



# DZIENNIK USTAW

## RZECZYPOSPOLITEJ POLSKIEJ

---

Warszawa, dnia 16 lutego 2017 r.

Poz. 275

### UMOWA

**między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Cypryjskiej  
o wzajemnej ochronie informacji niejawnych,**

podpisana w Nikozji dnia 10 września 2015 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 10 września 2015 r. w Nikozji została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Cypryjskiej o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

### UMOWA

**między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Cypryjskiej  
o wzajemnej ochronie informacji niejawnych**

**Rząd Rzeczypospolitej Polskiej oraz Rząd Republiki Cypryjskiej,**

**zwane dalej „Stronami”,**

**mając na uwadze zagwarantowanie wzajemnej ochrony wszystkich informacji,  
którym nadano klauzule tajności zgodnie z prawem krajowym jednej ze Stron  
i przekazano lub przesłano drugiej Stronie, jak również wspólnie wytworzono,**

**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,**

**potwierdzając, iż niniejsza Umowa nie stoi w sprzeczności ze zobowiązaniami**

**Stron wynikającymi z innych umów międzynarodowych,**

**uzgodniły, co następuje:**

## **ARTYKUŁ 1**

### **DEFINICJE**

W rozumieniu niniejszej Umowy następujące definicje oznaczają:

- 1) „informacje niejawne” – wszelkie materiały lub informacje, niezależnie od formy, nośnika i sposobu ich utrwalenia, także podczas procesu ich wytwarzania, które wymagają ochrony przed nieuprawnionym ujawnieniem zgodnie z prawem krajowym każdej ze Stron;
- 2) „kontrakt niejawny” – umowę regulującą wzajemne prawa i obowiązki zawierających ją podmiotów, której realizacja wiąże się z dostępem do informacji niejawnych, bądź z wytworzeniem takich informacji;
- 3) „właściwe organy” – podmioty uprawnione do przekazywania, przesyłania, otrzymywania, przechowywania, ochrony i wykorzystywania informacji niejawnych zgodnie z prawem krajowym swojej Strony, w tym także właściwe organy bezpieczeństwa;
- 4) „właściwe organy bezpieczeństwa” – organy, o których mowa w artykule 3 ustęp 2 niniejszej Umowy;
- 5) „kontrahent” – osobę prawną powołaną zgodnie z prawem krajowym każdej ze Stron realizującą kontrakt niejawny lub ubiegającą się o jego zawarcie;
- 6) „zamawiający” – organ państwowy lub osobę prawną uprawnioną do zawierania kontraktów niejawnych, powołaną zgodnie z prawem krajowym każdej ze Stron;
- 7) „Strona trzecia” – każdą organizację międzynarodową, podmiot lub państwo niebędące Stroną niniejszej Umowy oraz instytucje państwowe, organizacje i obywatele jak również osoby nie posiadające obywatelstwa.

## **ARTYKUŁ 2**

### **KLASYFIKOWANIE INFORMACJI NIEJAWNYCH**

1. Informacjom niejawnym nadaje się klauzulę tajności odpowiednią do ich treści zgodnie z prawem krajowym Strony wytwarzającej. Strona otrzymująca gwarantuje równorzędny poziom ochrony otrzymanym informacjom niejawnym, zgodnie z postanowieniami ustępu 3.
2. Klauzula tajności może zostać zmieniona lub zniesiona wyłącznie przez właściwy organ, który ją nadał. Odbiorca zostaje niezwłocznie poinformowany o każdym przypadku zmiany lub zniesienia klauzuli tajności.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

<b>RZECZPOSPOLITA POLSKA</b>	<b>REPUBLIKA CYPRYJSKA</b>	<b>ODPOWIEDNIK W JĘZYKU ANGIELSKIM</b>
ŚCIŚLE TAJNE	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
TAJNE	ΑΠΟΡΡΗΤΟ	SECRET
POUFNE	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
ZASTRZEŻONE	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

## **ARTYKUŁ 3**

### **WŁAŚCIWE ORGANY BEZPIECZEŃSTWA**

1. Właściwe organy bezpieczeństwa Stron sprawują nadzór nad realizacją niniejszej Umowy.
2. Dla celów niniejszej Umowy właściwymi organami bezpieczeństwa są:
  - 1) w Rzeczypospolitej Polskiej - Szef Agencji Bezpieczeństwa Wewnętrznego;
  - 2) w Republice Cypryjskiej - Krajowa Władza Bezpieczeństwa.

3. W celu zapewnienia skutecznej współpracy będącej przedmiotem niniejszej Umowy, w zakresie kompetencji przyznanych im prawem krajowym, właściwe organy bezpieczeństwa mogą w razie potrzeby i za obopólną zgodą zawierać szczegółowe uzgodnienia techniczne lub organizacyjne.

#### **ARTYKUŁ 4**

#### **ZASADY OCHRONY INFORMACJI NIEJAWNYCH**

1. Zgodnie z niniejszą Umową oraz swoim prawem krajowym, Strony podejmują stosowne działania w celu ochrony informacji niejawnych, które są przekazywane, przesyłane lub zostają wytworzone w wyniku wspólnej działalności Stron lub właściwych organów, w tym także wytworzonych w związku z realizacją kontraktu niejawnego.
2. Otrzymane informacje niejawne mogą być wykorzystane wyłącznie w celach określonych przy ich przekazaniu lub przesłaniu.
3. W celu uzyskania dostępu do informacji niejawnych o klauzuli ΠΟΥΦΝΕ/ ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL lub wyższej niezbędne jest przeprowadzenie postępowania sprawdzającego, zgodnie z prawem krajowym Strony otrzymującej takie informacje.
4. Dostęp do informacji o klauzuli ΖΑΣΤΡΕΖΟΝΕ/ ΠΕΠΙΟΠΙΣΜΕΝΗΣ ΧΡΗΣΗ/ RESTRICTED jest regulowany prawem krajowym Strony otrzymującej takie informacje.
5. Strona nie przekazuje informacji, o których mowa w ustępie 1, żadnej Stronie trzeciej bez uprzedniej pisemnej zgody właściwego organu drugiej Strony, który nadał klauzulę tajności.

## **ARTYKUŁ 5**

### **KONTRAKTY NIEJAWNE**

1. Zamawiający może zawrzeć kontrakt niejawnny z kontrahentem, który posiada siedzibę na terytorium jednej ze Stron.
2. W przypadku, o którym mowa w ustępie 1, zamawiający składa wniosek do właściwego organu bezpieczeństwa swojej Strony o wystąpienie do właściwego organu bezpieczeństwa drugiej Strony z prośbą o wydanie pisemnego zapewnienia, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego odpowiednie do klauzuli informacji, do których będzie miał dostęp.
3. Wydanie zapewnienia, o którym mowa w ustępie 2, gwarantuje, że kontrahent spełnia warunki w zakresie ochrony informacji niejawnnych określone prawem krajowym Strony, na terytorium której posiada siedzibę.
4. Informacje niejawne nie będą udostępniane kontrahentowi do czasu uzyskania zapewnienia, o którym mowa w ustępie 2.
5. Zamawiający przekazuje kontrahentowi instrukcję bezpieczeństwa przemysłowego niezbędną do realizacji kontraktu niejawnego, która stanowi nieodłączną część kontraktu niejawnego. Instrukcja zawiera postanowienia dotyczące wymogów bezpieczeństwa, w szczególności:
  - 1) wykaz informacji niejawnnych odnoszących się do danego kontraktu niejawnego, z uwzględnieniem ich klauzul tajności;
  - 2) zasady nadawania klauzul tajności informacjom wytworzonym podczas realizacji danego kontraktu niejawnego;
  - 3) właściwe organy bezpieczeństwa, o których mowa w artykule 3 ustęp 2 odpowiedzialne za współpracę w zakresie ochrony informacji niejawnnych wytworzonych podczas realizacji danego kontraktu niejawnego;

- 4) obowiązek informowania właściwego organu bezpieczeństwa swojej Strony o każdym przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych lub o podejrzeniu ich naruszenia.
6. Zamawiający przekazuje kopię instrukcji bezpieczeństwa przemysłowego właściwemu organowi bezpieczeństwa swojej Strony, który przesyła ją właściwemu organowi bezpieczeństwa Strony kontrahenta.
7. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych będzie możliwa po spełnieniu przez kontrahenta warunków niezbędnych do ochrony informacji niejawnych, zgodnie z odpowiednią instrukcją bezpieczeństwa.
8. Każdy podwykonawca spełnia te same warunki ochrony informacji niejawnych, jakie zostały nałożone na kontrahenta.

## **ARTYKUŁ 6**

### **PRZEKAZYWANIE I PRZESYŁANIE INFORMACJI NIEJAWNYCH**

1. Informacje niejawne oznaczone klauzulą **POUFNE/ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL** i wyższą są przekazywane drogą dyplomatyczną lub w inny sposób zapewniający ochronę przed nieuprawnionym ujawnieniem, uzgodniony między właściwymi organami bezpieczeństwa Stron, o których mowa w artykule 3 ustęp 2. Odbiorca potwierdza pisemnie odbiór informacji niejawnych.
2. Informacje niejawne są przesyłane, jeśli to konieczne, za pomocą bezpiecznych systemów, uzgodnionych między właściwymi organami bezpieczeństwa Stron, o których mowa w artykule 3 ustęp 2.
3. W Republice Cypryjskiej głównym punktem odbierania i wysyłania informacji niejawnych wymienianych w ramach realizacji niniejszej Umowy jest:

The Central TOP SECRET Registry at the Ministry of Foreign Affairs

Presidential Palace Avenue, 1447, Nicosia

**ARTYKUŁ 7****POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH**

1. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/AKPΩΣ AΠOΠPHTO/ TOP SECRET są powielane i tłumaczone tylko po uprzednim wydaniu pisemnego zezwolenia przez właściwy organ, który przekazał te informacje.
2. Powielanie i tłumaczenie informacji niejawnych odbywa się zgodnie z prawem krajowym 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 8****NISZCZENIE INFORMACJI NIEJAWNYCH**

1. Informacje niejawne, z zastrzeżeniem ustępu 2, są niszczone zgodnie z prawem krajowym Stron w taki sposób, aby uniemożliwić ich częściowe lub całkowite odtworzenie.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/AKPΩΣ AΠOΠPHTO/ TOP SECRET nie są niszczone. Po wykorzystaniu będą one zwracane właściwemu organowi drugiej Strony.

**ARTYKUŁ 9****WIZYTY**

1. Osobom przybywającym z wizytą na terytorium państwa drugiej Strony zezwala się na dostęp w niezbędnym zakresie do informacji niejawnych, a także do obiektów, w których informacje niejawne są wykorzystywane, przetwarzane lub przechowywane, tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ bezpieczeństwa drugiej Strony.

2. Co najmniej 30 dni przed planowaną wizytą właściwy organ bezpieczeństwa Strony przyjmującej wizytę otrzymuje wniosek o wizytę od właściwego organu bezpieczeństwa drugiej Strony.
3. Wniosek o wizytę, o którym mowa w ustępie 2, zawiera:
  - 1) cel, termin i program wizyty;
  - 2) imię i nazwisko osoby przybywającej z wizytą, datę i miejsce urodzenia, obywatelstwo, numer paszportu lub innego dokumentu tożsamości;
  - 3) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą instytucji lub jednostki, którą reprezentuje;
  - 4) klauzulę tajności informacji, do których osoba przybywająca z wizytą będzie miała dostęp;
  - 5) nazwę i adres odwiedzanej jednostki;
  - 6) imię, nazwisko oraz stanowisko służbowe osoby przyjmującej wizytę.
4. W wyjątkowych przypadkach, po uprzednim uzyskaniu zezwolenia wydanego przez właściwy organ bezpieczeństwa Strony przyjmującej wizytę, wniosek o wizytę może zostać przesłany z pominięciem terminu, o którym mowa w ustępie 2.
5. W przypadku kontraktu niejawnego właściwe organy bezpieczeństwa Stron mogą uzgodnić listę osób przyjeżdżających, uprawnionych do wizyt okresowych. Lista jest ważna przez okres nieprzekraczający 12 miesięcy i może być przedłużona o kolejny okres czasu, nieprzekraczający 12 miesięcy. Wnioski o wizyty okresowe są składane zgodnie z przepisami, o których mowa w ustępach 2 i 3. Po zatwierdzeniu listy przez właściwe organy bezpieczeństwa Stron, wizyty mogą być organizowane bezpośrednio przez zainteresowane podmioty.
6. Strony zapewnią ochronę danych osobowych osób przybywających z wizytą, zgodnie ze swoim prawem krajowym.



**ARTYKUŁ 10**  
**NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY**  
**INFORMACJI NIEJAWNYCH**

1. Naruszenie regulacji dotyczących ochrony informacji niejawnych jest wynikiem działania lub zaniechania osoby prawnej lub fizycznej, które jest sprzeczne z niniejszą Umową i prawem krajowym Stron.
2. Wszelkie przypadki naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych Strony wytwarzającej lub informacji niejawnych wytworzonych w wyniku wspólnej działalności Stron są niezwłocznie zgłaszane właściwemu organowi bezpieczeństwa Strony, na terytorium której naruszenie to miało miejsce.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych będzie zbadany zgodnie z prawem krajowym Strony, na terytorium której zdarzenie to miało miejsce.
4. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, o którym mowa w ustępie 1, właściwy organ bezpieczeństwa Strony, na terytorium której naruszenie to miało miejsce pisemnie informuje właściwy organ bezpieczeństwa drugiej Strony o fakcie, okolicznościach i wyniku czynności, o których mowa w ustępie 3.
5. Właściwe organy bezpieczeństwa Stron będą współpracować przy prowadzeniu czynności, o których mowa w ustępie 3, na wniosek jednego z nich.
6. W przypadku gdy naruszenie regulacji dotyczących ochrony informacji niejawnych, o którym mowa w ustępie 1, wystąpiło na terytorium Strony trzeciej, Strona która przekazywała lub przesyłała informacje niejawne we współpracy ze Stroną trzecią podejmie czynności, o których mowa w ustępach 2-5.

## **ARTYKUŁ 11**

### **KOSZTY**

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

## **ARTYKUŁ 12**

### **KONSULTACJE**

1. Właściwe organy bezpieczeństwa Stron informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym w zakresie ochrony informacji niejawnych, które dotyczą postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy bezpieczeństwa Stron konsultują się na wniosek jednego z tych organów.
3. Każda ze Stron zezwoli przedstawicielom właściwego organu bezpieczeństwa drugiej Strony na składanie wizyt na terytorium swojego kraju w celu omówienia procedur dotyczących ochrony informacji niejawnych, które zostały jej przesłane przez drugą Stronę.
4. W celu realizacji postanowień niniejszej Umowy Strony używają języka angielskiego lub swoich języków urzędowych, dołączając tłumaczenie na język urzędowy drugiej Strony lub na język angielski.

## **ARTYKUŁ 13**

### **ROZSTRZYGANIE SPORÓW**

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

3. W trakcie konsultacji Strony wypełniają nadal obowiązki wynikające z postanowień niniejszej Umowy.

#### **ARTYKUŁ 14**

#### **POŚWIADCZENIA BEZPIECZEŃSTWA ORAZ ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO**

1. W celu realizacji postanowień niniejszej Umowy, Strony uznają poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego o klauzuli POUFNE/ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL lub wyższej wydane zgodnie z prawem krajowym drugiej Strony.
2. Właściwe organy bezpieczeństwa Stron przekazują sobie bezzwłocznie wszelkie informacje dotyczące zmian we wzajemnie uznawanych poświadczeniach bezpieczeństwa i świadectwach bezpieczeństwa przemysłowego.
3. Na wniosek, właściwe organy bezpieczeństwa Stron, zgodnie ze swoim prawem krajowym, przekazują sobie informacje niezbędne do przeprowadzenia postępowań sprawdzających dotyczących obywateli, którzy mieszkają lub mieszkali na terytorium każdej ze Stron, lub na potrzeby postępowań bezpieczeństwa przemysłowego prowadzonych wobec kontrahentów Stron.

#### **ARTYKUŁ 15**


#### **POSTANOWIENIA KOŃCOWE**

1. Umowa niniejsza wejdzie w życie zgodnie z prawem krajowym 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

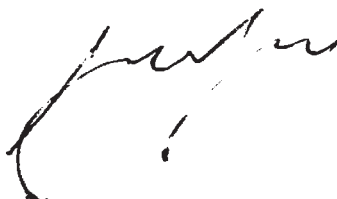
- przypadku utraci moc po upływie sześciu miesięcy od otrzymania noty informującej o wypowiedzeniu.
3. W przypadku wypowiedzenia, wszelkie informacje niejawne przekazane, przesłane lub wytworzone w wyniku wspólnej działalności Stron lub właściwych organów, w tym także wytworzone w związku z realizacją kontraktu niejawnego, będą chronione zgodnie z postanowieniami niniejszej Umowy, dopóki Strona wytwarzająca pisemnie nie zwolni Strony otrzymującej z tego obowiązku.
  4. Umowa niniejsza może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1.

Sporządzono w Nikozji..... dnia 10 WRZEŚNIA 2015..... roku, w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, greckim i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W przypadku rozbieżności przy ich interpretacji, tekst w języku angielskim uważany jest za rozstrzygający.

Z UPOWAŻNIENIA  
RZĄDU RZECZYPOSPOLITEJ  
POLSKIEJ



Z UPOWAŻNIENIA  
RZĄDU REPUBLIKI  
CYPRYJSKIEJ



**ΣΥΜΦΩΝΙΑ**  
**ΜΕΤΑΞΥ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ**  
**ΤΗΣ ΠΟΛΩΝΙΑΣ**  
**ΚΑΙ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ**  
**ΔΗΜΟΚΡΑΤΙΑΣ**  
**ΓΙΑ ΤΗΝ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ**  
**ΠΛΗΡΟΦΟΡΙΩΝ**

Η Κυβέρνηση της Δημοκρατίας της  
Πολωνίας και η κυβέρνηση της κυπριακής Δημοκρατίας, εφεξής καλούμενες  
«τα Μέρη»,

σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία όλων των πληροφοριών  
οι οποίες διαβαθμίστηκαν σύμφωνα με τη εθνική νομοθεσία του ενός εκ των δύο  
Μερών και μεταδόθηκαν ή διαβιβάστηκαν στο άλλο κράτος ή που παράγονται  
από κοινού,

αναγνωρίζοντας την ανάγκη θέσπισης κανόνων σχετικά με την αμοιβαία  
προστασία Διαβαθμισμένων Πληροφοριών, οι οποίοι πρόκειται να είναι  
δεσμευτικοί σε σχέση με κάθε αμοιβαία συνεργασία στον τομέα της ανταλλαγής  
Διαβαθμισμένων Πληροφοριών,

επιβεβαιώνοντας ότι η παρούσα Συμφωνία δεν θα επηρεάσει τις δεσμεύσεις των  
Μερών, οι οποίες απορρέουν από άλλες διεθνείς συμφωνίες,

συμφώνησαν τα ακόλουθα:

## ΑΡΘΡΟ 1 ΟΡΙΣΜΟΙ

Για τους σκοπούς της παρούσας Συμφωνίας:

- 1) «Διαβαθμισμένες Πληροφορίες» σημαίνει κάθε αντικείμενο ή πληροφορία, ανεξαρτήτως της μορφής ή του τρόπου καταγραφής τους, συμπεριλαμβανομένων και αυτών που βρίσκονται στο στάδιο παραγωγής, τα οποία χρήζουν προστασίας από μη εξουσιοδοτημένη κοινολόγηση σύμφωνα με την εθνική νομοθεσία των Μερών.
- 2) «Διαβαθμισμένη Σύμβαση» σημαίνει κάθε συμφωνία η οποία ρυθμίζει εκτελεστά δικαιώματα και υποχρεώσεις μεταξύ των Μερών που υπογράφουν την συμφωνία, η εκτέλεση της οποίας απαιτεί πρόσβαση σε Διαβαθμισμένες Πληροφορίες ή δημιουργία Διαβαθμισμένων Πληροφοριών,
- 3) «Αρμόδιες Αρχές» σημαίνει φορείς οι οποίοι εξουσιοδοτούνται να αποστέλλουν, να διαβιβάζουν, να λαμβάνουν, να αποθηκεύουν, να προστατεύουν και να χρησιμοποιούν Διαβαθμισμένες Πληροφορίες σύμφωνα με την εθνική νομοθεσία των Μερών, συμπεριλαμβανομένων και των Αρμόδιων Αρχών Ασφαλείας.
- 4) «Αρμόδιες Αρχές Ασφαλείας» σημαίνει τις αρχές που αναφέρονται στο Άρθρο 3, Παράγραφος 2, της παρούσας Συμφωνίας.
- 5) «Εργολάβος» σημαίνει τη νομική οντότητα που εγκαθιδρύεται δυνάμει των εθνικών νομοθεσιών των δυο Μερών και στην οποία έχει ανατεθεί μία Διαβαθμισμένη Σύμβαση ή έχει αποταθεί για τη ανάθεση μιας Διαβαθμισμένης Σύμβασης.
- 6) «Εργοδότης» σημαίνει την κρατική αρχή ή τη νομική οντότητα που συστήνεται και έχει τη νομική ικανότητα σύναψης Διαβαθμισμένων Συμβάσεων σύμφωνα με την εθνική νομοθεσία των Μερών.

- 7) «Τρίτο Μέρος» σημαίνει οποιονδήποτε διεθνή οργανισμό, οντότητα ή κράτος το οποίο δεν είναι συμβαλλόμενο μέρος της παρούσας Συμφωνίας, τους κρατικούς του φορείς, και οργανισμούς, τους πολίτες του καθώς και άτομα χωρίς υπηκοότητα

## ΑΡΘΡΟ 2

### ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

1. Στις Διαβαθμισμένες Πληροφορίες παρέχεται ένα επίπεδο διαβάθμισης ασφαλείας σύμφωνα με το περιεχόμενό τους, δυνάμει της εθνικής νομοθεσίας του Μέρους Προέλευσης. Το Μέρος Παραλήπτης διασφαλίζει το ανάλογο επίπεδο προστασίας για τις παραληφθείσες Διαβαθμισμένες Πληροφορίες, σύμφωνα με τις διατάξεις της Παραγράφου 3.
2. Το επίπεδο διαβάθμισης ασφαλείας δύναται να αλλάξει ή να αρθεί μόνο από την Αρμόδια Αρχή η οποία το παρέχει. Το Μέρος παραλήπτης ειδοποιείται αμέσως για κάθε αλλαγή ή διαφοροποίηση του επιπέδου διαβάθμισης ασφαλείας.
3. Τα Μέρη συμφωνούν ότι τα ακόλουθα Επίπεδα Διαβάθμισης Ασφαλείας είναι ισοδύναμα:

ΔΗΜΟΚΡΑΤΙΑ ΤΗΣ ΠΟΛΩΝΙΑΣ	ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ	ΑΝΤΙΣΤΟΙΧΗ ΑΓΓΛΙΚΗ ΟΡΟΛΟΓΙΑ
ŚCISŁE TAJNE	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
TAJNE	ΑΠΟΡΡΗΤΟ	SECRET
POUFNE	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
ZASTRZEŻONE	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

**ΑΡΘΡΟ 3****ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ**

1. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών εποπτεύουν την εφαρμογή της παρούσας Συμφωνίας.
2. Για τους σκοπούς της παρούσας Συμφωνίας, οι Αρμόδιες Αρχές Ασφαλείας θα είναι:
  - 1) Για την Δημοκρατία της Πολωνίας: ο Επικεφαλής της Υπηρεσίας Εσωτερικής Ασφάλειας.
  - 2) Για την Κυπριακή Δημοκρατία: η Εθνική Αρχή Ασφαλείας.
3. Για να διασφαλιστεί η αποτελεσματική συνεργασία υπό την παρούσα Συμφωνία και εντός του πλαισίου της εξουσίας που αναγνωρίζεται από την εθνική νομοθεσία, οι Αρμόδιες Αρχές Ασφαλείας δύνανται, εάν είναι αναγκαίο και κατόπιν αμοιβαίας συνεννόησης, να συνάπτουν γραπτές, λεπτομερείς, τεχνικές ή οργανωτικές διευθετήσεις.

**ΑΡΘΡΟ 4****ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

1. Σύμφωνα με την παρούσα Συμφωνία και την εθνική τους νομοθεσία, τα Μέρη λαμβάνουν όλα τα κατάλληλα μέτρα για την προστασία Διαβαθμισμένων Πληροφοριών οι οποίες μεταδίδονται, διαβιβάζονται ή παράγονται ως αποτέλεσμα της αμοιβαίας συνεργασίας των δύο Μερών ή των Αρμοδίων Αρχών, συμπεριλαμβανομένων και των πληροφοριών που παράγονται σε σχέση με την εκτέλεση Διαβαθμισμένης Σύμβασης.
2. Οι ληφθείσες Διαβαθμισμένες Πληροφορίες θα χρησιμοποιούνται αποκλειστικά για τους σκοπούς που ορίζονται στην μετάδοση και διαβίβαση αυτών.
3. Για να εξασφαλιστεί πρόσβαση σε πληροφορίες με διαβάθμιση ΡΟΥΦΝΕ/ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL και άνω, θα πρέπει να εφαρμοστεί η διαδικασία έκδοσης Εξουσιοδότησης Ασφαλείας Προσωπικού, σύμφωνα με την εθνική νομοθεσία του Μέρους Παραλήπτης.



4. Η πρόσβαση σε πληροφορίες με διαβάθμιση ZASTRZEŻONE/ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/RESTRICTED, ρυθμίζεται από την εθνική νομοθεσία του Μέρους Παραλήπτης.
5. Το Μέρος Παραλήπτης δεν διαβιβάζει τις διαβαθμισμένες πληροφορίες που αναφέρονται στην Παράγραφο 1 σε κανένα Τρίτο Μέρος, χωρίς την εκ των προτέρων γραπτή συγκατάθεση της Αρμόδιας Αρχής του Μέρους Προέλευσης το οποίο καθόρισε το επίπεδο διαβάθμισης ασφαλείας.

## **ΑΡΘΡΟ 5**

### **ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΒΑΣΕΙΣ**

1. Ο Εργοδότης δύναται να συνάπτει Διαβαθμισμένες Συμβάσεις με τον Εργολάβο που βρίσκεται στην επικράτεια του ενός εκ των δύο Μερών.
2. Στην περίπτωση που αναφέρεται στην Παράγραφο 1, ο Εργοδότης υποβάλλει αίτηση στην οικεία Αρμόδια Αρχή Ασφαλείας, ζητώντας όπως η Αρμόδια Αρχή Ασφαλείας του άλλου Μέρους εκδώσει γραπτή εγγύηση ότι ο Εργολάβος είναι κάτοχος έγκυρης Εξουσιοδότησης Ασφαλείας Φορέα κατάλληλης για το επίπεδο διαβάθμισης ασφαλείας των Διαβαθμισμένων Πληροφοριών στις οποίες ο Εργολάβος έχει πρόσβαση.
3. Η έκδοση της εξουσιοδότησης που αναφέρεται στην Παράγραφο 2 αποτελεί εγγύηση ότι ο Εργολάβος πληροί τα κριτήρια που ισχύουν για την προστασία των Διαβαθμισμένων Πληροφοριών, όπως ορίζονται στην εθνική νομοθεσία του Μέρους στην επικράτεια του οποίου είναι εγκατεστημένος ο Εργολάβος.
4. Ο Εργολάβος δεν θα έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες έως ότου ληφθεί η εξουσιοδότηση που αναφέρεται στην Παράγραφο 2.
5. Ο Εργοδότης διαβιβάζει στον Εργολάβο οδηγίες ασφάλειας φορέα, οι οποίες είναι απαραίτητες για την εκτέλεση Διαβαθμισμένων Συμβάσεων και αποτελούν αναπόσπαστο μέρος των Διαβαθμισμένων Συμβάσεων. Οι οδηγίες αυτές περιλαμβάνουν πρόνοιες για τις απαιτήσεις ασφαλείας και πιο συγκεκριμένα:

- 1) τον κατάλογο με τα είδη Διαβαθμισμένων Πληροφοριών που σχετίζονται με μία συγκεκριμένη Διαβαθμισμένη Σύμβαση, συμπεριλαμβανομένων των επιπέδων διαβάθμισης ασφαλείας.
  - 2) τους κανόνες καθορισμού επιπέδων διαβάθμισης ασφαλείας σε πληροφορίες που παράγονται κατά την εκτέλεση συγκεκριμένης Διαβαθμισμένης Σύμβασης.
  - 3) τις Αρμόδιες Αρχές Ασφαλείας, όπως αναφέρονται στο Άρθρο 3, Παράγραφος 2, οι οποίες είναι υπεύθυνες για τη συνεργασία στο πλαίσιο προστασίας Διαβαθμισμένων Πληροφοριών που παράγονται κατά την εκτέλεση συγκεκριμένης Διαβαθμισμένης Σύμβασης.
  - 4) την υποχρέωση ειδοποίησης της οικείας Αρμόδιας Αρχής Ασφαλείας για τυχόν παραβίαση της ασφάλειας ή υποψία παραβίασης της ασφάλειας.
6. Ο Εργοδότης δίδει αντίγραφο των οδηγιών ασφαλείας φορέα στην οικεία Αρμόδια Αρχή Ασφαλείας η οποία θα το διαβιβάσει στην Αρμόδια Αρχή Ασφαλείας του Εργολάβου.
  7. Η εκτέλεση της Διαβαθμισμένης Σύμβασης που αφορά στο τμήμα που σχετίζεται με την πρόσβαση σε Διαβαθμισμένες Πληροφορίες, θα επιτραπεί εφόσον ο Εργολάβος πληροί τα κριτήρια που απαιτούνται για την προστασία των Διαβαθμισμένων Πληροφοριών, σύμφωνα με τις εφαρμοστές οδηγίες ασφαλείας φορέα.
  8. Κάθε υπο-εργολάβος οφείλει να συμμορφώνεται με τους ίδιους όρους που ισχύουν για τον Εργολάβο αναφορικά με την προστασία των Διαβαθμισμένων Πληροφοριών.

## **ΑΡΘΡΟ 6**

### **ΜΕΤΑΔΟΣΗ ΚΑΙ ΔΙΑΒΙΒΑΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

1. Πληροφορίες με διαβάθμιση ΡΟΥΦΝΕ/ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL και άνω, διαβιβάζονται μέσω της διπλωματικής οδού ή με άλλους τρόπους που διασφαλίζουν την προστασία τους από μη εξουσιοδοτημένη κοινολόγηση,

και οι οποίοι συμφωνήθηκαν μεταξύ των Αρμοδίων Αρχών Ασφαλείας και των δύο Μερών όπως αναφέρεται στο Άρθρο 3, Παράγραφος 2. Το Μέρος παραλήπτης επιβεβαιώνει γραπτώς την λήψη Διαβαθμισμένων Πληροφοριών.

2. Οι Διαβαθμισμένες Πληροφορίες θα διαβιβάζονται, εάν είναι αναγκαίο, μέσω προστατευμένων συστημάτων τα οποία θα συμφωνηθούν μεταξύ των Αρμοδίων Αρχών Ασφαλείας των δύο Μερών όπως αναφέρονται στο Άρθρο 3, Παράγραφος 2.
3. Για την Κυπριακή Δημοκρατία το κύριο σημείο εισόδου και εξόδου διαβαθμισμένων Πληροφοριών οι οποίες ανταλλάσσονται βάσει της παρούσας Συμφωνίας είναι:

Η Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ του Υπουργείου Εξωτερικών  
Λεωφόρος Προεδρικού Μεγάρου, 1447 Λευκωσία.

#### **ΑΡΘΡΟ 7**

##### **ΑΝΤΙΓΡΑΦΗ ΚΑΙ ΜΕΤΑΦΡΑΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

1. Πληροφορίες με διαβάθμιση ŚCISLE TAJNE/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TOP SECRET αντιγράφονται και μεταφράζονται μόνο κατόπιν γραπτής άδειας την οποία εκδίδει η Αρμόδια Αρχή που παρέχει την εν λόγω πληροφορία.
2. Η αντιγραφή και μετάφραση Διαβαθμισμένων Πληροφοριών θα διεξάγεται δυνάμει της εθνικής νομοθεσίας του κάθε Μέρους. Οι πληροφορίες που αντιγράφηκαν και μεταφράστηκαν θα προστατεύονται όπως και οι πρωτότυπες πληροφορίες. Ο αριθμός των αντιγράφων και μεταφράσεων περιορίζεται στον αριθμό που απαιτείται για επίσημη χρήση.

#### **ΑΡΘΡΟ 8**

##### **ΚΑΤΑΣΤΡΟΦΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

1. Τηρουμένης της Παραγράφου 2, οι Διαβαθμισμένες Πληροφορίες καταστρέφονται σύμφωνα με την εθνική νομοθεσία του κάθε Μέρους και με τρόπο ώστε να αποφεύγεται η μερική ή ολική ανακατασκευή τους.

2. Οι Πληροφορίες με διαβάθμιση ŚCISŁE TAJNE/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TOP SECRET δεν καταστρέφονται. Μετά την χρήση τους επιστρέφονται στην Αρμόδια Αρχή του άλλου Μέρους Προέλευσης.

## **ΑΡΘΡΟ 9**

### **ΕΠΙΣΚΕΨΕΙΣ**

1. Επιτρέπεται σε άτομα που επισκέπτονται την επικράτεια του άλλου Μέρους η πρόσβαση σε Διαβαθμισμένες Πληροφορίες στο επίπεδο διαβάθμισης ασφαλείας που απαιτείται, καθώς και στις εγκαταστάσεις όπου οι εν λόγω Διαβαθμισμένες Πληροφορίες τηρούνται, τυγχάνουν επεξεργασίας ή αποθηκεύονται, μόνο εάν εξασφαλίσουν την εκ των προτέρων γραπτή συγκατάθεση της Αρμόδιας Αρχής του άλλου Μέρους.
2. Η Αρμόδια Αρχή Ασφαλείας του ενός Μέρους οφείλει να αποστέλλει αίτημα επίσκεψης στην φιλοξενούσα Αρμόδια Αρχή Ασφαλείας, τουλάχιστον 30 ημέρες πριν από την προγραμματισθείσα επίσκεψη.
3. Το αίτημα επίσκεψης, που αναφέρεται στην παράγραφο 2, θα περιλαμβάνει:
  - 1) τον σκοπό, την ημερομηνία και το πρόγραμμα της επίσκεψης,
  - 2) το ονοματεπώνυμο, την ημερομηνία και τον τόπο γέννησης, την εθνικότητα και τον αριθμό διαβατηρίου ή ταυτότητας του επισκέπτη,
  - 3) τη θέση του επισκέπτη καθώς και την ονομασία του οργανισμού ή του φορέα τον οποίο εκπροσωπεί,
  - 4) το επίπεδο διαβάθμισης ασφαλείας των πληροφοριών στις οποίες ο επισκέπτης έχει δικαίωμα πρόσβασης,
  - 5) την ονομασία και την διεύθυνση των εγκαταστάσεων που πρόκειται να δεχθούν την επίσκεψη,
  - 6) το όνομα, το επώνυμο και τη θέση του ατόμου που πρόκειται να δεχθεί την επίσκεψη.
4. Σε εξαιρετικές περιπτώσεις, κατόπιν εξασφάλισης γραπτής άδειας από την Αρμόδια Αρχή Ασφαλείας του φιλοξενούντος Μέρους, το αίτημα επίσκεψης μπορεί να διαβιβαστεί χωρίς να ληφθεί υπόψη η ημερομηνία που αναφέρεται στην Παράγραφο 2.

5. Σε περίπτωση Διαβαθμισμένης Σύμβασης, οι Αρμόδιες Αρχές Ασφαλείας των Μερών δύνανται να καταρτίσουν έναν κατάλογο επισκεπτών οι οποίοι είναι εξουσιοδοτημένοι να πραγματοποιούν επαναλαμβανόμενες επισκέψεις. Ο κατάλογος αυτός θα ισχύει για περίοδο που δεν θα υπερβαίνει τους 12 μήνες και η ισχύς του δύναται να παραταθεί για μέγιστο χρονικό διάστημα 12 μηνών. Τα αιτήματα για επαναλαμβανόμενες επισκέψεις υποβάλλονται σύμφωνα με τις πρόνοιες της Παραγράφου 2 και 3. Μετά την έγκριση του καταλόγου από τις Αρμόδιες Αρχές Ασφαλείας των Μερών, οι επισκέψεις μπορεί να διευθετούνται άμεσα μεταξύ των εμπλεκόμενων Μερών.
6. Τα Μέρη διασφαλίζουν, σύμφωνα με την εθνική τους νομοθεσία, την προστασία των προσωπικών δεδομένων των επισκεπτών.

## **ΑΡΘΡΟ 10**

### **ΠΑΡΑΒΙΑΣΗ ΑΣΦΑΛΕΙΑΣ**

1. Η παραβίαση ασφαλείας είναι το αποτέλεσμα πράξης ή παράληψης από νομικό ή φυσικό πρόσωπο, η οποία αντιβαίνει στην παρούσα Συμφωνία και την εθνική νομοθεσία των Μερών.
2. Κάθε παραβίαση ασφαλείας ή υποψία παραβίασης ασφαλείας αναφορικά με Διαβαθμισμένες Πληροφορίες οι οποίες παράγονται ως αποτέλεσμα της αμοιβαίας συνεργασίας μεταξύ των Μερών, θα αναφέρεται αμέσως στην Αρμόδια Αρχή Ασφαλείας του Μέρους στην επικράτεια του οποίου επήλθε η παραβίαση.
3. Κάθε παραβίαση ασφαλείας ή υποψία παραβίασης ασφαλείας θα διερευνάται σύμφωνα με την εθνική νομοθεσία του Μέρους στην επικράτεια του οποίου επήλθε η παραβίαση.
4. Σε περίπτωση παραβίασης ασφαλείας, η οποία αναφέρεται στην Παράγραφο 1, η Αρμόδια Αρχή Ασφαλείας του Μέρους στην επικράτεια του οποίου επήλθε η παραβίαση, ενημερώνει γραπτώς την Αρμόδια Αρχή Ασφαλείας του άλλου Μέρους, σχετικά με το γεγονός, τις συγκυρίες και το αποτέλεσμα των ενεργειών που αναφέρονται στην Παράγραφο 3.

5. Κατόπιν αιτήματος, οι Αρμόδιες Αρχές Ασφαλείας των Μερών συνεργάζονται για την διεξαγωγή των ενεργειών που αναφέρονται στην Παράγραφο 3.
6. Εάν η παραβίαση ασφαλείας, η οποία αναφέρεται στην Παράγραφο 1, έχει επέλθει στην επικράτεια τρίτου μέρους, το Μέρος που μετέδωσε ή διαβίβασε τις Διαβαθμισμένες Πληροφορίες σε συνεργασία με το εν λόγω τρίτο μέρος, αναλαμβάνουν τις ενέργειες που αναφέρονται στις Παραγράφους 2 – 5.

## **ΑΡΘΡΟ 11**

### **ΕΞΟΔΑ**

Κάθε Μέρος αναλαμβάνει τα δικά του έξοδα τα οποία θα προκύψουν από την εφαρμογή της παρούσας Συμφωνίας.

## **ΑΡΘΡΟ 12**

### **ΔΙΑΒΟΥΛΕΥΣΕΙΣ**

1. Οι Αρμόδιες Αρχές Ασφαλείας ειδοποιούν η μία την άλλη για τυχόν τροποποιήσεις στις εθνικές τους νομοθεσίες αναφορικά με την προστασία Διαβαθμισμένων Πληροφοριών, οι οποίες επηρεάζουν την παρούσα Συμφωνία.
2. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών διαβουλεύονται μεταξύ τους, κατόπιν αιτήματος του ενός εκ των δύο Μερών, για να διασφαλιστεί η στενή συνεργασία στην εφαρμογή των προνοιών της παρούσας Συμφωνίας.
3. Κάθε Μέρος επιτρέπει στους εκπροσώπους της Αρμόδιας Αρχής Ασφαλείας του άλλου Μέρους να επισκέπτονται την επικράτειά του για να συζητήσουν τις διαδικασίες προστασίας των Διαβαθμισμένων Πληροφοριών που διαβιβάζονται από το άλλο Μέρος.
4. Στο πλαίσιο εφαρμογής των προνοιών της παρούσας Συμφωνίας, τα Μέρη χρησιμοποιούν την αγγλική γλώσσα ή τις επίσημες γλώσσες τους, επισυνάπτοντας στην συνέχεια, τη μετάφραση στην επίσημη γλώσσα του άλλου Μέρους ή στην αγγλική γλώσσα.

**ΑΡΘΡΟ 13****ΔΙΕΥΘΕΤΗΣΗ ΔΙΑΦΟΡΩΝ**

1. Τυχόν διαφορές που αφορούν στην εφαρμογή της παρούσας Συμφωνίας διευθετούνται με απευθείας διαβουλεύσεις μεταξύ των Αρμοδίων Αρχών Ασφαλείας των Μερών.
2. Εάν η διευθέτηση κάποιας διαφοράς δεν είναι δυνατόν να επέλθει με τον τρόπο που αναφέρεται στην Παράγραφο 1, η εν λόγω διαφορά θα διευθετείται μέσω της διπλωματικής οδού.
3. Κατά την διάρκεια των διαβουλεύσεων αυτών, τα Μέρη συνεχίζουν να πληρούν τις υποχρεώσεις τους που απορρέουν από τις πρόνοιες της παρούσας Συμφωνίας.

**ΑΡΘΡΟ 14****ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΩΠΙΚΟΥ ΚΑΙ  
ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΑΣΦΑΛΕΙΑΣ ΦΟΡΕΑ**

1. Στο πλαίσιο εφαρμογής των προνοιών της παρούσας Συμφωνίας, τα Μέρη αναγνωρίζουν τις Εξουσιοδοτήσεις Ασφαλείας Προσωπικού και τις Εξουσιοδοτήσεις Ασφαλείας Φορέα επιπέδου ROUFNE/ ΕΜΠΙΣΤΕΥΤΙΚΟ/ CONFIDENTIAL και άνω, τα οποία εκδόθηκαν σύμφωνα με την εθνική νομοθεσία του άλλου Μέρους.
2. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών ειδοποιούν η μία την άλλη χωρίς αδικαιολόγητη καθυστέρηση, για τυχόν αλλαγές αναφορικά με αναγνωρισμένες Εξουσιοδοτήσεις Ασφαλείας Προσωπικού και Εξουσιοδοτήσεις Ασφαλείας Φορέα.
3. Κατόπιν αιτήματος, οι Αρμόδιες Αρχές Ασφαλείας των Μερών παρέχουν η μία στην άλλη, σύμφωνα με την εθνική τους νομοθεσία, πληροφορίες που απαιτούνται για τις ανάγκες των διαδικασιών ελέγχου αναφορικά με πολίτες που ζουν ή ζούσαν στην επικράτεια ενός εκ των δύο Μερών ή των διαδικασιών ελέγχου αναφορικά με Εργολάβους των Μερών.

**ΑΡΘΡΟ 15****ΤΕΛΙΚΕΣ ΠΡΟΝΟΙΕΣ**

1. Η παρούσα Συμφωνία τίθεται σε ισχύ σύμφωνα με την εθνική νομοθεσία του κάθε Μέρους, η οποία δηλώνεται με ανταλλαγή Διπλωματικών Διακοινώσεων. Η παρούσα Συμφωνία τίθεται σε ισχύ την πρώτη ημέρα του δεύτερου μήνα μετά την ημερομηνία λήψης της τελευταίας γραπτής Διπλωματικής Διακοίνωσης.
2. Η παρούσα Συμφωνία συνάπτεται για απεριόριστο χρονικό διάστημα. Δύναται να καταγγελθεί από ένα εκ των δύο Μερών δίνοντας ειδοποίηση στο άλλο Μέρος. Στην προκειμένη περίπτωση, η παρούσα Συμφωνία θα λήξει έξι μήνες μετά την λήψη της ειδοποίησης τερματισμού.
3. Σε περίπτωση καταγγελίας της παρούσας Συμφωνίας, τυχόν Διαβαθμισμένες Πληροφορίες που μεταδόθηκαν, διαβιβάστηκαν ή παράχθηκαν ως αποτέλεσμα της αμοιβαίας συνεργασίας των Μερών ή των Αρμοδίων Αρχών Ασφαλείας, συμπεριλαμβανομένων και αυτών που παράχθηκαν σε σχέση με την εκτέλεση Διαβαθμισμένης Σύμβασης, θα συνεχίσουν να προστατεύονται δυνάμει των προνοιών της παρούσας Συμφωνίας, έως ότου το Μέρος προέλευσης απαλλάξει γραπτώς το Μέρος παραλήπτη από την εν λόγω υποχρέωση.
4. Η παρούσα Συμφωνία δύναται να τροποποιείται βάσει αμοιβαίας γραπτής έγκρισης και των δύο Μερών. Οι εν λόγω τροποποιήσεις τίθενται σε ισχύ σύμφωνα με τις πρόνοιες της Παραγράφου 1.



Συντάχθηκε στη *Λευκωσία*, στις *10.9.15*..... σε δύο πρωτότυπα αντίτυπα, στην πολωνική, ελληνική και αγγλική γλώσσα, και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση διαφωνίας στην ερμηνεία, το αγγλικό κείμενο υπερισχύει.

**ΕΚ ΜΕΡΟΥΣ  
ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ  
ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ  
ΠΟΛΩΝΙΑΣ**



**ΕΚ ΜΕΡΟΥΣ  
ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ  
ΤΗΣ ΚΥΠΡΙΑΚΗΣ  
ΔΗΜΟΚΡΑΤΙΑΣ**



## **AGREEMENT**

**between**

**the Government of the Republic of Poland**

**and**

**the Government of the Republic of Cyprus**

**on the Mutual Protection of Classified Information**

The Government of the Republic of Poland and the Government of the Republic

of Cyprus, hereinafter referred to as the “Parties”,

having due regard for guaranteeing the mutual protection of all information which has been classified pursuant to the national law of one of the Parties and conveyed or transmitted to the other Party, as well as this jointly produced.

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

cooperation connected with exchange of Classified Information,

confirming that this Agreement shall not affect the commitments of the Parties

which stem from other international Agreements,

have agreed as follows:

## **ARTICLE 1**

### **DEFINITIONS**

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

- 1) “Classified Information” – any objects or information, irrespective of the form and manner of recording thereof, also in the process of being originated, which require protection against unauthorized disclosure in accordance with the national law of both Parties;
- 2) “Classified Contract” – an agreement regulating enforceable rights and obligations between the bodies concluding the agreement, performance of which involves access to Classified Information or originating of such information;
- 3) “Competent Authorities” – bodies authorized to convey, transmit, receive, store, protect and use Classified Information in accordance with the national law of their Party, including the Competent Security Authorities;
- 4) “Competent Security Authorities” – authorities referred to in Article 3 Paragraph 2 of this Agreement;
- 5) “Contractor” – a legal entity established under the national law of either of the Parties which has been awarded a Classified Contract or is applying for a Classified Contract;
- 6) “Principal” – a state authority or legal entity entitled to conclude a Classified Contract and established under the national law of either of the Parties;
- 7) “Third Party” – any international organization, entity or States which is not a Party to this Agreement, its state bodies, organisations and its citizens as well as persons without citizenship.

## ARTICLE 2

### THE CATEGORISATION OF CLASSIFIED INFORMATION

1. Classified Information is granted a security classification level in accordance to its content, pursuant to the national law of the originating Party. The recipient Party shall guarantee an equivalent level of protection for the received Classified Information, according to the provisions of Paragraph 3.
2. The security classification level shall be changed or removed only by the Competent Authority, which has granted it. The recipient shall be immediately notified of every change or removal of the security classification level.
3. The Parties agree that the following security classification levels are equivalent:

REPUBLIC OF POLAND	REPUBLIC OF CYPRUS	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
TAJNE	ΑΠΟΡΡΗΤΟ	SECRET
POUFNE	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
ZASTRZEŻONE	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

## ARTICLE 3

### COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities of the Parties shall supervise the implementation of this Agreement.
2. For the purposes of this Agreement, the Competent Security Authorities shall be:
  - 1) for the Republic of Poland: the Head of the Internal Security Agency;

- 2) for the Republic of Cyprus: The National Security Authority.
3. In order to ensure the effective cooperation under this Agreement and in the scope of authority acknowledged by the national law, the Competent Security Authorities may, if necessary and upon mutual consent, conclude written detailed technical or organisational arrangements.

#### **ARTICLE 4**

#### **PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION**

1. In accordance with this Agreement and their national law, the Parties shall adopt appropriate measures aimed at the protection of Classified Information which is conveyed, transmitted or originated as a result of the mutual cooperation of both Parties or the Competent Authorities, including this originated in connection with the performance of a Classified Contract.
2. The received Classified Information shall be used exclusively for the purposes defined at the conveyance and the transmission thereof.
3. In order to obtain access to information classified as POUFNE/ ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL or above, a personnel security clearance procedure needs to be conducted in accordance with the national law of the Party receiving such information.
4. Access to information classified as ZASTRZEŻONE/ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ RESTRICTED is regulated by the national law of the Party receiving such information.
5. The Party shall not release the information referred to in Paragraph 1 to any Third Parties without a prior written consent of the Competent Authority of the other Party, which has granted the security classification level.

## **ARTICLE 5**

### **CLASSIFIED CONTRACTS**

1. The Principal may conclude a Classified Contract with the Contractor located in the territory of one of the Parties.
2. In the case referred to in Paragraph 1, the Principal shall apply to its Competent Security Authority to request the Competent Security Authority of the other Party to issue a written assurance that the Contractor is a holder of a valid Facility Security Clearance appropriate for the security classification level of the Classified Information the Contractor is authorized to have access to.
3. Issuing of the assurance referred to in Paragraph 2 shall be a guarantee that the Contractor meets the criteria applicable to the protection of Classified Information, as specified in the national law of the Party, in the territory of which the Contractor is located.
4. Classified Information shall not be accessible to the Contractor until the receipt of the assurance referred to in Paragraph 2.
5. The Principal shall transmit to the Contractor a facility security instruction necessary to perform a Classified Contract, which is an integral part of the 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, including their security classification levels;
  - 2) the rules for granting security classification levels to information originated during the performance of a given Classified Contract;
  - 3) the Competent Security Authorities, as referred to Article 3 Paragraph 2, which are responsible for cooperation in the scope of the protection of Classified Information originated during the performance of a given Classified Contract;

- 4) the obligation to notify its Competent Authority of any breach of security or any suspicion of breach of security.
6. The Principal shall put forward a copy of the facility security instruction to its Competent Security Authority, which shall transmit it to the Competent Security Authority of the Contractor.
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. Any subcontractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

**ARTICLE 6**  
**CONVEYANCE AND TRANSMISSION OF CLASSIFIED**  
**INFORMATION**

1. Information classified as **POUFNE/ EMIISTEYTIKO/ CONFIDENTIAL** and above shall be conveyed through diplomatic channels or through other channels ensuring protection against unauthorised disclosure, agreed upon between the Competent Security Authorities of both Parties as referred to in Article 3 Paragraph 2. The recipient shall confirm in writing the receipt of Classified Information.
2. Classified Information shall be transmitted, if necessary, via protected systems agreed upon between the Competent Security Authorities of the Parties as referred to in Article 3 Paragraph 2.
3. For the Republic of Cyprus the main point of entry and exit for the Classified Information exchanged under this Agreement shall be:

The Central TOP SECRET Registry at the Ministry of Foreign Affairs  
Presidential Palace Avenue. 1447, Nicosia

**ARTICLE 7****COPYING AND TRANSLATING OF CLASSIFIED INFORMATION**

1. Information classified as **ŚCIŚLE TAJNE/AKPΩΣ ΑΠΟΠΗΤΟ/TOP SECRET** shall be copied and translated only after a prior written permission issued by the Competent Authority which provided this information.
2. Copying and translating of Classified Information shall be conducted pursuant to the national law of each of the Parties. Copied and translated information shall be placed under the same protection as the original information. The number of copies and translations shall be reduced to that required for official purposes.

**ARTICLE 8****DESTRUCTION OF CLASSIFIED INFORMATION**

1. Subject to Paragraph 2, Classified Information shall be destroyed according to the national law of the Parties, in such a manner as to eliminate its partial or total reconstruction of the same.
2. Information classified as **ŚCIŚLE TAJNE/AKPΩΣ ΑΠΟΠΗΤΟ/TOP SECRET** shall not be destroyed. After being used, the Classified Information shall be returned to the Competent Authorities of the other Party.

**ARTICLE 9****VISITS**

1. Persons arriving on a visit in the territory of the other Party shall be allowed access to Classified Information to the necessary extent, as well as to the premises in which such Classified Information is handled,



- processed or stored, only after receiving a prior written consent issued by the Competent Security Authority of the other Party.
2. At least 30 days prior to the planned visit, the Competent Security Authority of the hosting Party shall receive a request for a visit from the Competent Security Authority of the other Party.
  3. Request for a visit, referred to in Paragraph 2, shall include:
    - 1) purpose, date and the program of the visit;
    - 2) name and surname of the visitor, date and place of birth, nationality, passport number or other identity card number;
    - 3) position of the visitor together with the name of the institution or facility which he or she represents;
    - 4) security classification of information a person arriving on a visit is authorized to have access to;
    - 5) name and address of the facility to be visited;
    - 6) name, surname and position of the person to be visited.
  4. In exceptional cases, after receiving a prior written permission issued by the Competent Security Authority of the hosting Party, request for a visit may be transmitted with the omission of the date referred to in Paragraph 2.
  5. In case of a Classified Contract, the Competent Security Authorities of the Parties may agree on a list of visitors entitled to recurring visits. The list shall be valid for a period not exceeding 12 months and may be extended for a further period of time, not exceeding 12 months. Requests for recurring visits shall be submitted in accordance with the provisions of Paragraphs 2 and 3. Once a list has been approved by the Competent Security Authorities of the Parties, visits may be arranged directly between the entities involved.
  6. The Parties shall ensure, pursuant to their national law, the protection of the personal data of the persons arriving on a visit.

## **ARTICLE 10**

### **BREACH OF SECURITY**

1. A breach of security is the result of an act or an omission by a legal entity or a natural person which is contrary to this Agreement and the national law of the Parties.
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 the mutual cooperation between the Parties shall be immediately reported to the Competent Security Authority of the Party in the territory of which the breach has occurred.
3. Every breach of security or a suspicion of breach of security shall be investigated pursuant to the national law of the Party in the territory of which it has occurred.
4. In case of a breach of security, referred to in Paragraph 1, the Competent Security Authority of the Party in the territory of which the breach has occurred shall notify the Competent Security Authority of the other Party in writing about the fact, the circumstances and the outcome of the actions referred to in Paragraph 3.
5. Upon request, the Competent Security Authorities of the Parties shall cooperate in the actions referred to in Paragraph 3.
6. If breach of security referred to in Paragraph 1 has occurred in the territory of a Third Party, the Party which conveyed and transmitted the Classified Information in cooperation with the Third Party in question shall take the actions referred to in Paragraphs 2 – 5.

## **ARTICLE 11**

### **EXPENSES**

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

## **ARTICLE 12**

### **CONSULTATIONS**

1. The Competent Security Authorities of the Parties shall notify each other of any amendments to their national law concerning the protection of Classified Information that affect the provisions of this Agreement.
2. The Competent Security Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions hereof.
3. Each Party shall allow the representatives of the Competent Security Authority of the other Party to come on visits to its own territory to discuss the procedures for the protection of Classified Information transmitted by the other Party.
4. In the scope of the implementation of the provisions of this Agreement, the Parties shall use the English language or their official languages, attaching then, the translation into the official language of the other Party or into English.

## **ARTICLE 13**

### **SETTLEMENT OF DISPUTES**

1. Any disputes concerning the application of this Agreement shall be settled by direct consultations between the Competent Security Authorities of the Parties.
2. If the settlement of a dispute cannot be reached in the manner referred to in Paragraph 1, such a dispute shall be settled through diplomatic channels.
3. During these consultations, the Parties shall continue to fulfill their obligations stemming from the provisions of this Agreement.

**ARTICLE 14**  
**PERSONNEL SECURITY CLEARANCES AND FACILITY**  
**SECURITY CLEARANCES**

1. In the scope of implementation of this Agreement, the Parties shall recognize Personnel Security Clearances and Facility Security Clearances at the level of POUFNE/ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIAL or above issued in accordance with the national law of the other Party.
2. The Competent Security Authorities of the Parties shall notify each other without undue delay any changes concerning mutually recognized Personnel Security Clearances and Facility Security Clearances.
3. Upon request, the Competent Security Authorities of the Parties shall, in accordance with their national law, provide each other with information required for the needs of vetting procedures concerning citizens who live or lived in the territory of either Party or vetting procedures concerning Contractors of the Parties.

**ARTICLE 15**  
**FINAL PROVISIONS**

1. This Agreement shall enter into force in accordance with the national law of each of the Parties, which shall be stated by way of exchange of 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 upon giving notice to the other Party. In such case, this Agreement shall expire six months following the receipt of the termination notice.
3. In the event of termination of the Agreement, any Classified Information conveyed, transmitted or originated as a result of the mutual cooperation of the Parties or the Competent Authorities, including those originated in

connection with performance of a Classified Contract, shall continue to be protected pursuant to the provisions of this Agreement as long as the originating Party dispenses the Party receiving classified information from this obligation in writing.

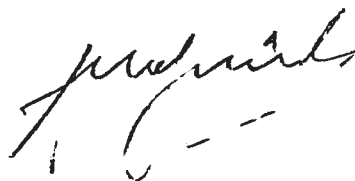
4. This Agreement may be amended upon the basis of a mutual written consent by both Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1.

Done at.....*NICOSIA*.....on...*10 SEPTEMBER 2015*...in two original copies, each in the Polish, Greek and English languages, all texts being equally authentic. In case of divergences in the interpretation, the English text shall prevail.

ON BEHALF OF  
THE GOVERNMENT OF  
THE REPUBLIC OF POLAND



ON BEHALF OF  
THE GOVERNMENT OF  
THE REPUBLIC OF CYPRUS



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 27 czerwca 2016 r.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *B. Szydło*