Warszawa, dnia 1 marca 2012 r.

Pozycja 232

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o wzajemnej ochronie informacji niejawnych,

podpisana w Hanoi dnia 9 września 2010 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 9 września 2010 r. w Hanoi została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Socjalistycznej Republiki Wietnamu o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Socjalistycznej Republiki Wietnamu,

zwane dalej „Stronami”,

mając na uwadze zagwarantowanie wzajemnej ochrony wszystkich informacji, które zostały zakwalifikowane jako informacje niejawne zgodnie z prawem wewnętrznym jednej ze Stron i przekazane drugiej Stronie lub powstały w wyniku współpracy,

kierując się zamiarem stworzenia regulacji w zakresie wzajemnej ochrony informacji niejawnych, która obowiązywać będzie w odniesieniu do wszelkiej wspólnej działalności związanej z wymianą informacji niejawnych przyjmując, że niniejsza Umowa nie narusza obowiązków żadnej ze Stron w odniesieniu do traktatów i umów zawartych przez Strony,

uzgodniły co następuje:

ARTYKUŁ 1
DEFINICJE

W rozumieniu niniejszej Umowy następujące definicje oznaczają:

1) „informacje niejawne" – wszelkie informacje niezależnie od formy, nośnika i sposobu ich utrwalenia oraz przedmioty lub dowolne ich części, które wymagają ochrony przed nieuprawnionym ujawnieniem zgodnie z prawem wewnętrznym każdej ze Stron i niniejszą Umową;
2) „właściwe organy" – organy, o których mowa w artykule 3 niniejszej Umowy;
3) „upoważnione podmioty" – osoby fizyczne, osoby prawne lub inne jednostki organizacyjne właściwe do przekazywania, otrzymywania, przechowywania, ochrony i wykorzystywania informacji niejawnych zgodnie z prawem wewnętrznym swojej Strony, w tym także właściwe organy;
4) „kontrakt niejawny" – umowę, której realizacja wiąże się z dostępem do informacji niejawnych, bądź z wytworzeniem takich informacji;
5) „kontrahent" – osobę fizyczną, osobę prawną albo jednostkę organizacyjną, która posiada zdolność do zawierania umów;
6) „zamawiający" – podmiot, który posiada zdolność do zlecania kontraktu niejawnego;
7) „Strona wytwarzająca" – Stronę, osobę fizyczną oraz każdy podmiot publiczny lub prywatny znajdujący się pod jej jurysdykcją, która wytwarza i przekazuje informacje niejawne drugiej Stronie;
8) „Strona otrzymująca" – Stronę, osobę fizyczną oraz każdy podmiot publiczny lub prywatny znajdujący się pod jej jurysdykcją, która otrzymuje informacje niejawne od drugiej Strony;

9) „Strona trzecia" – państwo, osobę fizyczną albo każdy podmiot publiczny lub prywatny znajdujący się pod jego jurysdykcją, jak również każdą organizację międzynarodową, nie będącą Stroną niniejszej Umowy.

ARTYKUŁ 2
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności zgodnie z prawem wewnętrznym Strony wytwarzającej. Strona otrzymująca gwarantuje równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami ustępu 3.
2. Klauzula tajności może być zmieniona lub zniesiona wyłącznie przez upoważniony podmiot, który ją nadał. Strona otrzymująca jest pisemnie informowana o każdym przypadku zmiany lub zniesienia klauzuli tajności wcześniej otrzymanych informacji niejawnych.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	SOCJALISTYCZNA REPUBLIKA WIETNAMU	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	TUYỆT MẬT	TOP SECRET
TAJNE	TỐI MẬT	SECRET
POUFNE	MẬT	CONFIDENTIAL

4. Informacje otrzymane z Rzeczypospolitej Polskiej oznaczone klauzulą tajności jako ZASTRZEŻONE są chronione jako MẬT w Socjalistycznej Republice Wietnamu.

ARTYKUŁ 3
WŁAŚCIWE ORGANY

W rozumieniu niniejszej Umowy właściwymi organami są:

1) W Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego – w sferze cywilnej i Szef Służby Kontrwywiadu Wojskowego – w sferze wojskowej.
2) w Socjalistycznej Republice Wietnamu: Minister Bezpieczeństwa Publicznego – w sferze cywilnej i Minister Obrony Narodowej – w sferze wojskowej.

ARTYKUŁ 4
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Zgodnie z niniejszą Umową i prawem wewnętrznym, Strony podejmą stosowne działania w celu ochrony informacji niejawnych, które będą przekazywane lub wytwarzane w wyniku wspólnej działalności Stron lub upoważnionych podmiotów, w tym także w związku z realizacją kontraktu niejawnego.
2. Strona otrzymująca wykorzystuje informacje niejawne wyłącznie w celach określonych przy ich przekazaniu.
3. Strona otrzymująca nie udostępnia informacji, o których mowa w ustępie 1 stronom trzecim bez uprzedniej pisemnej zgody Strony wytwarzającej.

4. Informacje niejawne mogą być udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które po przeprowadzeniu niezbędnego postępowania sprawdzającego zostały upoważnione do dostępu do nich oraz zostały przeszkolone w zakresie ochrony informacji niejawnych, zgodnie z prawem wewnętrznym Strony otrzymującej.

ARTYKUŁ 5
POŚWIADCZENIA BEZPIECZEŃSTWA I ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Dla celów określonych niniejszą Umową Strony uznają wzajemnie zapewnienia o spełnianiu bezpieczeństwa osobowego oraz zapewnienia o bezpieczeństwie przemysłowym wydane zgodnie z prawem wewnętrznym Stron.

ARTYKUŁ 6
KONTRAKTY NIEJAWNE

1. Zamawiający może zawrzeć kontrakt niejawny z kontrahentem.
2. W przypadku, o którym mowa w ustępie 1, zamawiający składa wniosek do właściwego organu swojej Strony, o wystąpienie do właściwego organu drugiej Strony, z prośbą o wydanie pisemnego zapewnienia, że kontrahent posiada zapewnienie bezpieczeństwa przemysłowego oznaczone odpowiednią klauzulą tajności.
3. Udzielenie zapewnienia, o którym mowa w ustępie 2, jest równoznaczne z gwarancją, że zostały przeprowadzone czynności niezbędne do stwierdzenia, że kontrahent spełnia warunki w zakresie ochrony informacji niejawnych określone w prawie wewnętrznym Strony, na terytorium której posiada siedzibę.

4. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zapewnienia, o którym mowa w ustępach 2 i 3.
5. Zamawiający przekazuje kontrahentowi instrukcję bezpieczeństwa przemysłowego niezbędną do realizacji kontraktu niejawnego, która jest nieodłączną częścią każdego kontraktu niejawnego. Instrukcja ta zawiera postanowienia dotyczące wymogów bezpieczeństwa, w szczególności:
   1) wykaz rodzajów informacji niejawnych odnoszących się do danego kontraktu niejawnego, z uwzględnieniem ich klauzul tajności;
   2) zasady przyznawania klauzul tajności informacjom wytworzonym podczas realizacji danego kontraktu niejawnego.
6. Kopia instrukcji bezpieczeństwa przemysłowego przekazywana jest właściwemu organowi Strony, na terytorium której kontrahent posiada siedzibę.
7. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych będzie możliwa po zakończeniu przez kontrahenta niezbędnych działań zapewniających ochronę informacji niejawnych, zgodnie z odpowiednią instrukcją bezpieczeństwa przemysłowego .
8. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie ustalono dla kontrahenta.

ARTYKUŁ 7
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

Informacje niejawne będą przekazywane drogą dyplomatyczną albo w inny sposób zapewniający ochronę przed nieuprawnionym ujawnieniem, uzgodniony przez właściwe organy Stron w trybie określonym w Artykule 14 ustęp 4. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.

ARTYKUŁ 8
POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/ TUYỆT MẬT będą powielane i tłumaczone tylko po uprzednim wydaniu pisemnego zezwolenia przez upoważniony podmiot.
2. Powielanie i tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem wewnętrznym każdej ze Stron. Powielone i przetłumaczone informacje podlegają takiej samej ochronie jak oryginały. Liczba kopii i tłumaczeń będzie ograniczona do liczby wymaganej dla celów służbowych.

ARTYKUŁ 9
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne, z zastrzeżeniem ustępu 2, będą niszczone zgodnie z prawem wewnętrznym Strony otrzymującej w taki sposób, żeby uniemożliwić ich częściowe lub całkowite odtworzenie.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/ TUYỆT MẬT nie będą niszczone. Będą one zwracane Stronie wytwarzającej.

ARTYKUŁ 10
WIZYTY

1. Osobom przybywającym z wizytą z jednej Strony do drugiej Strony zezwala się na dostęp do informacji niejawnych, tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ drugiej Strony.

2. Co najmniej 30 dni przed planowaną wizytą, właściwy organ strony przyjmującej wizytę powinien otrzymać wniosek w sprawie wizyty od właściwego organu drugiej Strony.
3. Wniosek w sprawie wizyty, o którym mowa w ustępie 2 powinien zawierać:
   1) cel, termin i program wizyty;
   2) imię i nazwisko osoby przybywającej z wizytą, datę i miejsce urodzenia, obywatelstwo, numer paszportu;
   3) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą instytucji lub jednostki, którą reprezentuje;
   4) potwierdzenie poziomu oraz daty ważności zapewnienia bezpieczeństwa, jakie posiada osoba przybywająca z wizytą;
   5) nazwę i adres odwiedzanej jednostki;
   6) imię, nazwisko oraz stanowisko służbowe osoby przyjmującej.
4. Do ochrony danych osobowych przekazywanych w związku z postanowieniami ustępu 3 stosuje się, z uwzględnieniem przepisów prawa wewnętrznego każdej ze Stron, następujące postanowienia:
   1) wykorzystanie danych osobowych przez stronę przyjmującą wizytę jest dopuszczalne wyłącznie w celu oraz na warunkach określonych przez drugą stronę;
   2) strona przyjmująca wizytę nie przechowuje danych osobowych dłużej, aniżeli jest to niezbędne dla osiągnięcia celu przetwarzania;
   3) w przypadku przekazania danych, których nie wolno było przekazać zgodnie z prawem wewnętrznym strony, strona przekazująca dane osobowe zawiadamia o tym stronę przyjmującą wizytę, która jest zobowiązana do usunięcia tych danych;

4) strona przekazująca dane osobowe odpowiada za poprawność przekazywanych danych i jeśli okaże się, że przekazane zostały dane nieprawdziwe lub niekompletne, zawiadamia o tym stronę przyjmującą wizytę, która jest zobowiązana do sprostowania lub usunięcia tych danych;

5) strona przekazująca dane osobowe oraz strona przyjmująca wizytę są zobowiązane do rejestrowania przekazywania, otrzymywania i usuwania danych osobowych;

6) strona przekazująca oraz strona przyjmująca wizytę są zobowiązane do skutecznego zabezpieczania przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, nieuprawnionym dokonywaniem zmian tych danych, ich utratą, uszkodzeniem lub zniszczeniem.

ARTYKUŁ 11
NARUSZENIE REGULACJI DOTYCZĄCYCH WZAJEMNEJ OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących ochrony informacji niejawnych jest wynik działania lub zaniechania osoby fizycznej, które jest sprzeczne z niniejszą Umową i prawem wewnętrznym Stron. Odnosi się to również do nieuprawnionego ujawnienia informacji niejawnych.
2. Informacja o każdym przypadku naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych Strony wytwarzającej lub informacji niejawnych wytworzonych w wyniku wspólnego działania Stron będzie niezwłocznie przekazywana właściwemu organowi Strony, na terytorium której miało miejsce lub zaistniało podejrzenie takiego naruszenia.

3. Każdy przypadek naruszenia lub podejrzenie naruszenia regulacji dotyczących ochrony informacji niejawnych będzie wyjaśniany zgodnie z prawem wewnętrznym Strony, na terytorium której zdarzenie miało miejsce.
4. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, o których mowa w ustępie 1, właściwy organ Strony na terytorium której naruszenie miało miejsce, pisemnie informuje właściwy organ drugiej Strony o tym fakcie, okolicznościach naruszenia oraz wyniku czynności, o których mowa w ustępie 3.
5. Na wniosek, właściwe organy Stron współpracują przy czynnościach, o których mowa w ustępie 3.

ARTYKUŁ 12
JĘZYKI

W zakresie stosowania postanowień niniejszej Umowy, Strony używają swoich języków urzędowych, dołączając tłumaczenie na język urzędowy drugiej Strony lub na język angielski.

ARTYKUŁ 13
KOSZTY

Każda ze Stron pokrywa koszty własne, poniesione w związku z realizacją postanowień niniejszej Umowy.

ARTYKUŁ 14
KONSULTACJE

1. Właściwe organy Stron informują się wzajemnie o wszelkich zmianach w swoim prawie wewnętrznym w zakresie ochrony informacji niejawnych, które dotyczą postanowień niniejszej Umowy.

2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy Stron konsultują się na wniosek jednego z tych organów.
3. Każda ze Stron zezwoli przedstawicielom właściwego organu drugiej Strony na składanie wizyt na swoim terytorium w celu omówienia procedur służących ochronie informacji niejawnych, które zostały jej przekazane przez drugą Stronę.
4. W celu zapewnienia skutecznej współpracy, będącej przedmiotem niniejszej Umowy, i w zakresie kompetencji przyznanych im prawem wewnętrznym, właściwe organy mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne lub organizacyjne.

ARTYKUŁ 15
ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące stosowania niniejszej Umowy będą rozstrzygane w drodze bezpośrednich rozmów między właściwymi organami Stron.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, będzie on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 16
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa wejdzie w życie zgodnie z prawem wewnętrznym każdej ze Stron, co zostanie stwierdzone w drodze wymiany not. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.

2. Umowa niniejsza zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim przypadku utraci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
3. W przypadku wypowiedzenia, informacje niejawne chronione na podstawie niniejszej Umowy, będą nadal chronione zgodnie z postanowieniami niniejszej Umowy tak długo, jak wymaga tego obowiązywanie klauzuli tajności.
4. Niniejsza Umowa może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1 niniejszego artykułu i stanowią integralną część Umowy.

Sporządzono w Hanoi..... dnia 03/09/2010 roku w dwóch egzemplarzach, każdy w językach polskim, wietnamskim i angielskim, przy czym wszystkie teksty są jednakowo autentyczne. W przypadku rozbieżności przy ich interpretacji tekst w języku angielskim uważany będzie za rozstrzygający.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ

Z UPOWAŻNIENIA RZĄDU SOCJALISTYCZNEJ REPUBLIKI WIETNAMU

HIỆP ĐỊNH
GIỮA
CHÍNH PHỦ CỘNG HÒA BA LAN
VÀ
CHÍNH PHỦ CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
VỀ CÙNG BẢO VỆ TIN MẬT

Chính phủ Cộng hòa Ba Lan và Chính phủ Cộng hòa xã hội chủ nghĩa Việt Nam, sau đây gọi là "các Bên",

Coi trọng đảm bảo việc cùng bảo vệ tất cả tin được xác định là mật theo pháp luật của mỗi Bên và được chuyển cho Bên kia hoặc được tạo lập trong quá trình hợp tác,

Được chỉ dẫn bởi việc xây dựng các quy định trong lĩnh vực cùng bảo vệ tin mật có tính chất ràng buộc liên quan tới hợp tác song phương gắn với việc trao đổi tin mật,

Khẳng định rằng Hiệp định này không ảnh hưởng tới bất kì nghĩa vụ nào của mỗi Bên có liên quan đến các điều ước quốc tế hoặc thoả thuận quốc tế mà các Bên là thành viên,

Đã thoả thuận như sau:

Điều 1
GIẢI THÍCH TỪ NGỮ

Theo quy định của Hiệp định này, các từ ngữ dưới đây được hiểu như sau:

1. "Tin mật" là bất kỳ thông tin nào không phân biệt hình thức, nơi chứa và tính chất lưu giữ và các đối tượng hoặc một phần của đối tượng cần được bảo vệ để chống lại việc tiết lộ bất hợp pháp theo quy định của pháp luật mỗi Bên và theo quy định của Hiệp định này;

2. "Những người có thẩm quyền" là những người được nêu tại Điều 3 của Hiệp định này;

3. "Các đối tượng có thẩm quyền" là các cá nhân, pháp nhân hoặc các tổ chức có thẩm quyền chuyển, nhận, lưu giữ, bảo vệ và sử dụng tin mật phù hợp với luật pháp của mỗi Bên, bao gồm cả những người có thẩm quyền;

4. "Hợp đồng mật" là thoả thuận mà việc thực hiện thoả thuận đó có liên quan tới việc tiếp cận tin mật hoặc nguồn của tin đó;

5. "Bên ký kết hợp đồng mật" là một cá nhân, pháp nhân hoặc tổ chức có tư cách pháp lý để ký kết hợp đồng;

6. "Bên ủy nhiệm" là một cơ quan có tư cách pháp lý đưa ra Hợp đồng mật;

7. "Bên cung cấp tin" là Bên mà cá nhân và tất cả tổ chức nhà nước hoặc tư nhân trong phạm vi thẩm quyền của mình tạo lập và thực hiện việc chuyển giao tin mật cho Bên kia;

8. "Bên nhận tin" là Bên mà cá nhân và mọi tổ chức nhà nước hoặc tư nhân trong phạm vi thẩm quyền của mình thực hiện việc nhận tin mật từ Bên kia;

9. "Bên thứ ba" là một Nhà nước, một cá nhân hoặc mọi tổ chức nhà nước hoặc tư nhân có thẩm quyền cũng như các tổ chức quốc tế, không phải là một Bên của Hiệp định này.

Điều 2
CẤP ĐỘ TIN MẬT

1. Tin mật được xác định cấp độ bảo mật tùy thuộc nội dung của tài liệu đó theo quy định pháp luật của Bên cung cấp tin. Bên nhận tin phải đảm bảo cấp độ bảo vệ tương đương đối với tin mật đã nhận được, theo quy định tại Khoản 3.

2. Cấp độ mật chỉ được thay đổi hoặc huỷ bỏ bởi các cơ quan có thẩm quyền đã xác định cấp độ mật đó. Bên nhận tin sẽ được thông báo bằng văn bản về sự thay đổi hoặc huỷ bỏ cấp độ mật của tin mật đã nhận được trước đó.

3. Các Bên đồng ý rằng các cấp độ mật tương đương như sau:

Cộng hòa Ba Lan	Cộng hòa xã hội chủ nghĩa Việt Nam	Tương đương trong tiếng Anh
ŚCIŚLE TAJNE	TUYỆT MẬT	TOP SECRET
TAJNE	TỐI MẬT	SECRET
POUFNE	MẬT	CONFIDENTIAL

4. Thông tin nhận được từ Cộng hoà Ba Lan được xác định là ZASTRZEŻONE sẽ được bảo vệ như thông tin MẬT tại Cộng hoà xã hội chủ nghĩa Việt Nam.

Điều 3
NHỮNG NGƯỜI CÓ THẨM QUYỀN

Theo quy định của Hiệp định này, những người có thẩm quyền sẽ là:

1. Đối với Cộng hòa Ba Lan: Người đứng đầu của Cơ quan An ninh nội địa trong lĩnh vực dân sự và người đứng đầu của Cơ quan phản gián quân đội trong lĩnh vực quân sự.

2. Đối với Cộng hòa xã hội chủ nghĩa Việt Nam: Bộ trưởng Bộ Công an trong lĩnh vực dân sự và Bộ trưởng Bộ Quốc phòng trong lĩnh vực quân sự.

Điều 4
CÁC NGUYÊN TẮC BẢO VỆ TIN MẬT

1. Theo Hiệp định này và pháp luật của mỗi nước, các Bên sẽ thông qua các biện pháp phù hợp nhằm mục đích bảo vệ tin mật được chuyển giao hoặc có được do kết quả của hợp tác song phương giữa hai Bên, hoặc các đối tượng có thẩm quyền, kể cả tin có được liên quan tới việc thực hiện Hợp đồng mật.

2. Bên nhận tin chỉ được sử dụng tin mật vào các mục đích nêu tại thời điểm chuyển giao tin.

3. Bên nhận tin không được cung cấp tin nêu ở Khoản 1 cho Bên thứ 3 nếu không có sự đồng ý trước bằng văn bản của Bên cung cấp tin.

4. Tiếp cận tin mật chỉ dành cho những người có trách nhiệm và những người đã được uỷ quyền tiếp cận với các tin đó sau khi đã được chấp thuận đối với cấp độ mật tương ứng cũng như đã được thông báo về phạm vi bảo vệ tin mật theo pháp luật của Bên nhận tin.

Điều 5
CẤP PHÉP AN NINH

Theo quy định của Hiệp định này, các Bên sẽ công nhận lẫn nhau kết quả kiểm tra an ninh về con người và trang thiết bị được thực hiện theo quy định của nội luật của các Bên.

Điều 6
HỢP ĐỒNG MẬT

1. Bên uỷ nhiệm có thể ký kết Hợp đồng mật với một Bên ký kết hợp đồng.

2. Trong trường hợp nêu tại Khoản 1, Bên uỷ nhiệm sẽ đề nghị Người có thẩm quyền của Bên mình yêu cầu Người có thẩm quyền của Bên kia cấp một văn bản đảm bảo rằng Bên ký hợp đồng được phép tiếp cận với tin mật ở cấp độ mật cụ thể.

3. Việc cấp văn bản bảo đảm nêu tại Khoản 2 là tương đương với việc bảo đảm thực hiện các hoạt động cần thiết để xác nhận rằng Bên ký hợp đồng đã đáp ứng các tiêu chí về bảo vệ tin mật theo quy định pháp luật của Bên đó, trong lãnh thổ của nước mà Bên ký hợp đồng cư trú.

4. Bên ký hợp đồng chỉ được tiếp cận tin mật sau khi đã nhận được văn bản đảm bảo nêu tại Khoản 2 và Khoản 3.

5. Bên uỷ nhiệm sẽ thông báo cho Bên ký hợp đồng các chỉ dẫn an ninh cần thiết để thực hiện hợp đồng mật - một phần không thể tách rời của hợp đồng mật. Chỉ dẫn này bao gồm các quy định về các yêu cầu an ninh, cụ thể là:

1) Danh mục tin mật và cấp độ tin mật liên quan tới hợp đồng đã ký.

2) Các quy định để xác định cấp độ mật đối với những tin phát sinh trong quá trình thực hiện Hợp đồng.

6. Bản sao chỉ dẫn an ninh được chuyển cho Cơ quan có thẩm quyền của Bên mà Bên ký kết Hợp đồng đặt trụ sở.

7. Bên ký hợp đồng chỉ được thực hiện phần liên quan tới tiếp cận tin mật của Hợp đồng mật khi đáp ứng được các tiêu chí cần thiết để bảo vệ tin mật theo chỉ dẫn an ninh được áp dụng.

8. Bên ký hợp đồng phụ phải tuân thủ các điều kiện bảo vệ tin mật giống như những điều kiện đặt ra cho Bên ký hợp đồng.

Điều 7
CHUYỂN GIAO TIN MẬT

Tin mật được chuyển thông qua kênh ngoại giao hoặc các kênh khác được bảo mật để chống việc tiết lộ bất hợp pháp, theo thỏa thuận giữa những người có thẩm quyền của hai Bên, theo cách thức nêu tại Khoản 4 Điều 14. Bên nhận tin phải khẳng định bằng văn bản việc đã nhận được tin mật.

Điều 8
NHÂN BẢN VÀ DỊCH TIN MẬT

1. Tin ŚCIŚLE TAJNE/TUYỆT MẬT chỉ được nhân bản và dịch sau khi được đối tượng có thẩm quyền cho phép bằng văn bản.

2. Việc nhân bản và dịch tin mật phải phù hợp với pháp luật của mỗi Bên. Tin được nhân bản hoặc dịch phải được bảo vệ như bản gốc. Bản sao và bản dịch được giới hạn số lượng cần thiết cho những mục đích chính thức.

Điều 9
HỦY TIN MẬT

1. Trừ quy định tại Khoản 2, tin mật phải được huỷ theo quy định pháp luật của Bên nhận tin, theo cách loại bỏ hoàn toàn khả năng khôi phục một phần hoặc toàn bộ tin mật.

2. Tin ŚCIŚLE TAJNE/TUYỆT MẬT không được huỷ mà phải được gửi trả lại cho Bên cung cấp tin.

Điều 10
CÁC CHUYẾN THĂM

1. Người từ Bên này sang thăm Bên kia chỉ được phép tiếp cận với tin mật sau khi nhận được sự đồng ý trước bằng văn bản của người có thẩm quyền của Bên kia.

2. Cơ quan có thẩm quyền bên cử đoàn phải thông báo cho Cơ quan có thẩm quyền của bên tiếp nhận đoàn về yêu cầu chuyến thăm ít nhất 30 ngày trước thời gian dự kiến thực hiện chuyến thăm.

3. Yêu cầu của chuyến thăm nêu tại Khoản 2 bao gồm:

1) Mục đích, ngày và chương trình chuyến thăm;

2) Họ tên, ngày và nơi sinh, quốc tịch, số hộ chiếu của khách;
3) Chức vụ của khách và tên cơ quan họ đại diện;
4) Xác nhận về cấp độ mật và thời hạn được tiếp cận tin mật của khách;
5) Tên và địa chỉ nơi được đến thăm;
6) Họ tên và chức vụ của người được đến thăm.

4. Để bảo vệ tài liệu cá nhân được chuyển theo quy định tại Khoản 3 và nội luật của các Bên, những quy định sau sẽ được áp dụng:

1) Bên tiếp nhận chỉ được sử dụng tài liệu cá nhân nhận được với mục đích và các điều kiện mà Bên kia đã đề ra;
2) Bên tiếp nhận sẽ lưu giữ tài liệu tin cá nhân trong thời hạn cần thiết tùy theo mục đích của việc chuyển tài liệu đó.
3) Trường hợp tài liệu cá nhân được chuyển không phù hợp với nội luật của một Bên, Bên chuyển tài liệu phải thông báo cho Bên tiếp nhận để huỷ tài liệu đó.
4) Bên chuyển tài liệu có trách nhiệm kiểm tra thông tin cá nhân được chuyển và trong trường hợp thông tin không chính xác hoặc không đầy đủ, phải thông báo cho Bên tiếp nhận biết để Bên này chỉnh sửa hoặc hủy tài liệu đó.
5) Bên chuyển tài liệu và Bên tiếp nhận có trách nhiệm đăng ký việc chuyển giao, nhận và huỷ bỏ tài liệu.
6) Bên chuyển tài liệu và Bên tiếp nhận có trách nhiệm bảo vệ tài liệu cá nhân nhận được một cách hữu hiệu để chống lại việc tiết lộ với người không có thẩm quyền, việc sửa chữa tài liệu trái phép, việc đánh mất tài liệu hoặc tài liệu bị hư hỏng hoặc bị hủy hoại hoàn toàn.

Điều 11
VI PHẠM CÁC QUY ĐỊNH AN NINH LIÊN QUAN VIỆC CÙNG BẢO VỆ TIN MẬT

1. Vi phạm các quy định về an ninh là kết quả của hành động hoặc không hành động của một cá nhân trái với Hiệp định này cũng như luật pháp của các Bên. Hành vi này bao gồm cả việc tiết lộ tin mật trái phép.

2. Mọi vi phạm hoặc nghi vi phạm về an ninh liên quan đến tin mật được cung cấp hoặc phát sinh trong quá trình hợp tác phải được thông báo ngay cho người có thẩm quyền của Bên mà việc vi phạm hoặc nghi ngờ vi phạm về an ninh đã xảy ra trên lãnh thổ của Bên này.
3. Mọi vi phạm hoặc nghi ngờ vi phạm an ninh phải được điều tra theo pháp luật của Bên mà vi phạm xảy ra.
4. Trong trường hợp vi phạm an ninh nêu tại Khoản 1, người có thẩm quyền của Bên mà vi phạm xảy ra phải thông báo cho người có thẩm quyền

của Bên kia bằng văn bản về sự việc, bối cảnh và kết quả điều tra nêu tại Khoản 3.

5. Theo yêu cầu, những người có thẩm quyền của các Bên sẽ hợp tác trong các hoạt động nêu tại Khoản 3.

Điều 12
NGÔN NGỮ

Trong quá trình thực hiện các quy định của Hiệp định này, các Bên phải sử dụng ngôn ngữ chính thức của mình, kèm theo bản dịch sang ngôn ngữ chính thức của Bên kia hoặc sang tiếng Anh.

Điều 13
CHI PHÍ

Mỗi Bên sẽ tự chịu chi phí liên quan đến việc thực hiện Hiệp định này.

Điều 14
THAM VẤN

1. Những người có thẩm quyền của các Bên phải thông báo cho nhau những sửa đổi về pháp luật liên quan đến việc bảo vệ tin mật có ảnh hưởng đến các quy định của Hiệp định này.

2. Những người có thẩm quyền của các Bên sẽ tham vấn nhau, theo yêu cầu của một Bên, nhằm đảm bảo hợp tác chặt chẽ trong việc thực hiện các quy định của Hiệp định này.

3. Mỗi Bên cho phép các đại diện của người có thẩm quyền của Bên kia tới thăm nước họ để trao đổi về các thủ tục bảo vệ tin mật đã được Bên kia cung cấp.

4. Để đảm bảo sự hợp tác hiệu quả theo Hiệp định này và trong phạm vi thẩm quyền mà luật pháp của mỗi nước công nhận, cơ quan có thẩm quyền có thể ký kết các thoả thuận chi tiết về tổ chức và kỹ thuật nếu thấy cần thiết.

Điều 15
GIẢI QUYẾT TRANH CHẤP

1. Mọi tranh chấp liên quan đến việc áp dụng Hiệp định này được giải quyết thông qua đàm phán trực tiếp giữa những người có thẩm quyền của các Bên.

2. Nếu không giải quyết được theo cách thức nêu tại Khoản 1, tranh chấp đó sẽ được giải quyết thông qua đường ngoại giao.

Điều 16
ĐIỀU KHOẢN CUỐI CÙNG

1. Hiệp định này sẽ có hiệu lực theo quy định pháp luật của mỗi Bên, được xác nhận bằng việc trao đổi công hàm. Hiệp định sẽ có hiệu lực vào ngày đầu tiên của tháng thứ hai kể từ thời điểm nhận được công hàm sau cùng.

2. Hiệp định này có hiệu lực vô thời hạn. Hiệp định có thể được chấm dứt bởi một trong hai Bên bằng cách gửi văn bản thông báo tới Bên kia. Trong trường hợp đó, Hiệp định này sẽ hết hiệu lực sau sáu tháng kể từ ngày nhận được thông báo trên.

3. Trong trường hợp chấm dứt Hiệp định, mọi tin mật được bảo vệ theo Hiệp định này sẽ tiếp tục được bảo vệ theo quy định của Hiệp định trong thời gian mà cấp độ mật tương ứng đòi hỏi.

4. Hiệp định này có thể được sửa đổi trên cơ sở có sự đồng ý bằng văn bản giữa hai Bên. Những sửa đổi đó sẽ có hiệu lực theo quy định tại Khoản 1 Điều này và là phần không tách rời của Hiệp định này.

Làm tại Hà Nội, ngày 09 tháng 09 năm 2010 thành hai bản gốc, mỗi bản bằng tiếng Ba Lan, tiếng Việt và tiếng Anh, các văn bản đều có giá trị như nhau. Trong trường hợp có sự giải thích khác nhau, văn bản tiếng Anh sẽ được dùng làm cơ sở.

THAY MẶT
CHÍNH PHỦ CỘNG HÒA
BA LAN

THAY MẶT
CHÍNH PHỦ CỘNG HÒA
XÃ HỘI CHỦ NGHĨA
VIỆT NAM

AGREEMENT

between the Government of the Republic of Poland and the Government of the Socialist Republic of Vietnam on mutual protection of classified information

The Government of the Republic of Poland and the Government of the Socialist Republic of Vietnam, hereinafter referred to as the "Parties",

having due regard for guaranteeing mutual protection of all information which has been classified pursuant to the internal laws of one of the Parties and transmitted to the other Party or produced during the cooperation course,

being guided by creation of regulation in the scope of mutual protection of Classified Information, which is to be binding in relation to all mutual cooperation connected with exchange of Classified Information,

assuming that this Agreement shall not prejudice any obligation of each Party in the relation to the treaties or agreements that the Parties adhered to,

have agreed as follows:

ARTICLE 1
DEFINITIONS

For the purpose of this Agreement, the following definitions mean:

1. "Classified Information" – any information irrespective of the form, carrier and manner of recording thereof and objects or any part thereof, which require protection against unauthorized disclosure in accordance with the internal laws of each of the Parties and this Agreement;
2. "Competent Authorities" – authorities referred to in Article 3 of this Agreement;
3. "Authorized Bodies " – individuals, legal entities or other organizational units, competent to transmit, receive, store, protect and use Classified Information in accordance with the internal laws of their Party, including the Competent Authorities;
4. "Classified Contract" - an agreement, performance of which involves access to Classified Information or originating of such information;
5. "Contractor" – an individual, a legal entity or an organizational unit, which has legal capacity to conclude contracts;
6. "Principal" – a body which has legal capacity to let a Classified Contract;
7. "Originating Party" – the Party, an individual and every public or private entity under its jurisdiction, which originates and releases Classified Information to the other Party;
8. "Recipient Party" – the Party, an individual and every public or private entity under its jurisdiction, which receives Classified Information from the other Party;
9. "Third Party" – a state, an individual or every public or private entity under its jurisdiction, as well as every international organization, not being a Party to this Agreement.

ARTICLE 2
SECURITY CLASSIFICATION LEVELS

1. Classified Information is granted a security classification level in accordance to its content, pursuant to the internal laws of the Originating Party. The Recipient Party shall guarantee the equivalent level of protection of the received Classified Information, according to provisions of Paragraph 3.
2. The security classification level shall be changed or removed only by the Authorized Bodies, which has granted it. The Recipient Party shall be notified in writing of every change or removal of the security classification level of previously received Classified Information.
3. The Parties agree that the following security classification levels are equivalent:

REPUBLIC OF POLAND	SOCIALIST REPUBLIC OF VIETNAM	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	TUYỆT MẬT	TOP SECRET
TAJNE	TỐI MẬT	SECRET
POUFNE	MẬT	CONFIDENTIAL

4. Information received from the Republic of Poland classified as ZASTRZEŻONE shall be protected as MẬT in the Socialist Republic of Vietnam.

ARTICLE 3
COMPETENT AUTHORITIES

For the purpose of this Agreement, the Competent Authorities shall be:

1. for the Republic of Poland: the Head of the Internal Security Agency in the civilian sphere and the Head of the Military Counter-Intelligence Service in the military sphere;
2. for the Socialist Republic of Vietnam: The Minister of Public Security in the civilian sphere and the Minister of National Defence in the military sphere.

ARTICLE 4
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. In accordance with this Agreement and the internal laws, the Parties shall adopt appropriate measures aimed at the protection of Classified Information which is transmitted or originated as a result of mutual co-operation of both Parties or the Authorized Bodies, including this originated in connection with performance of Classified Contract.
2. The Recipient Party shall use the Classified Information exclusively for the purposes defined at the transmission thereof.
3. The Recipient Party shall not release the information referred to in Paragraph 1 to Third Parties without a prior written consent of the Originating Party.
4. Access to Classified Information shall be granted only to those persons who have a need-to-know and who have been authorized access to such information after having been cleared to the relevant level as well as briefed in the scope of the protection of Classified Information according to the internal laws of the Recipient Party .

ARTICLE 5
SECURITY CLEARANCES

For the purposes of this Agreement, the Parties shall recognize each other's personnel security assurance and facility security assurance issued in accordance with the internal laws of the Parties.

ARTICLE 6
CLASSIFIED CONTRACTS

1. A Principal can conclude a Classified Contract with a Contractor.
2. In the case referred to in Paragraph 1, the Principal shall apply to its Competent Authority to request the Competent Authority of the other Party to assure a written assurance that the Contractor is the holder of a facility security assurance of the specified security classification level.
3. Issuing of the assurance referred to in Paragraph 2 shall be tantamount to a guarantee of the conduct of actions necessary for establishment that the Contractor fulfils the criteria in the scope of the protection of Classified Information, according to the internal laws of the Party, in whose territory it is located.
4. Classified Information shall not be accessible to the Contractor until the receipt of the assurance referred to in Paragraphs 2 and 3.
5. The Principal shall notify the Contractor a facility security instruction necessary to perform the Classified Contract, which is an integral part of every Classified Contract. This instruction contains provisions on the security requirements, in particular:
    1) the list of types of Classified Information related to a given Classified Contract, taking under consideration their security classification levels;

2) the rules for granting security classification levels to information originated during the performance of a given Classified Contract.

6. A copy of the facility security instruction shall be transmitted to the Competent Authority of the Party, in whose territory the Contractor is located.

7. The performance of the Classified Contract in the part connected with access to Classified Information shall be allowed upon the Contractor's meeting the criteria necessary for the protection of Classified Information, according to the applicable facility security instruction.

8. Every subcontractor shall be obliged to comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

ARTICLE 7
TRANSMISSION OF CLASSIFIED INFORMATION

Classified Information shall be transmitted through diplomatic channels or through other channels ensuring protection against unauthorized disclosure, agreed upon between the Competent Authorities of both Parties in the way referred to in Article 14 Paragraph 4. The Recipient Party shall confirm in writing the receipt of Classified Information.

ARTICLE 8
REPRODUCTION AND TRANSLATION OF CLASSIFIED INFORMATION

1. Information classified as ŚCIŚLE TAJNE/ TUYỆT MẬT shall be reproduced and translated only after prior written permission issued by the Authorized Body.

2. Reproduction and translation of Classified Information shall be pursuant to the internal laws of each of the Parties. Reproduced and translated information shall be placed under the same protection as the originals. Number of copies and translations shall be reduced to that required for official purposes.

ARTICLE 9
DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Information, subject to Paragraph 2, shall be destroyed according to the internal laws of the Recipient Party, in such a manner as to eliminate the partial or total reconstruction.
2. Classified Information marked as ŚCIŚLE TAJNE/ TUYỆT MẬT shall not be destroyed. It shall be returned to the Originating Party.

ARTICLE 10
VISITS

1. Persons arriving on a visit from one Party to the other Party shall be allowed access to Classified Information only after receiving a prior written consent issued by the Competent Authority of the other Party.
2. At least 30 days prior to the planned visit, the Competent Authority of the hosting party shall receive a request for a visit from the Competent Authority of the other Party.
3. Request for a visit, referred to in Paragraph 2 shall include:

   1) purpose, date and program of the visit;

   2) name and surname of the visitor, date and place of birth, nationality, passport number;

   3) position of the visitor together with the name of the institution or facility which he or she represents;

4) confirmation of the level and the date of validity of personnel security assurance held by the visitor;

5) name and address of the organization to be visited;

6) name, surname and position of the person to be visited.

4. In order to protect personal data transmitted in accordance with Paragraph 3 and the internal laws of the Parties, the following provisions shall apply:

1) received personal data shall be used by the hosting party exclusively for the purpose and on conditions defined by the other Party;

2) personal data shall be stored by the hosting party no longer than it is necessary for the purpose of its transmission;

3) in case of personal data transmitted against the internal law of the Party, the transmitting party shall notify the hosting party, which is obliged to remove the data;

4) the transmitting party shall take the responsibility for the correctness of the transmitted personal data and in case the data appears to be untrue or incomplete, it shall inform the h osting party, which is obliged to correct or remove the data;

5) the transmitting party and the hosting party are obliged to register the transmission, receiving and destroying the data;

6) the transmitting party and the hosting party are obliged to protect the received personal data efficiently against its disclosure to unauthorized persons, unauthorized modifications of the data, its loss, damage or total destruction.

ARTICLE 11
BREACH OF SECURITY REGULATIONS CONCERNING MUTUAL PROTECTION OF CLASSIFIED INFORMATION

1. Breach of security occurs as the result of an act or an omission by an individual which is contrary to this Agreement and the internal laws of the Parties. This includes unauthorized disclosure of Classified Information.
2. Every breach of security or a suspicion of breach of security concerning Classified Information of the Originating Party or Classified Information originated as a result of mutual co-operation of the Parties shall be immediately reported to the Competent Authority of the Party in which territory the breach or a suspicion of the breach of security has occurred.
3. Every breach of security or a suspicion of a breach of security shall be investigated pursuant to the internal laws of the Party in whose territory it has occurred.
4. In case of a breach of security, referred to in Paragraph 1, the Competent Authority of the Party in whose territory the breach has occurred shall inform the Competent Authority of the other Party in writing about that fact, the circumstances and the outcome of the actions referred to in Paragraph 3.
5. Upon request, the Competent Authorities of the Parties shall cooperate in the actions referred to in Paragraph 3.

ARTICLE 12
LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use their official languages, attaching the translation into the official language of the other Party or into English.

ARTICLE 13
EXPENSES

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

ARTICLE 14
CONSULTATIONS

1. The Competent Authorities of the Parties shall notify each other of any amendments to the national regulations concerning the protection of Classified Information that affect the provisions of this Agreement.
2. The Competent Authorities of the Parties shall consult each other, upon the request of either of them, in order to ensure close cooperation in the implementation of the provisions of this Agreement.
3. Each Party shall allow the representatives of the Competent Authority of the other Party to come on visits to its own territory to discuss the procedures for protection of Classified Information transmitted by the other Party.
4. In order to ensure the effective cooperation under this Agreement and in the scope of authority acknowledged by their internal laws, the Competent Authorities may, if necessary, conclude written detailed technical or organizational arrangements.

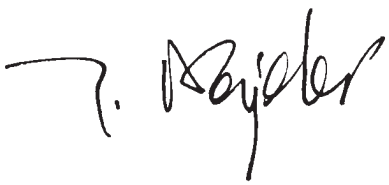
ARTICLE 15
SETTLEMENT OF DISPUTES

1. Any dispute concerning the application of this Agreement shall be settled by direct negotiations between the Competent Authorities of the Parties.
2. If the settlement of a dispute may not be reached in the manner referred to in Paragraph 1, such a dispute shall be settled through diplomatic channels.

ARTICLE 16
FINAL PROVISIONS

1. This Agreement shall enter into force in accordance with the internal laws of each of the Parties, what shall be confirmed by exchange of the notes. The Agreement shall enter into force on the first day of the second month following the receipt of the latter of the notes.
2. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party by giving written notice to the other Party. In such a case, this Agreement shall expire after six months following the receipt of the termination notice.
3. In the event of termination thereof, any Classified Information protected under this Agreement shall continue to be protected pursuant to the provisions of this Agreement, as long as required under the relevant security classification levels.
4. This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1 of this Article and form an integral part of this Agreement.

Done at Hanoi on 09.09.2010 in two original copies, each in the Polish, Vietnamese and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

ON BEHALF OF THE GOVERNMENT OF THE REPUBLIC OF POLAND	ON BEHALF OF THE GOVERNMENT OF THE SOCIALIST REPUBLIC OF VIETNAM
	

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 5 października 2011 r.

Prezydent Rzeczypospolitej Polskiej: *B. Komorowski*

L.S.

Prezes Rady Ministrów: *D. Tusk*