeństwa oraz zostały upoważnione przez uprawnione organy.

4. Strona otrzymująca oznacza otrzymane informacje niejawne równorzędną klauzulą tajności, zgodnie z odpowiednikami określonymi w artykule 5 niniejszej Umowy.
5. Strony będą się informować o wszelkich późniejszych zmianach klauzul tajności przekazanych informacji niejawnych.
6. Strona otrzymująca i/albo podmioty reprezentujące Państwo Strony otrzymującej nie obniża ani nie znosi klauzul tajności otrzymanych informacji niejawnych bez uprzedniej pisemnej zgody Strony przekazującej.
7. Przekazane informacje niejawne są wykorzystywane wyłącznie w celach, w jakich zostały przekazane, zgodnie z postanowieniami porozumień zawartych między Stronami lub kontraktów podpisanych między podmiotami.
8. Strona otrzymująca nie przekazuje informacji niejawnych Stronie trzeciej, osobie fizycznej posiadającej obywatelstwo Strony trzeciej, lub podmiotowi Strony trzeciej, bez uprzedniego pisemnego upoważnienia Strony przekazującej.

ARTYKUŁ 7
WSPÓŁPRACA PRZY POSTĘPOWANIU SPRAWDZAJĄCYM

1. Na wniosek, krajowe władze bezpieczeństwa, zgodnie z prawem wewnętrznym każdej ze Stron, współpracują podczas przeprowadzania postępowań sprawdzających poprzedzających wydanie poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego.
2. Poświadczenie bezpieczeństwa oraz świadectwo bezpieczeństwa przemysłowego wydane zgodnie z prawem wewnętrznym jednej Strony

są uznawane przez drugą Stronę. Równorzędność poświadczeń bezpieczeństwa oraz świadectw bezpieczeństwa przemysłowego jest zgodna z odpowiednikami określonymi w artykule 5 niniejszej Umowy.

3. Krajowe władze bezpieczeństwa informują się o wszelkich zmianach w wydanych poświadczeniach bezpieczeństwa oraz świadectwach bezpieczeństwa przemysłowego mających wpływ na stosowanie postanowień niniejszej Umowy, a w szczególności o przypadkach ich cofnięcia lub obniżenia klauzuli tajności.

ARTYKUŁ 8
TŁUMACZENIE, POWIELANIE I NISZCZENIE

1. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/MUITO SECRETO/TOP SECRET są tłumaczone lub powielane wyłącznie po uzyskaniu pisemnego zezwolenia krajowej władzy bezpieczeństwa Strony przekazującej.
2. Tłumaczenie oraz powielanie informacji niejawnych jest wykonywane zgodnie z następującymi procedurami:
   a) osoby tłumaczące lub powielające posiadają odpowiednie poświadczenie bezpieczeństwa;
   b) tłumaczenia oraz kopie są oznaczane i ochronione tak, jak oryginały;
   c) tłumaczenia oraz liczba powielonych informacji są ograniczone do liczby niezbędnej do celów służbowych;
   d) na tłumaczeniach nanosi się odpowiednią adnotację w języku, na który dokonano przekładu, że zawierają one informacje niejawne otrzymane od Strony przekazującej.
3. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/MUITO SECRETO/TOP SECRET nie będą niszczone i będą zwracane krajowej władzy bezpieczeństwa Strony przekazującej.

4. O zniszczeniu informacji niejawnych o klauzuli TAJNE/SECRETO/SECRET informuje się Stronę przekazującą.
5. Informacje niejawne do klauzuli POUFNE/CONFIDENCIAL/CONFIDENTIAL włącznie są niszczone zgodnie z prawem wewnętrznym każdej ze Stron.

ARTYKUŁ 9
PRZEKAZYWANIE MIĘDZY STRONAMI

1. Informacje niejawne są przekazywane drogą dyplomatyczną.
2. W przypadku, gdy przekazanie informacji niejawnych drogą dyplomatyczną okazałoby się niepraktyczne, lub nazbyt opóźniające ich odbiór, mogą tego dokonać pracownicy, wobec których przeprowadzono odpowiednie postępowanie sprawdzające posiadający certyfikat kurierski wydany przez Stronę przekazującą informacje niejawne.
3. Strony mogą przekazywać informacje niejawne za pośrednictwem środków elektronicznych zgodnie z procedurami obustronnie uzgodnionymi przez krajowe władze bezpieczeństwa.
4. Każdorazowe dostarczenie większej ilości informacji niejawnych odbywa się po uprzednim zatwierdzeniu przez krajowe władze bezpieczeństwa.
5. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.

ARTYKUŁ 10
KONTRAKTY NIEJAWNE

1. Strona, która w ramach niejawnego projektu chce zawrzeć kontrakt niejawny z kontrahentem drugiej Strony, lub chce upoważnić jednego ze swoich kontrahentów do zawarcia kontraktu niejawnego na terytorium Państwa drugiej Strony, powinna otrzymać, za pośrednictwem właściwej

krajowej władzy bezpieczeństwa, wcześniejsze pisemne zapewnienie od krajowej władzy bezpieczeństwa drugiej Strony, że proponowany kontrahent posiada odpowiednie świadectwo bezpieczeństwa przemysłowego.

2. Kontrahent zobowiązuje się do:
   a) posiadania odpowiedniego świadectwa bezpieczeństwa przemysłowego;
   b) zapewnienia, aby osoby, których obowiązki służbowe wiążą się z dostępem do informacji niejawnych, posiadały odpowiednie poświadczenia bezpieczeństwa;
   c) zapewnienia, że wszystkie osoby, które będą miały dostęp do informacji niejawnych, są poinformowane o swojej odpowiedzialności za ochronę informacji niejawnych, zgodnie z prawem wewnętrznym każdej ze Stron;
   d) udzielania zezwoleń na dokonywanie inspekcji w swoich obiektach.
3. Każdy ewentualny podwykonawca zobowiązany będzie do przestrzegania tych samych wymogów bezpieczeństwa, jakie obowiązują kontrahenta.
4. Zapewnienie, że kontrahent spełnia warunki wymienione w ustępie 2 niniejszego artykułu, należy do kompetencji krajowej władzy bezpieczeństwa.
5. Każdy kontrakt niejawny, zawarty między podmiotami Stron, zgodnie z wymogami niniejszej Umowy, powinien zawierać instrukcję bezpieczeństwa przemysłowego określającą następujące kwestie:
   a) wytyczne w zakresie nadawania klauzul tajności w ramach projektu oraz wykaz informacji niejawnych;
   b) procedury informowania o zmianach klasyfikacji informacji;
   c) formy przekazywania informacji oraz środki przekazu elektromagnetycznego;

d) procedury dotyczące transportu informacji niejawnych;

e) nazwy właściwych organów odpowiedzialnych za koordynację oraz ochronę informacji niejawnych związanych z kontraktem;

f) zobowiązanie do informowania o faktycznej lub domniemanej utracie, ujawnieniu lub naruszeniu bezpieczeństwa informacji niejawnych.

6. W celu umożliwienia właściwego nadzoru i kontroli bezpieczeństwa, kopia instrukcji bezpieczeństwa przemysłowego, odnoszącego się do kontraktu niejawnego, jest przekazywana krajowej władzy bezpieczeństwa Strony, na terytorium Państwa której kontrakt niejawny będzie realizowany.

7. Przedstawiciele krajowych władz bezpieczeństwa mogą składać sobie wizyty, których celem będzie analiza efektywności zastosowanych przez kontrahenta środków ochrony informacji niejawnych związanych z kontraktem niejawnym. Zawiadomienie o wizycie powinno nastąpić z co najmniej trzydziestodniowym wyprzedzeniem.

ARTYKUŁ 11
WIZYTY

1. Wizyty obywateli Państwa jednej Strony na terytorium Państwa drugiej Strony, które wiążą się z dostępem do informacji niejawnych, wymagają wcześniejszego pisemnego upoważnienia wydanego przez krajową władzę bezpieczeństwa Strony przyjmującej.

2. Personel wizytujący jednej ze Stron otrzymuje od drugiej Strony zezwolenie na wizytę, która wiąże się z dostępem do informacji niejawnych tylko jeżeli:

a) posiada poświadczenie bezpieczeństwa wydane przez właściwą krajową władzę bezpieczeństwa lub inny odpowiedni organ Strony wysyłającej;

b) został upoważniony do otrzymywania lub dostępu do informacji niejawnych zgodnie z zasadą ograniczonego dostępu oraz prawem wewnętrznym.

3. Krajowa władza bezpieczeństwa Strony wysyłającej zwraca się do krajowej władzy bezpieczeństwa Strony przyjmującej z wnioskiem o wyrażenie zgody na wizytę co najmniej trzydzieści dni przed planowanym terminem wizyty.

4. W nagłych przypadkach, wniosek o wyrażenie zgody na wizytę może być przekazany z co najmniej siedmiodniowym wyprzedzeniem.

5. Wniosek o wyrażenie zgody na wizytę zawiera:

a) imię i nazwisko, miejsce i datę urodzenia, obywatelstwo, numer paszportu lub dowodu tożsamości osoby przybywającej z wizytą;

b) nazwę podmiotu, który osoba wizytująca reprezentuje, lub do którego należy;

c) nazwę i adres podmiotu odwiedzanego;

d) ważne poświadczenie bezpieczeństwa;

e) przedmiot i cel wizyty lub wizyt;

f) spodziewany termin i czas trwania wizyty lub wizyt oraz, w przypadku wizyt powtarzających się, całkowity czas ich trwania;

g) imię, nazwisko oraz numer telefonu osoby w odwiedzanej jednostce wyznaczonej jako punkt kontaktowy, dane osób, z którymi odwiedzający kontaktował się uprzednio oraz wszelkie inne informacje, które mogą być pomocne w przypadku konieczności potwierdzenia wizyty lub wizyt;

h) datę, podpis oraz oficjalną pieczęć właściwej krajowej władzy bezpieczeństwa.

6. Na wizyty, które wiążą się z dostępem do informacji niejawnych przez obywateli trzeciego Państwa, zezwala się tylko za wspólnym porozumieniem Stron.

7. Krajowa władza bezpieczeństwa Strony przyjmującej powiadamia pełnomocnika ochrony odwiedzanej jednostki o danych osobowych członków zatwierdzonego personelu wizytującego.

8. W przypadku wizyt powtarzających się, okres ważności upoważnienia nie może przekraczać 12 miesięcy.
9. W przypadku jakiegokolwiek projektu, programu lub kontraktu, krajowe władze bezpieczeństwa mogą wyrazić zgodę na ustalenie list personelu upoważnionego do składania powtarzających się wizyt. Listy te są ważne przez okres początkowy 12 miesięcy i mogą być przedłużane.
10. Po zaakceptowaniu takiej listy przez krajową władzę bezpieczeństwa, terminy wizyt uzgadniane są bezpośrednio między osobami przybywającymi z wizytą a przedstawicielami odwiedzanych jednostek, zgodnie z ustalonymi warunkami.

ARTYKUŁ 12
NARUSZENIE I NARAŻENIE NA SZWANK BEZPIECZEŃSTWA

1. W przypadku naruszenia lub narażenia na szwank bezpieczeństwa, którego skutkiem jest faktyczne lub domniemane narażenie na szwank bezpieczeństwa informacji niejawnych wytworzonych przez lub otrzymanych od drugiej Strony, krajowa władza bezpieczeństwa Strony, na terytorium Państwa której doszło do naruszenia lub narażenia na szwank bezpieczeństwa, informuje o tym jak najszybciej krajową władzę bezpieczeństwa drugiej Strony i przeprowadza odpowiednie dochodzenie.
2. Jeżeli naruszenie lub narażenie na szwank bezpieczeństwa ma miejsce w kraju innym, niż Państwa Stron niniejszej Umowy, wówczas krajowa władza bezpieczeństwa Strony przekazującej podejmuje kroki opisane w ustępie 1 niniejszego artykułu.
3. Jeżeli zachodzi taka potrzeba, druga Strona współpracuje w dochodzeniu.
4. W każdym przypadku, druga Strona będzie poinformowana na piśmie o wynikach dochodzenia. Informacja taka będzie zawierać przyczyny naruszenia lub narażenia na szwank bezpieczeństwa, wielkość wyrządzonej szkody oraz wnioski z przeprowadzonego dochodzenia.

ARTYKUŁ 13
KOSZTY

Każda ze Stron będzie pokrywała swoje własne koszty poniesione w związku z wprowadzeniem w życie oraz nadzorem wszystkich aspektów niniejszej Umowy.

ARTYKUŁ 14
KONSULTACJE

1. W celu osiągnięcia oraz utrzymania porównywalnych standardów bezpieczeństwa, krajowe władze bezpieczeństwa, na wniosek, informują się o standardach bezpieczeństwa, procedurach oraz praktykach ochrony informacji niejawnych.
2. Na wniosek, krajowe władze bezpieczeństwa prowadzą konsultacje w celu zapewnienia bliskiej współpracy przy wprowadzaniu postanowień niniejszej Umowy w życie.
3. Każda ze Stron może wyrazić zgodę przedstawicielom krajowej władzy bezpieczeństwa drugiej Strony na przybycie na terytorium swojego kraju w celu omówienia procedur ochrony informacji niejawnych przekazanych przez drugą Stronę.

ARTYKUŁ 15
ROZSTRZYGANIE SPORÓW

Wszelkie kwestie sporne dotyczące interpretacji lub stosowania postanowień niniejszej Umowy będą rozstrzygane drogą dyplomatyczną.

ARTYKUŁ 16
ZMIANY

1. Na wniosek jednej ze Stron, do niniejszej Umowy mogą być wprowadzane zmiany na podstawie obustronnej pisemnej zgody.
2. Zmiany wejdą w życie zgodnie z zasadami określonymi w artykule 17 niniejszej Umowy.

ARTYKUŁ 17
WEJŚCIE W ŻYCIE

Niniejsza Umowa wchodzi w życie trzydziestego dnia po dniu otrzymania, drogą dyplomatyczną, ostatniej pisemnej noty informującej o zakończeniu przez Strony wszystkich wewnętrznych procedur niezbędnych do wejścia Umowy w życie.

ARTYKUŁ 18
CZAS TRWANIA I WYPOWIEDZENIE

1. Niniejsza Umowa zawarta jest na czas nieokreślony.
2. Każda ze Stron może, w każdym czasie, w drodze pisemnej notyfikacji drogą dyplomatyczną, wypowiedzieć niniejszą Umowę.
3. Niniejsza Umowa traci moc po upływie sześciu miesięcy od dnia otrzymania takiej notyfikacji.
4. Bez względu na wypowiedzenie, wszelkie informacje niejawne przekazane na podstawie niniejszej Umowy będą nadal chronione zgodnie z jej postanowieniami, chyba, że Strony ustalą inaczej.

Sporządzono w .....Lizbonie..... , dnia .....2...sierpnia...2007 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, portugalskim i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W razie rozbieżności przy ich interpretacji tekst w języku angielskim uważany będzie za rozstrzygający.

W IMIENIU
RZECZYPOSPOLITEJ POLSKIEJ

W IMIENIU
REPUBLIKI PORTUGALSKIEJ

ACORDO
entre a República da Polónia
e República Portuguesa
sobre a protecção mútua de informação
classificada

A República da Polónia

e

a República Portuguesa

doravante designadas por "Partes",

Por forma a garantir a protecção mútua de toda a informação que foi classificada de acordo com o Direito de cada Parte e transmitida à outra Parte por autoridades competentes ou pessoas autorizadas para o efeito;

Desejando estabelecer um conjunto de regras para protecção mútua de Informação Classificada trocada entre as Partes;

Acordaram no seguinte:

ARTIGO 1.º
OBJECTO DO ACORDO

O presente Acordo estabelece as regras de segurança aplicáveis a todos os contratos que prevejam a transmissão de Informação Classificada. celebrados ou a celebrar pelas autoridades nacionais competentes das Partes ou por entidades autorizadas para esse efeito.

ARTIGO 2.º
ÂMBITO DA APLICAÇÃO

O presente Acordo estabelece os procedimentos para a protecção de Informação Classificada trocada entre as Partes.

ARTIGO 3.º
DEFINIÇÕES

Para os efeitos do presente Acordo:

a) "Informação Classificada", designa informação, documentos e materiais, independemente da sua forma, natureza e meio de transmissão, aos quais tenha sido atribuído um grau de classificação de segurança e que requeiram protecção contra divulgação não autorizada;

b) "Autoridade Nacional de Segurança", designa a autoridade designada por cada Parte, sendo responsável pela aplicação e supervisão do presente Acordo;

c) "A Parte Transmissora", designa a Parte que entrega ou transmite Informação Classificada à outra Parte;

d) "A Parte Destinatária", designa a Parte à qual é entregue ou transmitida Informação Classificada pela Parte Transmissora;

e) "Terceira Parte", designa qualquer organização internacional ou Estado que não é Parte no presente Acordo;

f) "Contracto Classificado", designa qualquer acordo entre dois ou mais Contratantes que estabelece ou define direitos e obrigações entre eles e que contém ou envolve acesso a Informação Classificada;

g) "Contratante", designa uma pessoa singular ou colectiva possuidora de capacidade legal para celebrar contratos;

h) "Credenciação de Segurança do Pessoal", designa a determinação feita pela Autoridade Nacional de Segurança ou outra autoridade competente, de que um indivíduo está habilitado para ter acesso a Informação Classificada, de acordo com o respectivo Direito em vigor;

i) "Credenciação de Segurança Industrial", designa a determinação feita pela Autoridade Nacional de Segurança ou outra autoridade qualificada de que, do ponto de vista de segurança, uma entidade tem capacidade física e organizacional para manusear e guardar Informação Classificada, de acordo com o respectivo Direito em vigor;

j) "Necessidade de conhecer", designa o acesso à Informação Classificada que só pode ser concedido à pessoa que tenha comprovada necessidade de

a conhecer, ou de a possuir, para cumprimento das suas funções e tarefas oficiais;

k) "Instrução de Segurança do Projecto" designa uma compilação de requisitos de segurança, que são aplicados a um determinado projecto para garantir a uniformização de procedimentos de segurança;

l) "Guia de Classificação de Segurança do Projecto", designa a parte da Instrução de Segurança do Projecto que identifica os elementos classificados, especificando os níveis de classificação de segurança.

ARTIGO 4.º

AUTORIDADES RESPONSÁVEIS

1. As Autoridades Nacionais de Segurança responsáveis pela aplicação do presente Acordo são:

Para a República da Polónia

- na esfera civil

Szef Agencji Bezpieczeństwa Wewnętrznego

ul. Rakowiecka 2A

00–993 Varsóvia

Polónia

- na esfera militar

Szef Służby Kontrwywiadu Wojskowego

ul. Oczki 1

02-007 Varsóvia

Polónia

Para a República Portuguesa

Autoridade Nacional de Segurança

Presidência do Conselho de Ministros

Av Ilha da Madeira, 1

1400–204 Lisboa

Portugal

2. Cada uma das Partes informará a outra, através dos canais diplomáticos, de qualquer alteração relativa à informação referida no número 1 do presente Artigo.

ARTIGO 5.º
CLASSIFICAÇÕES DE SEGURANÇA E EQUIVALÊNCIAS

As Partes acordam que os seguintes graus de classificação de segurança são equivalentes e correspondem aos graus de segurança especificados no respectivo Direito em vigor:

REPÚBLICA DA POLÓNIA	REPÚBLICA PORTUGUESA	EQUIVALENTE EM INGLÊS
ŚCIŚLE TAJNE	MUITO SECRETO	TOP SECRET
TAJNE	SECRETO	SECRET
POUFNE	CONFIDENCIAL	CONFIDENTIAL
ZASTRZEŻONE	RESERVADO	RESTRICTED

ARTIGO 6.º
REGRAS DE SEGURANÇA

1. Cada Parte assegurará que todas as entidades deverão cumprir as medidas de protecção de Informação Classificada que é transmitida nos termos do presente Acordo ou é produzida ou desenvolvida no âmbito a um Contrato Classificado ou de qualquer outra relação entre as Partes.
2. As Partes atribuirão a toda a Informação Classificada transmitida, produzida ou desenvolvida os mesmos graus de segurança previstos para a sua própria Informação Classificada de grau equivalente, como definido no artigo 5.º do presente Acordo.
3. O acesso à Informação Classificada é limitado às pessoas que, para o desempenho das suas funções, necessitem de ter acesso à mesma fundamentado na "Necessidade de Conhecer", estejam habilitados com uma Credenciação de Segurança do Pessoal apropriada, e estejam autorizadas pelas autoridades competentes.

4. A Parte Destinatária marcará a Informação Classificada recebida com as suas próprias marcas nacionais de classificação de segurança, em conformidade com as equivalências referidas no Artigo 5.º do presente Acordo.
5. As Partes informar-se-ão mutuamente sobre as alterações ulteriores à classificação da Informação Classificada transmitida.
6. A Parte Destinatária e/ou as suas entidades não poderão baixar o grau de classificação de segurança ou desclassificar a Informação Classificada recebida, sem prévia autorização escrita da Parte Transmissora.
7. A Informação Classificada transmitida deverá ser exclusivamente utilizada para o fim para o qual foi transmitida, segundo os acordos celebrados entre as Partes ou contratos celebrados entre entidades.
8. A Parte Destinatária não deverá transmitir Informação Classificada a uma terceira Parte ou a uma pessoa portadora de nacionalidade de um terceiro Estado, ou a uma entidade de um terceiro Estado, sem prévia autorização escrita da Parte Transmissora.

ARTIGO 7.º
COOPERAÇÃO NO ÂMBITO DA CREDENCIAÇÃO DE SEGURANÇA

1. Se solicitado, as Autoridades Nacionais de Segurança, tendo em conta o respectivo Direito em vigor, colaborarão mutuamente no decurso dos procedimentos para a credenciação de segurança precedendo a emissão da Credenciação de Segurança do Pessoal e da Credenciação de Segurança Industrial.
2. Cada Parte reconhecerá a Credenciação de Segurança do Pessoal e a Credenciação de Segurança Industrial emitidas de acordo com o Direito em vigor na outra Parte. A equivalência dos graus de segurança será feita em conformidade com o artigo 5.º do presente Acordo.

3. As Autoridades Nacionais de Segurança informar-se-ão mutuamente sobre quaisquer alterações relativas à Credenciação de Segurança do Pessoal e à Credenciação de Segurança Industrial, no âmbito da aplicação do presente Acordo, designadamente no caso de cancelamento ou abaixamento do grau de classificação de segurança atribuído.

ARTIGO 8.º
TRADUÇÃO, REPRODUÇÃO E DESTRUIÇÃO

1. A Informação Classificada marcada como ŚCIŚLE TAJNE/MUITO SECRETO/TOP SECRET só poderá ser traduzida ou reproduzida após autorização escrita da Autoridade Nacional de Segurança da Parte Transmissora.
2. As traduções e reproduções de Informação Classificada deverão obedecer aos seguintes procedimentos:
   a) As pessoas envolvidas deverão ser titulares de Credenciação de Segurança do Pessoal apropriada;
   b) As traduções e as reproduções serão marcadas e protegidas da mesma forma que a informação original;
   c) As traduções e o número de cópias a efectuar deverão ser limitadas às requeridas para uso oficial;
   d) As traduções deverão ter a indicação, na língua para que foram traduzidas, de que contém Informação Classificada recebida da Parte Transmissora.
3. A Informação Classificada marcada como ŚCIŚLE TAJNE/MUITO SECRETO/TOP SECRET, não poderá ser destruída, devendo ser devolvida à Autoridade Nacional de Segurança da Parte Transmissora.
4. A destruição de Informação Classificada marcada como TAJNE/ SECRETO/SECRET efectuada deverá ser notificada previamente à Parte Transmissora.

5. A Informação Classificada marcada até POUFNE/CONFIDENCIAL/ CONFIDENTIAL, inclusive, deverá ser destruída de acordo com o respectivo Direito em vigor.

ARTIGO 9.º
TRANSMISSÃO ENTRE AS PARTES

1. A Informação Classificada é transmitida entre as Partes utilizando canais diplomáticos.
2. Caso o uso dos canais diplomáticos se revele impraticável ou excessivamente moroso para a recepção de Informação Classificada, as transmissões podem ser efectuadas por pessoal devidamente credenciado e detentor de um certificado de correio emitido pela Parte que transmite a Informação Classificada.
3. As Partes podem transmitir Informação Classificada por meios electrónicos de acordo com os procedimentos de segurança aprovados em conjunto pelas Autoridades Nacionais de Segurança.
4. A transmissão de Informação Classificada volumosa ou em grande quantidade, acordada pontualmente, será aprovada por ambas as Autoridades Nacionais de Segurança.
5. A Parte Destinatária confirmará, por escrito, a recepção da Informação Classificada.

ARTIGO 10.º
CONTRATOS CLASSIFICADOS

1. Uma Parte que pretenda celebrar um Contrato Classificado com um Contratante da outra Parte, ou que pretenda autorizar um dos seus Contratantes a efectuar um Contrato Classificado no território da outra Parte, no âmbito de um projecto classificado, obterá, através da sua

Autoridade Nacional de Segurança, garantia escrita prévia da Autoridade Nacional de Segurança da outra Parte, em como o Contratante proposto está habilitado com uma Credenciação de Segurança Industrial com o grau de classificação de segurança adequado.

2. O Contratante obriga-se a:

   a) Ter uma Credenciação de Segurança Industrial adequada a essas instalações;

   b) Ter uma Credenciação de Segurança do Pessoal adequada às pessoas que necessitem ter acesso a Informação Classificada;

   c) Assegurar que todas as pessoas que tenham acesso a Informação Classificada estejam informadas das suas responsabilidades sobre a protecção de Informação Classificada, em conformidade com o Direito em vigor de cada Parte;

   d) Permitir inspecções de segurança às suas instalações.

3. Qualquer sub-contratante deverá cumprir as mesmas obrigações de segurança que o Contratante.

4. A Autoridade Nacional de Segurança detém a competência para assegurar o cumprimento pelo Contratante das disposições previstas no número 2 do presente Artigo.

5. Qualquer Contrato Classificado celebrado entre entidades das Partes, nos termos do presente Acordo, deverá incluir uma secção de segurança apropriada, identificando os seguintes aspectos:

   a) Guia de Classificação de Segurança do Projecto e lista da Informação Classificada;

   b) Procedimentos para a notificação de alterações à classificação de segurança de Informação Classificada;

   c) Canais de comunicação e meios de transmissão electromagnética;

   d) Procedimento para o transporte de Informação Classificada;

e) Autoridades responsáveis pela coordenação e salvaguarda de Informação Classificada relativa ao Contrato;

f) Obrigatoriedade de notificação de perda, extravio ou comprometimento de Informação Classificada.

6. Deverá ser enviada à Autoridade Nacional de Segurança da Parte em cujo território o Contrato Classificado será cumprido uma cópia da secção de segurança de qualquer Contrato Classificado, por forma a garantir adequada supervisão e controlo de segurança.

7. Representantes das Autoridades Nacionais de Segurança podem efectuar visitas mútuas a fim de verificarem a eficácia das medidas adoptadas pelo Contratante na protecção de Informação Classificada relativa ao Contrato Classificado. O aviso da visita deverá ser efectuado com uma antecedência mínima de trinta dias.

ARTIGO 11.º
VISITAS

1. As visitas que envolvam acesso a Informação Classificada por cidadãos de uma Parte à outra Parte estão sujeitas a autorização prévia, por escrito, conferida pela Autoridade Nacional de Segurança da Parte anfitriã.

2. As visitas que envolvam acesso a Informação Classificada serão autorizadas por uma Parte aos visitantes da outra Parte, apenas se estes:

a) Possuírem Credenciação de Segurança do Pessoal apropriada concedida pela Autoridade Nacional de Segurança ou outra autoridade relevante da Parte visitante;

b) Estiverem autorizados a receber ou ter acesso a Informação Classificada fundamentado na Necessidade de Conhecer, de acordo com o respectivo Direito em vigor.

3. A Autoridade Nacional de Segurança da Parte visitante notificará a visita planeada à autoridade competente da Parte anfitriã, endereçando um pedido de visita com uma antecedência mínima de trinta dias anterior à data prevista para a visita.
4. Em casos urgentes, o pedido para uma visita poderá ser efectuado com uma antecedência mínima de sete dias.
5. O pedido de visita deverá incluir:
   a) O primeiro e último nome do visitante, a data e o local de nascimento, nacionalidade e o número do passaporte ou do bilhete de identidade;
   b) O nome da entidade que o visitante representa ou a que pertence;
   c) Nome e morada da entidade a visitar;
   d) Certificado da Credenciação de Segurança do Pessoal do visitante e a respectiva validade;
   e) Objecto e propósito da visita ou visitas;
   f) A data prevista para a visita ou visitas e respectiva duração, e em caso de visitas recorrentes, o período total das visitas;
   g) Nome e número de telefone de contacto da instituição ou instalação a visitar, os contactos prévios e qualquer outra informação que seja útil para justificar a visita ou visitas;
   h) A data, a assinatura e a aposição do selo oficial da Autoridade Nacional de Segurança competente.
6. As visitas de cidadãos de um terceiro Estado que impliquem acesso a informação Classificada serão autorizadas mediante concordância entre as Partes.
7. A Autoridade Nacional de Segurança da Parte anfitriã deverá informar o responsável de segurança da entidade a ser visitada sobre os dados das pessoas autorizadas a realizar a visita.

8. Para visitas recorrentes a validade da autorização da visita não deverá exceder os doze meses.

9. Para qualquer projecto, programa ou contrato, as Autoridades Nacionais de Segurança podem acordar em elaborar listas de pessoas autorizadas a efectuar visitas recorrentes. Essas listas são válidas por um período inicial de doze meses, renovável.

10. Após aprovação das listas pelas Autoridades Nacionais de Segurança, os termos das visitas específicas podem ser directamente acordados com as autoridades competentes dos organismos a visitar pelas pessoas que constam daquelas listas, segundo os termos e condições acordados.

ARTIGO 12.º
QUEBRA E COMPROMETIMENTO DE SEGURANÇA

1. Em caso de quebra ou comprometimento de segurança que resulte em comprometimento ou suspeita de comprometimento de Informação Classificada com origem ou recebida da outra Parte, a Autoridade Nacional de Segurança da Parte onde ocorre a quebra ou o comprometimento informará prontamente a Autoridade Nacional de Segurança da outra Parte e instaurará a investigação apropriada.

2. Se a quebra ou comprometimento de segurança ocorrer num outro Estado, que não o das Partes, a Autoridade Nacional de Segurança da Parte despachante tomará as medidas descritas no número 1 do presente Artigo.

3. A outra Parte, se necessário, cooperará na investigação.

4. Em qualquer caso, a outra Parte deverá ser informada, por escrito, dos resultados da investigação. A informação deverá incluir a indicação das razões da quebra e comprometimento da segurança, a extensão dos danos e as conclusões da investigação.

ARTIGO 13.º
ENCARGOS

Cada Parte assumirá os encargos que para si advenham da aplicação e supervisão do presente Acordo.

ARTIGO 14.º
CONSULTAS

1. Por forma a garantir e a manter graus de segurança semelhantes, as Autoridades Nacionais de Segurança, se assim for solicitado, deverão trocar informação acerca dos níveis de segurança, procedimentos e práticas para a protecção de Informação Classificada.
2. As Autoridades Nacionais de Segurança das Partes consultar-se-ão, se assim for solicitado, a fim de assegurar uma estreita cooperação na implementação do presente Acordo.
3. Cada Parte pode autorizar que representantes da Autoridade Nacional de Segurança da outra Parte se desloquem ao seu território por forma a discutir os procedimentos de protecção de Informação Classificada transmitida pela outra Parte.

ARTIGO 15.º
SOLUÇÃO DE CONTROVÉRSIAS

Qualquer diferendo sobre a interpretação ou a aplicação do presente Acordo será resolvido por via diplomática.

ARTIGO 16.º
REVISÃO

1. A pedido de qualquer das Partes, o presente Acordo pode ser objecto de revisão por consentimento mútuo escrito.
2. As emendas entrarão em vigor nos termos previstos no Artigo 17.º do presente Acordo.

ARTIGO 17.º
ENTRADA EM VIGOR

O presente Acordo entrará em vigor no trigésimo dia após a recepção da última notificação, por escrito e por via diplomática, de que foram cumpridos os requisitos do internos das Partes necessários para o efeito.

ARTIGO 18.º
VIGÊNCIA E DENÚNCIA

1. O presente Acordo permanecerá em vigor por um período de tempo ilimitado.
2. Qualquer das Partes poderá, a qualquer momento, denunciar o presente Acordo através de notificação prévia, por escrito e por via diplomática.
3. O presente Acordo cessará a sua vigência seis meses após a data da recepção da notificação.
4. Em caso de denúncia, a Informação Classificada trocada na vigência do presente Acordo continuará a ser tratada em conformidade com as disposições do mesmo, a não ser que as Partes acordem de outra forma.

Feito em Lisboa, aos 2 de Agosto de 2007, em dois originais, em polaco, português e inglês, fazendo qualquer dos textos igualmente fé. Em caso de divergência na interpretação, o texto em inglês prevalecerá.

PELA REPÚBLICA DA POLÓNIA PELA REPÚBLICA PORTUGUESA

AGREEMENT
between the Republic of Poland
and
the Portuguese Republic
on Mutual Protection
of Classified Information

The Republic of Poland

and

the Portuguese Republic

hereinafter referred to as the "Parties",

Having due regard for guaranteeing mutual protection of all information which has been classified pursuant to the law of each Party

and transmitted to the other Party by competent authorities

or authorised persons;

Desiring to create a set of rules on the mutual protection of Classified Information exchanged between the Parties,

have agreed as follows:

ARTICLE 1
OBJECT OF THE AGREEMENT

The present Agreement establishes the security rules applicable to any contract, envisaging the transmission of Classified Information, which is signed or is to be signed between the adequate national authorities of both Parties or by entities duly authorised to that purpose.

ARTICLE 2
SCOPE OF APPLICATION

The present Agreement sets out procedures for the protection of Classified Information exchanged between the Parties.

ARTICLE 3

DEFINITIONS

For the purposes of the present Agreement:

a) "Classified Information", means the information, documents and materials, regardless of their form, nature, and means of transmission, determined to require protection against unauthorised disclosure, which has been so designated by security classification;

b) "National Security Authority" means the appropriated authority responsible for the implementation and supervision of the present Agreement;

c) "The Transmitting Party", means the Party, which gives or transmits Classified Information to the other Party;

d) "The Receiving Party" means the Party to which Classified Information is given or transmitted by the Transmitting Party;

e) "Third Party" means any international organisation or state that is not a Party to the present Agreement;

f) "Classified Contract" means an agreement creating and defining enforceable rights and obligations between two or more Contractors in case when the agreement contains or involves access to Classified Information;

g) "Contractor" means an individual or a legal entity possessing the legal capacity to conclude contracts;

h) "Personnel Security Clearance" means the determination by the National Security Authority or other relevant authority that an individual is eligible to have access to Classified Information, in accordance with the law in force of each Party;

i) "Facility Security Clearance" means the determination by the National Security Authority or other relevant authority that, from a security point of view, a facility has the physical and organisational capability to use and deposit Classified Information, in accordance with the law in force of each Party;

j) "Need-to-know" means the access to Classified Information that may only be granted to a person who has a verified requirement for

knowledge of, or possession of such information in order to perform his official and professional duties;

k) "Project Security Instruction" means a compilation of security requirements, which are applied to a specific project in order to standardise security procedures;

l) "Project Security Classification Guide" means the part of the Project Security Instruction which identifies the elements of the project that are classified, specifying the security classification levels.

ARTICLE 4

RESPONSIBLE AUTHORITIES

1. The National Security Authorities are:

For the Republic of Poland:

- in the civil sphere

Szef Agencji Bezpieczeństwa Wewnętrznego

ul. Rakowiecka 2A

00-993 Warszawa

Polska

- in the military sphere

Szef Służby Kontrwywiadu Wojskowego

ul Oczki 1

02-007 Warszawa

Polska

For the Portuguese Republic:

Autoridade Nacional de Segurança

Presidência do Conselho de Ministros

Av. Ilha da Madeira, 1

1400-204 Lisboa

Portugal

2. The Parties shall inform each other, through diplomatic channels, about any modification concerning the information provided in paragraph 1 of the present Article.

ARTICLE 5

SECURITY CLASSIFICATIONS AND EQUIVALENCES

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the law in force of each Party:

THE REPUBLIC OF POLAND	THE PORTUGUESE REPUBLIC	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	MUITO SECRETO	TOP SECRET
TAJNE	SECRETO	SECRET
POUFNE	CONFIDENCIAL	CONFIDENTIAL
ZASTRZEŻONE	RESERVADO	RESTRICTED

ARTICLE 6

SECURITY RULES

1. Each Party shall ensure that all entities comply with the measures to protect Classified Information which is transmitted under the present Agreement or produced or developed in connection with a Classified Contract or any relation between the Parties.
2. The Parties shall afford all transmitted, produced or developed Classified Information the same degree of security protection as provided for their own Classified Information of the equivalent level, as defined in Article 5 of the present Agreement.
3. Access to Classified Information is restricted to persons who, in order to perform their duties, have access to Classified Information on a Need-to-know basis, hold an appropriate Personnel Security Clearance and have been authorised by the appropriate authorities.

4. The Receiving Party shall mark the received Classified Information with its own equivalent security classification, in accordance with the equivalences referred in Article 5 of the present Agreement.

5. The Parties shall inform each other about all subsequent classification alterations to the transmitted Classified Information.

6. The Receiving Party and/or entities from its State shall neither downgrade nor declassify the received Classified Information without the prior written consent of the Transmitting Party.

7. The transmitted Classified Information shall be used only for the purpose that it was transmitted for, under the agreements concluded between the Parties or contracts signed between entities.

8. The Receiving Party shall not transmit the Classified Information to a Third Party, or to an individual holding the citizenship of a third State, or to an entity of a third State, without prior written authorisation from the Transmitting Party.

ARTICLE 7

CO-OPERATION ON SECURITY CLEARANCE

1. On request, the National Security Authorities, taking into account the law in force of each Party, shall assist each other during the clearance procedures preceding the issue of the Personnel Security Clearance and the Facility Security Clearance.

2. The Parties shall recognise the Personnel Security Clearance or the Facility Security Clearance issued in accordance with the law in force of the other Party. The equivalence of the security clearances shall be in compliance with Article 5 of the present Agreement.

3. The National Security Authorities shall inform each other about any changes of the Personnel Security Clearance and Facility Security Clearance, related to the application of the present Agreement, particularly concerning cases of withdrawal or downgrading of their classification level.

ARTICLE 8

TRANSLATION, REPRODUCTION AND DESTRUCTION

1. Classified Information marked as ŚCIŚLE TAJNE/MUITO SECRETO/TOP SECRET shall be translated or reproduced only upon the written permission of the National Security Authority of the Transmitting Party.
2. Translations and reproductions of Classified Information shall be made in accordance with the following procedures:
   a) The persons translating or reproducing shall hold the appropriate Personnel Security Clearance;
   b) The translations and the reproductions shall be marked and given the same protection as the original information;
   c) The translations and the number of reproductions shall be limited to the required official purposes;
   d) The translations shall bear an appropriate note in the language into which it is translated indicating that it contains Classified Information received from the Transmitting Party.
3. Classified Information marked as ŚCIŚLE TAJNE/MUITO SECRETO/TOP SECRET shall not be destroyed and it shall be returned to the National Security Authority of the Transmitting Party.
4. Destruction of Classified Information marked as TAJNE/SECRETO/ SECRET shall be notified to the Transmitting Party.

5. Classified Information marked up to POUFNE/CONFIDENCIAL/ CONFIDENTIAL, including, shall be destroyed in accordance with the law in force of each Party.

ARTICLE 9
TRANSMISSION BETWEEN THE PARTIES

1. Classified Information shall be transmitted between the Parties through diplomatic channels.
2. If the use of such channels would be impractical or would unduly delay the receipt of the Classified Information, transmissions may be undertaken by appropriately security cleared personnel empowered with a courier certificate issued by the Party which transmits the Classified Information.
3. The Parties may transmit Classified Information by electronic means in accordance with security procedures mutually approved by National Security Authorities.
4. Delivery of a large volume of Classified Information arranged on a case-by-case basis shall be approved by both National Security Authorities.
5. The Receiving Party shall confirm the receipt of the Classified Information in writing.

ARTICLE 10
CLASSIFIED CONTRACTS

1. One Party, wishing to place a Classified Contract with a Contractor of the other Party or wishing to authorise one of its own Contractors to place a Classified Contract in the territory of the other Party within a classified project shall obtain, through its National Security Authority,

prior written assurance from the National Security Authority of the other Party that the proposed Contractor holds a Facility Security Clearance of the appropriate level.

2. The Contractor commits itself to:

   a) Having a proper level of Facility Security Clearance granted to those facilities;

   b) Having a proper level of Personnel Security Clearance granted to persons who perform functions that require access to Classified Information;

   c) Ensuring that all persons with access to Classified Information are informed of their responsibilities for the protection of Classified Information, according to the law in force of each Party;

   d) Allowing security inspections of its facilities.

3. Any subcontractor must fulfil the same security obligations as the Contractor.

4. The National Security Authority holds the competence to assure the compliance of the Contractor with the commitments set in paragraph 2 of the present Article.

5. Every Classified Contract concluded between entities of the Parties, under the provisions of the present Agreement, shall include a Project Security Instruction identifying the following aspects:

   a) Project Security Classification Guide and the list of Classified Information;

   b) Procedure for the notification of changes in the classification of information;

   c) Communication channels and means for electromagnetic transmission;

d) Procedure for the transportation of Classified Information;

e) Relevant authorities responsible for the co-ordination of the safeguarding of Classified Information related to the Contract;

f) An obligation to notify any actual or suspected loss, leak or compromise of the Classified Information.

6. Copy of the Project Security Instruction of any Classified Contract shall be forwarded to the National Security Authority of the Party where the Classified Contract is to be performed to allow adequate security supervision and control.

7. Representatives of the National Security Authorities may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract. Notice of the visit shall be provided, at least, thirty days in advance.

ARTICLE 11

VISITS

1. Visits entailing access to Classified Information by citizens of one Party to the other Party are subject to prior written authorisation given by the appropriate National Security Authority of the host Party.

2. Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party only if they have been:

a) Granted appropriate Personnel Security Clearance by the appropriate National Security Authority or other relevant authority of the sending Party;

b) Authorised to receive or to have access to Classified Information on a Need-to- know basis, in accordance with the law in force.

3. The National Security Authority of the sending Party shall notify the National Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least thirty days before the visit or visits take place.

4. In urgent cases, the request for visit shall be transmitted at least seven days in advance.

5. The request for visit shall include:

   a) Visitor's first and last name, place and date of birth, citizenship, passport or identity card number;

   b) Name of the entity which the visitor represents or to which the visitor belongs;

   c) Name and address of entity to be visited;

   d) Certification of the visitor's Personnel Security Clearance and its validity;

   e) Object and purpose of the visit or visits;

   f) Expected date and duration of the requested visit or visits and, in case of recurring visits, the total period covered by the visits;

   g) Name and phone number of the point of contact at the facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;

   h) The date, signature and the official seal of the appropriate National Security Authority.

6. Visits entailing access to Classified Information by citizens from a third State shall only be authorised by a common agreement between the Parties.

7. The National Security Authority of the host Party shall inform the security officer of the entity to be visited about the data of the persons approved for a visit.

8. For recurring visits the validity of visit authorisation shall not exceed twelve months.

9. For any project, program or contract the National Security Authorities may agree to establish lists of authorised persons to make recurring visits. Those lists are valid for an initial period of twelve months that can be renewed.

10. Once those lists have been approved by the National Security Authorities, the terms of the specific visits shall be directly arranged with the representatives of the entities to be visited by those persons, in accordance with the terms and conditions agreed upon.

ARTICLE 12
BREACH AND COMPROMISE OF SECURITY

1. In case of breach or compromise of security that results in a certain or suspected compromise of Classified Information originated by or received from the other Party, the National Security Authority of the Party where the breach or compromise occurs shall inform the National Security Authority of the other Party, as soon as possible, and carry out the appropriate investigation.

2. If a breach or compromise of security occurs in a State other than the Parties, the National Security Authority of the despatching Party shall take the actions prescribed in paragraph 1 of the present Article.

3. The other Party shall, if required, co-operate in the investigation.

4. In any case, the other Party shall be informed of the results of the investigation in writing. The information shall include the reasons for the breach or the compromise of security, the extent of the damage and the conclusions of the investigation.

ARTICLE 13
EXPENSES

Each Party shall bear its own expenses incurred in connection with the application and supervision of all aspects of the present Agreement.

ARTICLE 14
CONSULTATIONS

1. In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about their security standards, procedures and practices for protection of Classified Information.
2. The National Security Authorities of the Parties shall, on request, consult each other, in order to ensure close cooperation in the implementation of the present Agreement.
3. Each Party may allow the representatives of the National Security Authority of the other Party to come to its own territory to discuss the procedures for protection of Classified Information transmitted by the other Party.

ARTICLE 15
SETTLEMENT OF DISPUTES

Any dispute concerning the interpretation or application of the present Agreement shall be settled through diplomatic channels.

ARTICLE 16
AMENDMENTS

1. On request of one of the Parties, the present Agreement may be amended on the basis of mutual written consent.
2. The amendments shall enter into force in accordance with the terms specified in Article 17 of the present Agreement.

ARTICLE 17
ENTRY INTO FORCE

The present Agreement shall enter into force on the thirtieth day following the receipt of the last written notification, through diplomatic channels, stating that all the internal requirements of each Party necessary for the entry into force have been fulfilled.

ARTICLE 18
DURATION AND TERMINATION

1. The present Agreement is concluded for an unlimited period of time.
2. Either Party may, at any time, through diplomatic channels, terminate the present Agreement upon a prior written notification.
3. The present Agreement shall terminate six months after the receipt of such notification.

4. Notwithstanding the termination, all Classified Information transmitted pursuant to the present Agreement shall continue to be protected in accordance with the provisions set forth herein, unless both Parties agree otherwise.

Done at .....Lisbon....., on August 2, 2007 in two originals, each one in the Polish, Portuguese and English languages, all texts being equally authentic. In case of any divergence of interpretation the English text shall prevail.

FOR THE REPUBLIC OF POLAND

FOR THE PORTUGUESE REPUBLIC

Po zaznajomieniu się z powyższą umową, w imieniu Rzeczypospolitej Polskiej oświadczam, że:

— została ona uznana za słuszną zarówno w całości, jak i każde z postanowień w niej zawartych,

— jest przyjęta, ratyfikowana i potwierdzona,

— będzie niezmiennie zachowywana.

Na dowód czego wydany został akt niniejszy, opatrzony pieczęcią Rzeczypospolitej Polskiej.

Dano w Warszawie dnia 15 lipca 2008 r.

Prezydent Rzeczypospolitej Polskiej: *L. Kaczyński*

L.S.

Prezes Rady Ministrów: *D. Tusk*