Ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Σλοβακίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2012 εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος.

Αριθμός 17(ΙΙΙ) του 2012

ΝΟΜΟΣ ΠΟΥ ΚΥΡΩΝΕΙ ΤΗ ΣΥΜΦΩΝΙΑ ΜΕΤΑΞΥ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΚΑΙ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΣΛΟΒΑΚΙΑΣ ΓΙΑ ΤΗΝ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η Βουλή των Αντιπροσώπων ψηφίζει ως ακολούθως:

Συνοπτικός τίτλος.

1. Ο παρών Νόμος θα αναφέρεται ως ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Σλοβακίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2012.

Ερμηνεία.

2. Στον παρόντα Νόμο, εκτός εάν από το κείμενο προκύπτει διαφορετική έννοια -

«Συμφωνία» σημαίνει τη Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Σλοβακίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών, η διαπραγμάτευση της οποίας έγινε κατόπιν της Απόφασης του Υπουργικού Συμβουλίου με αριθμό 2/2009 και ημερομηνία 20.5.2009 και η οποία υπογράφηκε στις 11.11.2010, κατόπιν της Απόφασης του Υπουργικού Συμβουλίου με αριθμό 6/2010 και ημερομηνία 27.9.2010.

Κύρωση της Συμφωνίας. Πίνακας. Μέρος Ι Μέρος ΙΙ Μέρος ΙΙΙ.

3. Με τον παρόντα Νόμο κυρώνεται η Συμφωνία, το κείμενο της οποίας εκτίθεται στην αγγλική γλώσσα στο Μέρος Ι του Πίνακα, στην ελληνική γλώσσα στο Μέρος ΙΙ του Πίνακα και στη σλοβακική γλώσσα στο Μέρος ΙΙΙ του Πίνακα:

Νοείται ότι, σε περίπτωση διαφοράς μεταξύ του κειμένου που εκτίθεται στο Μέρος ΙΙ και του κειμένου που εκτίθεται στο Μέρος ΙΙΙ του Πίνακα, υπερισχύει το κείμενο που εκτίθεται στο Μέρος Ι του Πίνακα.

Αρμόδια αρχή.

4. Ως αρμόδια αρχή για την εφαρμογή της Συμφωνίας, ορίζεται ο Υπουργός Άμυνας.

ΠΙΝΑΚΑΣ

(Άρθρο 3)

Μέρος Ι

Agreement
between
the Government of the Republic of Cyprus
and
the Government of the Slovak Republic
on Mutual Protection of Classified Information

The Government of the Republic of Cyprus
and
the Government of the Slovak Republic

(hereinafter referred to as "the Parties"),

Recognizing the need to set rules on protection of Classified Information mutually exchanged within the scope of political, military, economical, legal, scientific and technological or any other cooperation, as well as classified information arisen in the process of such cooperation,

Intending to ensure the mutual protection of all Classified Information, which has been classified in the state of the one Party and transferred to the state of the other Party,.

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

Considering the mutual interests in the protection of Classified Information, in accordance with the legislation of the states of the both Parties,

Have agreed as follows:

Article 1
Objective

The objective of this Agreement is to ensure the protection of classified information that is commonly generated or exchanged between the states of the Parties.

Article 2
Definitions

For the purposes of this Agreement:

a) "**Classified Contract**" means an agreement between two or more Contractors, which contains or involves Classified Information;

b) "**Classified Information**" means any information or material, irrespective of its form or nature, which requires protection against unauthorized manipulation and has been classified in accordance with the national legislation of the states of the Parties;

c) "**Competent Security Authority**" means the national security body responsible for the implementation and supervision of this Agreement;

d) "**Contractor**" means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;

e) "**Facility Security Clearance**" means the determination by the Competent Security Authority confirming, that the legal entity has the physical and organizational capability to use and store Classified Information in accordance with the respective national legislation;

f) "**Need-to-know**" means the necessity to have access to Classified Information in the scope of a given official position and for the performance of a specific task;

g) "**Originating Party**" means the state of the Party which transmits Classified Information to the state of the other Party;

h) "**Personnel Security Clearance**" means the determination by the Competent Security Authority confirming, in accordance with the respective national legislation, that the individual is eligible to have access to Classified Information;

i) "**Receiving Party**" means the state of the Party which Classified Information is transmitted to by the state of the other Party;

j) "**Third Party**" means any state, organization, legal entity or individual, which is not a party to this Agreement.

Article 3
Security Classification Levels

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national legislation of their respective states:

For the Republic of Cyprus	For the Slovak Republic	Equivalent English
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	PRÍSNE TAJNÉ	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNÉ	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	DÔVERNÉ	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	VYHRADENÉ	RESTRICTED

Article 4
Competent Security Authorities

1. The Competent Security Authorities of the Parties are:

For the Republic of Cyprus:
National Security Authority
4 Emmanuel Roidis str.
1432 Nicosia
Republic of Cyprus

For the Slovak Republic:
National Security Authority
Budatínska 30
850 07 Bratislava
Slovak Republic

2. The states of the Parties shall inform each other through diplomatic channels of any modification of contact data of the Competent Security Authorities.

3. On request, the Competent Security Authorities shall inform each other of respective national legislation on Classified Information and shall exchange information about the security standards, procedures and practices for the protection of Classified Information.

Article 5
Protection Measures and Access to Classified Information

1. In accordance with their national legislation, the states of the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. The same level of protection shall be assigned to such Classified Information as is provided for the national Classified Information of the equivalent security classification level in accordance with the Article 3.

2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information.

3. Access to Classified Information shall be limited to persons on a Need-to-know basis who are authorized in accordance with the national legislation to have access to Classified Information of the equivalent security classification level.

4. Within the scope of this Agreement, state of each Party shall recognize the Personnel and Facility Security Clearances granted in accordance with the national legislation of the state of the other Party. The security clearances shall be equivalent in accordance with Article 3.

5. The Competent Security Authorities shall, in accordance with the national legislation, assist each other upon request at carrying out vetting procedures necessary for the application of this Agreement.

6. Within the scope of this Agreement, the Competent Security Authorities shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about their withdrawal or downgrading.

7. The Receiving Party shall:

   a) submit Classified Information to any Third Party only upon prior written consent of the Originating Party;

   b) mark the received Classified Information in accordance with the Article 3;

   c) use Classified Information solely for the purposes it has been provided for.

Article 6
Transmission of Classified Information

1. Classified Information shall be transmitted through diplomatic channels unless otherwise approved on by the Competent Security Authorities. The Receiving Party shall confirm the receipt of Classified Information in writing.

2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means approved on by the Competent Security Authorities.

Article 7
Reproduction and Translation of Classified Information

1. Translations and reproductions of Classified Information shall be made in accordance with the national legislation of the Receiving Party and the following procedures:

   a) the individuals shall be granted the appropriate Personnel Security Clearance in accordance with their national legislation;

   b) the translations and the reproductions shall be marked and protected as the original Classified Information;

   c) the translations and the number of copies shall be limited to that required for official purposes;

   d) the translations shall bear an appropriate note in the language of the translation indicating that it contains Classified Information received from the Originating Party.

2. Classified Information marked SECRET or above shall be translated or reproduced only upon prior written consent of the Originating Party.

Article 8
Destruction of Classified Information

1. Classified Information shall be destroyed so as to prevent its partial or total reconstruction.

2. Classified Information marked up to SECRET shall be destroyed in accordance with the national legislation.

3. Classified Information marked TOP SECRET shall not be destroyed. It shall be returned to Competent Security Authority of the Originating Party.

4. A report on destruction of Classified Information shall be made and its translation in English shall be delivered to the Competent Security Authority of the Originating Party.

Article 9
Classified Contracts

1. State of one Party, wishing to place a Classified Contract with a Contractor of the state of the other Party, or wishing to authorize one of its own Contractors to place a Classified Contract in the territory of the state of the other Party within a classified project shall obtain, through its Competent Security Authority, prior written assurance from the Competent Security Authority of the state of the other Party that the proposed Contractor is granted Facility Security Clearance of the appropriate security classification level.

2. Each Classified Contract concluded in accordance with this Agreement shall include:

   a) commitment of the Contractor to ensure that its premises have necessary conditions for handling and storing Classified Information of appropriate security classification level;

   b) commitment of the Contractor to ensure that persons who perform duties requiring access to Classified Information are granted the appropriate level of Personnel Security Clearance;

   c) commitment of the Contractor to ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national legislation;

   d) commitment of the Contractor to perform periodical security inspections of its premises;

   e) list of Classified Information and list of areas in which Classified Information can arise;

   f) procedure for communication of changes in the security classification level of Classified Information;

   g) communication means and electronic means for transmission;

   h) procedure for the transportation of Classified Information;

   i) appropriate authorized individuals or legal entities responsible for the co-ordination of the safeguarding of Classified Information related to the Classified Contract;

   j) commitment of the Contractor to notify of any actual or suspected loss, leak or compromise of the Classified Information;

   k) commitment of the Contractor to forward a copy of the Classified Contract to its own Competent Security Authority;

   l) commitment of the subcontractor to fulfill the same security obligations as the Contractor.

3. As soon as pre-contractual negotiations begin between a potential Contractor in the territory of one state of the Parties and another possible Contractor located in the state of the other Party's territory, aiming at the signing of Classified Contracts, the Competent Security Authority shall inform the state of the other Party of the security classification level given to the Classified Information related to those pre-contractual negotiations.

4. Copy of each Classified Contract shall be forwarded to the Competent Security Authority of the state of the Party where the work is to be performed, to allow adequate security supervision and control.

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

Article 10
Visits

1. Visits involving access to Classified Information by nationals from the state of one Party to the state of the other Party are subject to prior written approval given by the Competent Security Authority of the host state.
2. Visits involving access to Classified Information shall be allowed by the state of one Party to visitors from the state of the other Party only if they have been granted the appropriate Personnel Security Clearance and authorized to receive or to have access to Classified Information in accordance with their national legislation.
3. Visits involving access to Classified Information by nationals from a third state shall only be authorized by a common agreement between the states of the Parties.
4. The Competent Security Authority of the host state shall receive a request for visit from the other Competent Security Authority at least thirty days in advance.
5. In urgent cases, the request for visit shall be transmitted at least seven days before.
6. The request for visit shall include:
   a) visitor's name and surname, place and date of birth, nationality, passport or identification document number;
   b) name of the legal entity represented by the visitor;
   c) name and address of the legal entity to be visited;
   d) confirmation of the visitor's Personnel Security Clearance and its validity;
   e) object and purpose of the visit;
   f) expected date and duration of the requested visit. In case of recurring visits the total period covered by the visits shall be stated;
   g) the date, signature and stamping of the official seal of the Competent Security Authority.

7. Once the visit has been approved the Competent Security Authority of the host state shall provide a copy of the request for visit to the security officers of the legal entity to be visited.

8. The validity of visit approval shall not exceed one year.

9. The states of the Parties may draw up lists of individuals authorized to make recurring visits. The lists are valid for an initial period of twelve months. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.

Article 11
Breach of Security

1. In case of breach of security in accordance with the national legislation that results in an actual or suspected compromise of Classified Information originated by or received from the state of the other Party, the Competent Security Authority of the state of the Party where the breach or compromise has arisen shall inform the Competent Security Authority of the state of the other Party, as soon as possible, and initiate the appropriate investigation.

2. If a breach of security arises in a state other than states of the Parties, the Competent Security Authority of the dispatching state shall take the actions prescribed in Paragraph 1.

3. The state of the other Party shall, upon request, co-operate in the investigation in accordance with Paragraph 1.

4. The state of the other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damage.

Article 12
Expenses

Each Party shall bear its own expenses incurred in the course of application and supervision of this Agreement.

Article 13
Settlement of Disputes

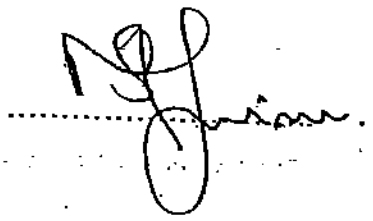
Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiations between the Competent Security Authorities.

Article 14
Final Provisions

1. This Agreement is concluded for an indefinite period of time and enters into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.
2. This Agreement may be amended any time on the basis of mutual written approval of the Parties.
3. Each Party may, at any time, terminate this Agreement by written notification to the other Party, through diplomatic channels. In this case, the termination takes effect six months after the date of the receipt of the respective notification.
4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Originating Party dispenses the Receiving Party from this obligation.

Done at Bratislava, on 11 November 2010, in two original sets, each in the Greek, Slovak and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

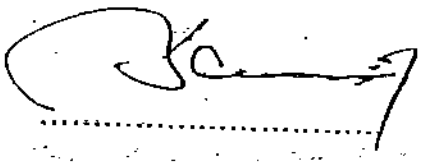
For the Government of the Republic of Cyprus



Markos Kyprianou

Minister of Foreign Affairs

For the Government of the Slovak Republic



František Blanárik

Director of National Security Agency

Μέρος ΙΙ

Συμφωνία
μεταξύ
της Κυβέρνησης της Κυπριακής Δημοκρατίας
και
της Κυβέρνησης της Δημοκρατίας της Σλοβακίας,
για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών

Η Κυβέρνησης της Κυπριακής Δημοκρατίας
και
η Κυβέρνησης της Δημοκρατίας της Σλοβακίας

(εφεξής καλούμενες τα «Μέρη»),

Αναγνωρίζοντας την ανάγκη για τον καθορισμό κανόνων σχετικά με την προστασία διαβαθμισμένων πληροφοριών, οι οποίες ανταλλάσσονται στα πλαίσια πολιτικής, στρατιωτικής, οικονομικής, νομικής, επιστημονικής και τεχνολογικής ή άλλης συνεργασίας, καθώς και διαβαθμισμένων πληροφοριών που προκύπτουν από την εν λόγω συνεργασίας,

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία όλων των Διαβαθμισμένων Πληροφοριών, οι οποίες διαβαθμίστηκαν στο ένα κράτος και διαβιβάστηκαν στο άλλο κράτος,

Επιθυμώντας να θεσπίσουν κανόνες για την αμοιβαία προστασία των Διαβαθμισμένων Πληροφοριών που ανταλλάσσουν τα Μέρη μεταξύ τους,

Λαμβάνοντας υπόψη το αμοιβαίο συμφέρον της προστασίας των Διαβαθμισμένων Πληροφοριών, σύμφωνα με τη νομοθεσία των δύο κρατών,

Συμφώνησαν τα ακόλουθα:

Άρθρο 1
Σκοπός

Σκοπός της παρούσας Συμφωνίας είναι η διασφάλιση της αμοιβαίας προστασίας διαβαθμισμένων πληροφοριών οι οποίες παράγονται από κοινού ή ανταλλάσσονται μεταξύ των δύο κρατών.

Άρθρο 2
Ορισμοί

Για τους σκοπούς της παρούσας Συμφωνίας:

α) «**Διαβαθμισμένη Σύμβαση**» σημαίνει κάθε συμφωνία μεταξύ δύο ή περισσοτέρων εργολάβων, η οποία περιέχει διαβαθμισμένες πληροφορίες.

β) «**Διαβαθμισμένες Πληροφορίες**» σημαίνει κάθε πληροφορία ή υλικό, ανεξαρτήτου τύπου ή φύσεως, που χρήζει προστασίας από μη εξουσιοδοτημένο χειρισμό και διαβαθμίστηκε σύμφωνα με την εθνική νομοθεσία των δύο συμβαλλομένων κρατών.

γ) «**Αρμόδια Αρχή Ασφαλείας**» σημαίνει τον φορέα εθνικής ασφαλείας που είναι υπεύθυνος για την εφαρμογή και εποπτεία της παρούσας Συμφωνίας.

δ) «**Εργολάβος**» σημαίνει το φυσικό ή νομικό πρόσωπο που έχει τη νομική ικανότητα ανάληψης Διαβαθμισμένων Συμβάσεων.

ε) «**Έλεγχος Ασφάλειας Φορέα**» σημαίνει την πιστοποίηση της Αρμόδιας Αρχής Ασφαλείας ότι το νομικό πρόσωπο έχει την ικανότητα να χρησιμοποιεί και να αποθηκεύει Διαβαθμισμένες Πληροφορίες σύμφωνα με την αντίστοιχη εθνική νομοθεσία.

στ) «**Ανάγκη για γνώση**» σημαίνει την ανάγκη πρόσβασης σε Διαβαθμισμένες Πληροφορίες στα πλαίσια συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας.

ζ) «**Μέρος αποστολέας**» σημαίνει το Μέρος το οποίο διαβιβάζει Διαβαθμισμένες Πληροφορίες στο άλλο Μέρος.

η) «**Έλεγχος Ασφαλείας Προσωπικού**» σημαίνει την πιστοποίηση της Αρμόδιας Αρχής Ασφαλείας, σύμφωνα με την αντίστοιχη εθνική νομοθεσία, ότι το φυσικό πρόσωπο δικαιούται να έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες.

θ) «**Μέρος παραλήπτης**» σημαίνει το Μέρος στο οποίο διαβιβάζονται Διαβαθμισμένες Πληροφορίες από το άλλο Μέρος.

ι) «**Τρίτο Μέρος**» σημαίνει το κράτος, τον οργανισμό, το νομικό ή φυσικό πρόσωπο το οποίο δεν είναι συμβαλλόμενο μέρος στην παρούσα Συμφωνία.

Άρθρο 3
Επίπεδα Ασφαλείας

Τα Μέρη συμφωνούν ότι τα ακόλουθα Επίπεδα Ασφαλείας είναι ισοδύναμα και αντιστοιχούν στα επίπεδα ασφαλείας τα οποία ορίζονται από την εθνική νομοθεσία των κρατών τους:

ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	PRÍSNE TAJNÉ	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNÉ	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	DÔVERNÉ	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	VYHRADENÉ	RESTRICTED

Άρθρο 4
Αρμόδια Αρχή Ασφαλείας

1. Η Αρμόδιες Αρχές Ασφαλείας των Μερών είναι:

Για την Κυπριακή Δημοκρατία
Εθνική Αρχή Ασφαλείας
Εμμανουήλ Ροΐδη 4
1432 Λευκωσία
Κυπριακή Δημοκρατία

Για την Δημοκρατία της Σλοβακίας
National Security Authority
Budatinska 30
850 07 Bratislava
Slovak Republic

2. Τα κράτη των Μερών θα αλληλοενημερώνονται μέσω της διπλωματικής οδού για τυχόν αλλαγές στα στοιχεία επικοινωνίας των Αρμόδιων Αρχών Ασφαλείας.

3. Κατόπιν αιτήματος, οι Αρμόδιες Αρχές Ασφαλείας θα αλληλοενημερώνονται για την αντίστοιχη εθνική νομοθεσία περί Διαβαθμισμένων Πληροφοριών και θα ανταλλάσσουν πληροφορίες σχετικά με τα πρότυπα, τις διαδικασίες και πρακτικές ασφαλείας για την προστασία Διαβαθμισμένων Πληροφοριών.

Άρθρο 5
Μέτρα Προστασίας και Πρόσβαση σε Διαβαθμισμένες Πληροφορίες

1. Σύμφωνα με την εθνική τους νομοθεσία, τα κράτη των Μερών λαμβάνουν όλα τα απαραίτητα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών οι οποίες ανταλλάσσονται ή παράγονται βάσει της παρούσας Συμφωνίας. Το ίδιο επίπεδο προστασίας θα καθορίζεται στις Διαβαθμισμένες Πληροφορίες, όπως προβλέπεται για τις εθνικές Διαβαθμισμένες Πληροφορίες του αντίστοιχου επιπέδου ασφαλείας σύμφωνα με το Άρθρο 3.

2. Το Μέρος Αποστολέας ενημερώνει γραπτός το Μέρος Παραλήπτη για τυχόν αλλαγή των βαθμών ασφαλείας της διαβιβασθέντων Διαβαθμισμένων Πληροφοριών.

3. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται σε πρόσωπα βάσει της αρχής της ανάγκης για γνώση, τα οποία είναι εξουσιοδοτημένα σύμφωνα με την εθνική νομοθεσία να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες του αντίστοιχου επιπέδου ασφαλείας.

4. Στα πλαίσια της παρούσας Συμφωνίας, το κράτος του κάθε Μέρους αναγνωρίζει την πιστοποίηση του Έλεγχου Ασφαλείας Προσωπικού και Φορέα, που παρέχεται σύμφωνα με την εθνική νομοθεσία του κράτους του άλλου Μέρους. Οι έλεγχοι ασφαλείας θα είναι ισοδύναμοι σύμφωνα με το Άρθρο 3.

5. Οι Αρμόδιες Αρχές Ασφαλείας, κατόπιν αιτήματος, θα αλληλοβοηθούνται, σύμφωνα με την εθνική νομοθεσία, στην διεξαγωγή των διαδικασιών ελέγχου ασφαλείας για την εφαρμογή της παρούσας Συμφωνίας.

6. Στα πλαίσια της παρούσας Συμφωνίας, οι Αρμόδιες Αρχές Ασφαλείας αλληλοενημερώνονται χωρίς καθυστέρηση σχετικά με τυχόν αλλαγές των Ελέγχων Ασφαλείας Προσωπικού και Φορέα, και πιο συγκεκριμένα όταν πρόκειται για την απόσυρση ή την υποβάθμισή τους.

7. Το Μέρος Παραλήπτης:

α) υποβάλλει Διαβαθμισμένες Πληροφορίες σε τυχόν Τρίτο Πρόσωπο μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα,

β) διαβαθμίζει την παραληφθείσα πληροφορία σύμφωνα με το Άρθρο 3,

γ) χρησιμοποιεί Διαβαθμισμένες Πληροφορίες μόνο για τους σκοπούς για τους οποίους επιλέχθηκε.

Άρθρο 6
Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται μέσω της διπλωματικής οδού, εκτός εάν προβλέπεται διαφορετικά από την Αρμόδια Αρχή Ασφαλείας. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτός την λήψη των διαβαθμισμένων Πληροφοριών.

2. Η ηλεκτρονική διαβίβαση Διαβαθμισμένων Πληροφοριών θα γίνεται μέσω πιστοποιημένων κρυπτογραφικών μέσων τα οποία εγκρίνονται από τις Αρμόδιες Αρχές Ασφαλείας.

Άρθρο 7
Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών

1. Οι μεταφράσεις και οι αναπαραγωγές Διαβαθμισμένων Πληροφοριών θα γίνονται σύμφωνα με την εθνική νομοθεσία του Μέρους Παραλήπτη και τις ακόλουθες διαδικασίες:

α) τα φυσικά πρόσωπα θα διαθέτουν την κατάλληλη πιστοποίηση Ελέγχου Ασφαλείας Προσωπικού, σύμφωνα με την εθνική νομοθεσία τους,

β) οι μεταφράσεις και οι αναπαραγωγές θα διαβαθμίζονται και προστατεύονται όπως και οι πρωτότυπες Διαβαθμισμένες Πληροφορίες,

γ) οι μεταφράσεις και ο αριθμός των αντιγράφων θα περιορίζονται στον αριθμό που απαιτείται για επίσημους σκοπούς,

δ) οι μεταφράσεις θα φέρουν κατάλληλη σημείωση στην γλώσσα μετάφρασης, υποδεικνύοντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες που λήφθηκαν από το Μέρος Αποστολέα.

2. Οι Πληροφορίες με διαβάθμιση ΑΠΟΡΡΗΤΟ και άνω, θα μεταφράζονται ή θα αναπαράγονται μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα.

Άρθρο 8
Καταστροφή Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες καταστρέφονται ώστε να αποφευχθεί η εν μέρει ή ολική ανακατασκευή.

2. Οι Πληροφορίες με διαβάθμιση ΑΠΟΡΡΗΤΟ καταστρέφονται σύμφωνα με την εθνική νομοθεσία.

3. Οι Πληροφορίες με διαβάθμιση ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ δεν καταστρέφονται. Επιστρέφονται στην Αρμόδια Αρχή Ασφαλείας του Μέρους Αποστολέα.

4. Συντάσσεται έκθεση για την καταστροφή των Διαβαθμισμένων Πληροφοριών και η μετάφρασή της στην αγγλική γλώσσα αποστέλλεται στην Αρμόδια Αρχή Ασφαλείας του Μέρους Αποστολέα.

Άρθρο 9
Διαβαθμισμένες Σύμβάσεις

1. Το κράτος του ενός Μέρους, το οποίο επιθυμεί να υπογράψει Διαβαθμισμένη Σύμβαση με κάποιον Εργολάβο από το κράτος του Άλλου Μέρους, ή επιθυμεί να επιτρέψει σε κάποιον από τους Εργολάβους του να υπογράψει Διαβαθμισμένη Σύμβαση στην επικράτεια του κράτους του άλλου Μέρους στα πλαίσια διαβαθμισμένου έργου οφείλει να εξασφαλίσει, μέσω της οικίας Αρμόδιας Αρχής Ασφαλείας, την εκ των προτέρων γραπτή εγγύηση της Αρμόδιας Αρχής Ασφαλείας του κράτους του άλλου Μέρους, ότι οι προτεινόμενος Εργολάβος διαθέτει πιστοποίηση Ελέγχου Ασφαλείας Φορέα του συγκεκριμένου επιπέδου ασφαλείας.

2. Κάθε Διαβαθμισμένη Σύμβαση που συνάπτεται σύμφωνα με την παρούσα Συμφωνία, περιλαμβάνει:

α) δέσμευση του Εργολάβου με την οποία διασφαλίζεται ότι οι εγκαταστάσεις του τηρούν τις απαραίτητες προϋποθέσεις για τον χειρισμό και αποθήκευση Διαβαθμισμένων Πληροφοριών στο συγκεκριμένο επίπεδο ασφαλείας,

β) δέσμευση του Εργολάβου με την οποία διασφαλίζεται ότι τα άτομα τα οποία εκτελούν καθήκοντα που απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες, διαθέτουν το κατάλληλο επίπεδο πιστοποίησης Ελέγχου Ασφαλείας Προσωπικού,

γ) δέσμευση του Εργολάβου με την οποία διασφαλίζεται όλα τα άτομα με πρόσβαση σε Διαβαθμισμένες Πληροφορίες έχουν ενημερωθεί για την ευθύνη τους αναφορικά με την προστασία Διαβαθμισμένων Πληροφοριών, σύμφωνα με την εθνική νομοθεσία,

δ) δέσμευση του Εργολάβου ότι θα προβαίνει σε περιοδικές επιθεωρήσεις ελέγχου των εγκαταστάσεών του,

ε) κατάλογο των Διαβαθμισμένων Πληροφοριών και κατάλογο τομέων στους οποίους μπορεί να προκύψουν Διαβαθμισμένες Πληροφορίες,

στ) διαδικασίες για την γνωστοποίηση των αλλαγών στα επίπεδα ασφαλείας των Διαβαθμισμένων Πληροφοριών,

ζ) μέσα επικοινωνίας και ηλεκτρονικά μέσα διαβίβασης,

η) διαδικασίες για την μεταφορά Διαβαθμισμένων Πληροφοριών,

θ) κατάλληλα εξουσιοδοτημένα φυσικά ή νομικά πρόσωπα τα οποία θα φέρουν την ευθύνη του συντονισμού της προστασίας των Διαβαθμισμένων Πληροφοριών που σχετίζονται με την Διαβαθμισμένη Σύμβαση,

ι) δέσμευση του Εργολάβου να ενημερώσει για τυχόν πραγματική ή ενδεχόμενη απώλεια, ή διαρροή Διαβαθμισμένων Πληροφοριών,

ια) δέσμευση του Εργολάβου να προωθήσει αντίγραφο της Διαβαθμισμένης Σύμβασης στην οικία Αρμόδια Αρχή Ασφαλείας,

ιβ) δέσμευση του υπεργολάβου να τηρήσει τις ίδιες υποχρεώσεις ασφαλείας με τον Εργολάβο.

3. Μόλις ξεκινήσουν οι διαπραγματεύσεις της σύμβασης μεταξύ του πιθανού Εργολάβου της επικράτειας του ενός κράτους με τον εργολάβο που βρίσκεται στο άλλο κράτος, και οι οποίες στοχεύουν στην σύναψη Διαβαθμισμένης Σύμβασης, η Αρμόδια Αρχή Ασφαλείας θα ενημερώσει το κράτος του άλλου Μέρους σχετικά με το επίπεδο ασφαλείας που δόθηκε στις Διαβαθμισμένες Πληροφορίες οι οποίες σχετίζονται με τις διαπραγματεύσεις αυτές.

4. Αντίγραφο της κάθε Διαβαθμισμένης Σύμβασης θα προωθηθεί στην Αρμόδια Αρχή Ασφαλείας του κράτους του Μέρους όπου πρόκειται να διεξαχθούν οι εργασίες, ώστε να επιτραπεί η κατάλληλη επίβλεψη και έλεγχος ασφαλείας.

5. Οι εκπρόσωποι των Αρμόδιων Αρχών Ασφαλείας δύνανται να ανταλλάσσουν επισκέψεις με σκοπό την ανάλυση της αποτελεσματικότητας των μέτρων που υιοθετεί ο Εργολάβος για την προστασία των Διαβαθμισμένων Πληροφοριών που αφορούν κάποια Διαβαθμισμένη Σύμβαση. Για την επίσκεψη θα αποστέλλεται ειδοποίηση τουλάχιστον 20 ημέρες νωρίτερα.

Άρθρο 10
Επισκέψεις

1. Οι επισκέψεις που αφορούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες από πολίτες του ενός κράτους στο άλλο κράτος, υπόκεινται στην εκ των προτέρων γραπτή έγκριση που παρέχεται από την Αρμόδια Αρχή Ασφαλείας του κράτους υποδοχής.

2. Οι επισκέψεις που αφορούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες επιτρέπονται από το κράτος του ενός Μέρους σε επισκέπτες από το κράτος του άλλου Μέρους, μόνο εάν έχουν εξασφαλίσει την κατάλληλη πιστοποίηση Ελέγχου Ασφαλείας Προσωπικού και την εξουσιοδότηση να λάβουν ή να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες σύμφωνα με την εθνική τους νομοθεσία.

3. Οι επισκέψεις που αφορούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες από πολίτες τρίτης χώρας επιτρέπονται μόνο με κοινή συμφωνία μεταξύ των κρατών των Μερών.

4. Η Αρμόδια Αρχή Ασφαλείας του κράτους υποδοχής θα πρέπει να λάβει την αίτηση επίσκεψης από την άλλη Αρμόδια Αρχή Ασφαλείας τουλάχιστον τριάντα ημέρες νωρίτερα.

5. Σε έκτακτες περιπτώσεις η αίτηση επίσκεψης μπορεί να διαβιβαστεί τουλάχιστον επτά ημέρες νωρίτερα.

6. Η αίτηση επίσκεψης περιλαμβάνει:

α) το ονοματεπώνυμο του επισκέπτη, τον τόπο και ημερομηνία γέννησης, την εθνικότητα και τον αριθμό διαβατηρίου ή ταυτότητας,

β) επωνυμία του νομικού προσώπου το οποίο εκπροσωπεί ο επισκέπτης,

γ) επωνυμία και διεύθυνση του νομικού προσώπου το οποίο πρόκειται να επισκεφτεί,

δ) επιβεβαίωση του πιστοποιητικού Ελέγχου Ασφαλείας Προσωπικού και της εγκυρότητάς του,

ε) σκοπό και λόγους της επίσκεψης,

στ) αναμενόμενη ημερομηνία και διάρκεια της επίσκεψης. Σε περίπτωση επαναλαμβανόμενων επισκέψεων, αναφέρεται η συνολική διάρκεια των επισκέψεων.

ζ) την ημερομηνία, υπογραφή και επίσημη σφραγίδα της Αρμόδιας Αρχής Ασφαλείας.

7. Μόλις εγκριθεί η επίσκεψη, η Αρμόδια Αρχή Ασφαλείας του κράτους υποδοχής αποστέλλει αντίγραφο της αίτησης επίσκεψης στους λειτουργούς ασφαλείας του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη.

8. Η ισχύς της έγκρισης επίσκεψης δεν υπερβαίνει το ένα έτος.

9. Τα κράτη των Μερών δύνανται να καταρτίσουν καταλόγους με φυσικά πρόσωπα τα οποία είναι εξουσιοδοτημένα να κάνουν επαναλαμβανόμενες επισκέψεις. Οι κατάλογοι ισχύουν για αρχική περίοδο δώδεκα μηνών. Οι όροι των αντίστοιχων επισκέψεων θα καθορίζονται από τα αρμόδια άτομα του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη, σύμφωνα με τους όρους και τις προϋποθέσεις που θα συμφωνηθούν.

Άρθρο 11
Παραβίαση της Ασφαλείας

1. Σε περίπτωση παραβίασης της ασφάλειας σύμφωνα με την εθνική νομοθεσία, η οποία επιφέρει πραγματική ή ενδεχόμενη διαρροή Διαβαθμισμένων Πληροφοριών οι οποίες στάλθηκαν ή λήφθηκαν από το κράτος του άλλου Μέρους, η Αρμόδια Αρχή Ασφαλείας του κράτους του Μέλους όπου έγινε η παραβίαση ή διαρροή, ενημερώνει την Αρμόδια Αρχή Ασφαλείας του κράτους του άλλου Μέρους, το συντομότερο δυνατόν, και ξεκινά την κατάλληλη έρευνα.

2. Εάν η παραβίαση της ασφάλειας γίνει σε Τρίτη χώρα, η Αρμόδια Αρχή Ασφαλείας του κράτους διανομής αναλαμβάνει δράσει σύμφωνα με την Παράγραφο 1.

3. Το κράτος του άλλου Μέρους, κατόπιν αιτήματος, συνεργάζεται στην έρευνα σύμφωνα με την Παράγραφο 1.

4. Το κράτος του άλλου Μέρους ενημερώνεται για τα αποτελέσματα της έρευνας και λαμβάνει την τελική έκθεση για τους λόγους και την έκταση της ζημιάς.

Άρθρο 12
Έξοδα

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

Άρθρο 13
Διευθέτηση Διαφορών

Τυχόν διαφορές που προκύπτουν από την ερμηνεία ή εφαρμογή της παρούσας Συμφωνίας, διευθετούνται με διαπραγματεύσεις μεταξύ των Αρμοδίων Αρχών Ασφαλείας.

Αρθρο 14
Τελικές Διατάξεις

1. Η συμφωνία αυτή συνάπτεται για απεριόριστο χρονικό διάστημα και τίθεται σε ισχύ την πρώτη ημέρα του δεύτερου μήνα μετά την ημερομηνία λήψης της τελευταίας γραπτής ειδοποίησης με την οποία τα Μέρη ανακοινώνουν το ένα στο άλλο, μέσω της διπλωματικής οδού, ότι έχουν εκπληρωθεί όλες οι αναγκαίες εθνικές νομικές προϋποθέσεις που απαιτούνται για την έναρξη ισχύος της παρούσας Συμφωνίας.

2. Η Συμφωνία αυτή δύναται να τροποποιείται από καιρό σε καιρό βάσει κοινής γραπτής έγκρισης των Μερών.

3. Κάθε Μέρος δύναται, ανά πάσα στιγμή, να καταγγείλει την Συμφωνία με γραπτή ειδοποίηση στο άλλο Μέρος, μέσω της διπλωματικής οδού. Στην περίπτωση αυτή, η λήξη της Συμφωνίας θα ισχύει έξι μήνες μετά την ημερομηνία λήψης της αντίστοιχης ανακοίνωσης.

4. Παρά την καταγγελία της παρούσας Συμφωνίας, τα Μέρη θα διασφαλίσουν ώστε όλες οι Διαβαθμισμένες Πληροφορίες θα συνεχίσουν να προστατεύονται έως ότου το Μέρος αποστολέας απαλλάξει το Μέρος παραλήπτη από τις υποχρεώσεις του.

Συντάχθηκε στην Μπρατισλάβα, στις 11 Νοεμβρίου 2010, σε δύο πρωτότυπα σετ αντιγράφων, στην ελληνική, σλοβακική και αγγλική γλώσσα και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση διαφωνίας στην ερμηνεία, το Αγγλικό κείμενο υπερισχύει.

Για την Κυβέρνηση της Κυπριακής Δημοκρατίας

.....

Μάρκος Κυπριανού
Υπουργός Εξωτερικών

Για την Κυβέρνηση της Δημοκρατίας της Σλοβακίας

.....

František Blanárik
Διευθυντής Εθνικής Αρχής Ασφαλείας

Μέρος III

Dohoda medzi vládou Cyperskej republiky a vládou Slovenskej republiky o vzájomnej ochrane utajovaných skutočností

Vláda Cyperskej republiky
a
vláda Slovenskej republiky

(ďalej len „zmluvné strany")

uznávajúc potrebu stanoviť pravidlá ochrany utajovaných skutočností navzájom vymieňaných v rámci politickej, vojenskej, ekonomickej, právnej, vedeckej, technologickej alebo inej spolupráce, ako i utajovaných skutočností, ktoré sa v priebehu takejto spolupráce vyskytnú,

majúc v úmysle zabezpečiť vzájomnú ochranu všetkých utajovaných skutočností, ktoré sú utajované v štáte jednej zmluvnej strany a odovzdané štátu druhej zmluvnej strany,

želajúc si vytvoriť sústavu pravidiel vzájomnej ochrany utajovaných skutočností vymieňaných medzi zmluvnými stranami,

berúc do úvahy vzájomné záujmy na ochrane utajovaných skutočností v súlade s právnymi predpismi štátov oboch zmluvných strán,

sa dohodli takto:

Článok 1
Cieľ dohody

Cieľom tejto dohody je zabezpečiť ochranu utajovaných skutočností spoločne vytvorených alebo vymenených medzi štátmi zmluvných strán.

Článok 2
Vymedzenie pojmov

Pre účely tejto dohody:

a) "utajovaný kontrakt" je dohoda medzi dvomi alebo viacerými kontrahentmi, ktorá obsahuje alebo zahŕňa utajované skutočnosti,

b) "utajované skutočnosti" sú akékoľvek informácie alebo veci bez ohľadu na svoju podobu alebo povahu, ktoré vyžadujú ochranu pred neoprávnenou manipuláciou a sú utajené v súlade s vnútroštátnymi právnymi predpismi štátov zmluvných strán,

c) "príslušný bezpečnostný orgán" je národný bezpečnostný orgán zodpovedný za implementáciu a dozor nad touto dohodou,

d) "kontrahent" je fyzická osoba alebo právnická osoba právne spôsobilá uzatvárať utajované kontrakty,

e) "previerka priemyselnej bezpečnosti" je zistenie príslušným bezpečnostným orgánom, že právnická osoba má fyzickú a organizačnú spôsobilosť používať a uchovávať utajované skutočnosti v súlade s príslušnými vnútroštátnymi právnymi predpismi,

f) "need-to-know" je potreba mať prístup k utajovaným skutočnostiam v rozsahu zastávanej funkcie a pre plnenie konkrétnych úloh,

g) "odovzdávajúca strana" je štát zmluvnej strany, ktorý odovzdáva utajované skutočnosti štátu druhej zmluvnej strany,

h) „previerka personálnej bezpečnosti" je zistenie príslušným bezpečnostným orgánom, že fyzická osoba je v súlade s príslušnými vnútroštátnymi právnymi predpismi oprávnená mať prístup k utajovaným skutočnostiam,

i) "prijímajúca strana" je štát zmluvnej strany, ktorému je utajovaná skutočnosť postúpená štátom druhej zmluvnej strany,

j) "tretia strana" je akýkoľvek štát, organizácia, právnická osoba alebo fyzická osoba, ktorá nie je zmluvnou stranou tejto dohody.

Článok 3
Stupne utajenia a oprávnenia

Zmluvné strany sa dohodli, že nasledujúce stupne utajenia a oprávnenia sú rovnocenné a zodpovedajú stupňom utajenia a oprávnenia stanoveným vnútroštátnymi právnymi predpismi ich štátov:

Pre Cyperskú republiku	Slovenská republika	Ekvivalent v anglickom jazyku
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	PRÍSNE TAJNÉ	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNÉ	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	DÔVERNÉ	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	VYHRADENÉ	RESTRICTED

Článok 4
Príslušné bezpečnostné orgány

1) Príslušné bezpečnostné orgány zmluvných strán sú:

Pre Cyperskú republiku:
Národný bezpečnostný úrad
4 Emmanuel Roidis str.
1432 Nikózia
Cyperská republika

Pre Slovenskú republiku:
Národný bezpečnostný úrad;
Budatínska 30
850 07 Bratislava
Slovenská republika

2) Štáty zmluvných strán sa navzájom informujú diplomatickou cestou o akýchkoľvek zmenách v kontaktných údajoch príslušných bezpečnostných orgánov.

3) Na žiadosť sa príslušné bezpečnostné orgány informujú o príslušných vnútroštátnych právnych predpisoch o ochrane utajovaných skutočností a vymieňajú si informácie o bezpečnostných štandardoch, postupoch a praxi pri ochrane utajovaných skutočností.

Článok 5
Ochranné opatrenia a prístup k utajovaným skutočnostiam

1) Štáty zmluvných strán vykonajú v súlade so svojimi vnútroštátnymi právnymi predpismi všetky príslušné opatrenia na ochranu utajovaných skutočností vymieňaných alebo vytvorených podľa tejto dohody. Takým utajovaným skutočnostiam sa prizná rovnaký stupeň ochrany, aký sa poskytuje národným utajovaným skutočnostiam so zodpovedajúcim stupňom utajenia v súlade s článkom 3.

2) Odovzdávajúca strana upovedomí prijímajúcu stranu písomne o akejkoľvek zmene v stupni utajenia postúpených utajovaných skutočností.

3) Prístup k utajovaným skutočnostiam sa obmedzí na základe need-to-know na osoby, ktoré sú v súlade s vnútroštátnymi právnymi predpismi oprávnené na prístup k utajovaným skutočnostiam zodpovedajúceho stupňa utajenia.

4) V rámci tejto dohody každý štát zmluvnej strany uzná previerky personálnej a priemyselnej bezpečnosti udelené v súlade s vnútroštátnymi právnymi predpismi štátu druhej zmluvnej strany. Bezpečnostné previerky sú ekvivalentné v súlade s článkom 3.

5) Príslušné bezpečnostné orgány si na žiadosť navzájom pomáhajú pri vykonávaní previerkového procesu potrebného pre vykonávanie tejto dohody.

6) V rámci tejto dohody sa príslušné bezpečnostné orgány navzájom bezodkladne informujú o akejkoľvek zmene týkajúcej sa previerok personálnej alebo priemyselnej bezpečnosti, najmä o ich zrušení alebo znížení stupňa oprávnenia.

7) Prijímajúca strana:

   a) utajované skutočnosti postúpi akejkoľvek tretej strane iba na základe predchádzajúceho písomného súhlasu odovzdávajúcej strany,

   b) označí prijaté utajované skutočnosti v súlade s článkom 3,

   c) použije utajované skutočnosti výlučne na účely, na ktoré boli postúpené.

Článok 6
Postupovanie utajovaných skutočností

1) Utajované skutočnosti sa postupujú diplomatickou cestou, ak sa príslušné bezpečnostné orgány nedohodnú inak. Prijímajúca strana potvrdí prijatie utajovaných skutočností písomne.

2) Elektronicky sa postupovanie utajovaných skutočností uskutoční prostredníctvom šifrových prostriedkov, na ktorých sa dohodnú príslušné bezpečnostné orgány.

Článok 7
Rozmnožovanie a preklad utajovaných skutočností

1) Preklady a rozmnožovanie utajovaných skutočností sa uskutočňujú v súlade s vnútroštátnymi právnymi predpismi prijímajúcej strany a týmito postupmi:

   a) fyzické osoby majú príslušnú previerku personálnej bezpečnosti v súlade s ich vnútroštátnymi právnymi predpismi,

   b) preklady a kópie sa označia a ochraňujú rovnako ako pôvodné utajované skutočnosti,

   c) preklady a počet kópií sú obmedzené úradnou potrebou,

   d) preklady obsahujú príslušnú poznámku v jazyku prekladu označujúcu, že preklad obsahuje utajované skutočnosti odovzdávajúcej strany.

2) Utajované skutočnosti označené TAJNÉ alebo vyšším stupňom utajenia sa prekladajú alebo rozmnožujú iba na základe predchádzajúceho písomného súhlasu odovzdávajúcej strany.

Článok 8
Zničenie utajovaných skutočností

1) Utajované skutočnosti sa zničia tak, aby sa vylúčilo ich čiastočné alebo úplné obnovenie.

2) Utajované skutočnosti označené TAJNÉ a nižším stupňom utajenia sa zničia v súlade s vnútroštátnymi právnymi predpismi.

3) Utajované skutočnosti označené PRÍSNE TAJNÉ sa nezničia. Vrátia sa príslušnému bezpečnostnému orgánu odovzdávajúcej strany.

4) O zničení utajovaných skutočností sa vyhotoví správa, ktorej anglický preklad sa doručí príslušnému bezpečnostnému orgánu odovzdávajúcej strany.

Článok 9
Utajované kontrakty

1) Štátu zmluvnej strany, ktorý má v úmysle uzavrieť utajovaný kontrakt s kontrahentom štátu druhej zmluvnej strany, alebo zamýšľa splnomocniť jedného zo svojich kontrahentov na uzavretie utajovaného kontraktu na území štátu druhej zmluvnej strany v rámci utajovaného projektu, sa doručí prostredníctvom jeho príslušného bezpečnostného orgánu predchádzajúce písomné uistenie od príslušného bezpečnostného orgánu štátu druhej zmluvnej strany, že navrhovaný kontrahent má previerku priemyselnej bezpečnosti príslušného stupňa oprávnenia

2) Každý utajovaný kontrakt uzavretý v súlade s touto dohodou obsahuje:

a) záväzok kontrahenta zabezpečiť, aby jeho priestory mali potrebné podmienky pre zaobchádzanie s utajovanými skutočnosťami príslušného stupňa utajenia a ich uchovávanie,

b) záväzok kontrahenta zabezpečiť, aby osoby, ktoré potrebujú na vykonávanie svojich povinností prístup k utajovaným skutočnostiam, mali príslušný stupeň previerky personálnej bezpečnosti,

c) záväzok kontrahenta zabezpečiť, aby všetky osoby, ktoré majú prístup k utajovaným skutočnostiam, boli oboznámené so svojou zodpovednosťou vo vzťahu k ochrane utajovaných skutočností v súlade s vnútroštátnymi právnymi predpismi,

d) záväzok kontrahenta vykonávať periodické bezpečnostné kontroly svojich priestorov,

e) zoznam utajovaných skutočností a zoznam oblastí, v ktorých môžu utajované skutočnosti vzniknúť,

f) postup pre oznámenie zmien stupňa utajenia utajovaných skutočností,

g) komunikačné a elektronické prostriedky pre postúpenie,

h) postup pri preprave utajovaných skutočností,

i) príslušné oprávnené fyzické osoby alebo právnické osoby zodpovedné za koordináciu dozoru nad utajovanými skutočnosťami vo vzťahu k utajovanému kontraktu,

j) záväzok kontrahenta oznámiť každú skutočnú alebo domnelú stratu, únik informácií alebo ohrozenie bezpečnosti utajovaných skutočností,

k) záväzok kontrahenta postúpiť kópiu utajovaného kontraktu svojmu príslušnému bezpečnostnému orgánu,

l) záväzok subkontrahenta splniť rovnaké bezpečnostné záväzky ako kontrahent.

3) Keď sa začnú predkontraktné rokovania medzi potenciálnym kontrahentom na území štátu jednej zmluvnej strany a iným potenciálnym kontrahentom z územia štátu druhej zmluvnej strany, s cieľom podpísať utajované kontrakty, príslušný bezpečnostný orgán informuje štát druhej zmluvnej strany o stupni utajenia utajovaných skutočností súvisiacich s predkontraktnými rokovaniami.

4) S cieľom umožniť adekvátny bezpečnostný dohľad a kontrolu sa kópia utajovaného kontraktu postúpi príslušnému bezpečnostnému orgánu štátu zmluvnej strany, kde sa majú práce vykonať.

5) Zástupcovia príslušných bezpečnostných orgánov môžu uskutočňovať vzájomné návštevy s cieľom analyzovať účinnosť opatrení prijatých kontrahentom na ochranu utajovaných skutočností, ktorých sa utajovaný kontrakt týka. Oznámenie o návšteve sa zašle najmenej dvadsať dní vopred.

Článok 10
Návštevy

1) Návštevy zahŕňajúce prístup štátnych príslušníkov štátu jednej zmluvnej strany k utajovaným skutočnostiam štátu druhej zmluvnej strany sú predmetom predchádzajúceho písomného súhlasu daného príslušným bezpečnostným orgánom hostiteľského štátu.

2) Návštevy zahŕňajúce prístup k utajovaným skutočnostiam povolí štát jednej zmluvnej strany návštevníkom zo štátu druhej zmluvnej strany, len ak návštevníkom bola udelená príslušným bezpečnostným orgánom vysielajúceho štátu previerka personálnej bezpečnosti príslušného stupňa oprávnenia a ak sú oprávnení prijať alebo mať prístup k utajovaným skutočnostiam v súlade s ich vnútroštátnymi právnymi predpismi.

3) Návštevy zahŕňajúce prístup štátnych príslušníkov tretieho štátu sa povolia len na základe spoločnej dohody štátov zmluvných strán.

4) Príslušnému bezpečnostnému orgánu hostiteľského štátu žiadosť o vykonanie návštevy doručí príslušný bezpečnostný orgán druhého štátu aspoň tridsať dní vopred.

5) V súrnych prípadoch sa žiadosť o návštevu postúpi najmenej sedem dní vopred.

6) Žiadosť o vykonanie návštevy obsahuje:

a) meno a priezvisko, dátum a miesto narodenia, štátnu príslušnosť, číslo pasu alebo identifikačného dokladu návštevníka,

b) názov právnickej osoby, ktorú návštevník zastupuje,

c) názov a adresu právnickej osoby, ktorá má byť navštívená,

d) potvrdenie o previerke personálnej bezpečnosti návštevníka a jej platnosti,

e) cieľ a účel návštevy,

f) predpokladaný dátum a trvanie návštevy, o ktorú sa žiada. V prípade opakovaných návštev celkové obdobie pokrývajúce všetky návštevy,

g) dátum, podpis a odtlačok úradnej pečiatky príslušného bezpečnostného orgánu.

7) Po schválení návštevy príslušný bezpečnostný orgán hostiteľského štátu poskytne kópiu žiadosti o návštevu bezpečnostným zamestnancom právnickej osoby, kde sa má návšteva uskutočniť.

8) Platnosť povolenia návštevy nepresiahne jeden rok.

9) Štáty zmluvných strán môžu zostaviť zoznamy fyzických osôb oprávnených vykonávať opakované návštevy. Zoznamy sú platné spočiatku dvanásť mesiacov. Termíny konkrétnych návštev sa dohodnú s príslušnými kontaktnými osobami právnických osôb, ktoré majú tieto fyzické osoby navštíviť, v súlade s dohodnutými termínmi a podmienkami.

Článok 11
Porušenie bezpečnosti

1) V prípade porušenia bezpečnosti podľa vnútroštátnych právnych predpisov, ktoré má za následok skutočné alebo možné ohrozenie bezpečnosti utajovaných skutočností pochádzajúcich alebo prijatých od štátu druhej zmluvnej strany, príslušný bezpečnostný orgán štátu zmluvnej strany, kde k porušeniu alebo ohrozeniu bezpečnosti došlo, čo najskôr informuje príslušný bezpečnostný orgán štátu druhej zmluvnej strany a začne príslušné vyšetrovanie.

2) Ak k porušeniu bezpečnosti dôjde v štáte inom ako štáty zmluvných strán, príslušný bezpečnostný orgán vysielajúceho štátu vykoná úkony podľa odseku 1.

3) Štát druhej zmluvnej strany na žiadosť pri vyšetrovaní spolupracuje v súlade s odsekom 1.

4) Štát druhej zmluvnej strany je oboznámený s výsledkami vyšetrovania a dostane konečnú správu o dôvodoch a rozsahu spôsobenej škody.

Článok 12
Náklady

Každá zmluvná strana hradí vlastné náklady, pokiaľ ide o vykonávanie a dohľad nad vykonávaním tejto dohody.

Článok 13
Riešenie sporov

Akýkoľvek spor ohľadom výkladu alebo uplatňovania tejto dohody sa rieši rokovaniami medzi príslušnými bezpečnostnými orgánmi.

Článok 14
Záverečné ustanovenia

1) Táto dohoda sa uzaviera na neurčitý čas a nadobudne platnosť v prvý deň druhého mesiaca nasledujúceho po dátume prijatia poslednej písomnej notifikácie, ktorou si zmluvné strany diplomatickou cestou oznamujú, že boli splnené všetky vnútroštátne právne podmienky potrebné pre nadobudnutie jej platnosti.

2) Túto dohodu možno kedykoľvek meniť na základe vzájomného písomného súhlasu zmluvných strán.

3) Každá zmluvná strana môže túto dohodu kedykoľvek vypovedať písomným oznámením diplomatickou cestou. V takom prípade sa platnosť tejto dohody skončí uplynutím šiestich mesiacov odo dňa prijatia oznámenia o vypovedaní.

4) Zmluvné strany zabezpečia ochranu utajovaných skutočnosti aj po skončení platnosti tejto dohody, kým odovzdávajúca strana nezbaví prijímajúcu stranu tohto záväzku.

Dané v Bratislave, dňa novembra 2010, v dvoch pôvodných vyhotoveniach, každé v gréckom, slovenskom a anglickom jazyku, pričom každé znenie má rovnakú platnosť. V prípade rozdielnosti výkladu je rozhodujúce znenie v anglickom jazyku.

Za vládu
Cyperskej republiky

Markos Kyprianou

minister zahraničných vecí

Za vládu
Slovenskej republiky

František Blanárik

riaditeľ Národného bezpečnostného úradu