

Ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Ομοσπονδιακής Κυβέρνησης της Αυστρίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2015 εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος.

Αριθμός 8(ΙΙΙ) του 2015

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

Προοίμιο.

ΕΠΕΙΔΗ στις 17 Ιουλίου 2014 υπογράφηκε στη Βιέννη Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Ομοσπονδιακής Κυβέρνησης της Αυστρίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών· και

ΕΠΕΙΔΗ το Υπουργικό Συμβούλιο με την Απόφασή του υπ' αριθμό 2/2009 και ημερομηνίας 20.5.2009 ενέκρινε την έναρξη διαπραγματεύσεων για σύναψη της εν λόγω Συμφωνίας· και

ΕΠΕΙΔΗ το Υπουργικό Συμβούλιο με την Απόφασή του υπ' αριθμό 75.446 στη συνεδρία του ημερομηνίας 10.7.2013, αποφάσισε να εξουσιοδοτήσει τον Υπουργό Εξωτερικών να υπογράψει την εν λόγω Συμφωνία·

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 Ομοσπονδιακής Κυβέρνησης της Αυστρίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2015.

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 Ομοσπονδιακής Κυβέρνησης της Αυστρίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών, η σύναψη της οποίας εγκρίθηκε με τις Αποφάσεις του Υπουργικού Συμβουλίου με αρ. 2/2009 και ημερομηνία 20.5.2009 και με αρ. 75.446 και ημερομηνία 10.7.2013 και η οποία, εν συνεχεία, υπογράφηκε στη Βιέννη στις 17 Ιουλίου 2014.

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

3. Με τον παρόντα Νόμο κυρώνεται η Συμφωνία, τα πρωτότυπα κείμενα της οποίας εκτίθενται στην αγγλική γλώσσα στο Μέρος Ι του Πίνακα, στην ελληνική γλώσσα στο Μέρος ΙΙ του Πίνακα και στη γερμανική γλώσσα στο Μέρος ΙΙΙ του Πίνακα:

Νοείται ότι, σε περίπτωση διαφοράς μεταξύ των κειμένων που εκτίθενται στον Πίνακα, υπερισχύει το κείμενο που εκτίθεται στην αγγλική γλώσσα στο Μέρος Ι αυτού.

Αρμόδια αρχή για την εφαρμογή της Συμφωνίας.

4. Ως αρμόδια αρχή για την εφαρμογή της Συμφωνίας, καθορίζεται ο Υπουργός Αμυνας.

(Αγγλική γλώσσα)

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC
OF CYPRUS AND THE AUSTRIAN FEDERAL GOVERNMENT ON
MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Cyprus
and
the Austrian Federal Government

(hereinafter referred to as "the Parties"),

Intending to ensure the mutual protection of all Classified Information, which has been classified by one Party and transferred to the other Party or commonly generated in the course of co-operation between the Parties,

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

Considering the mutual interest in the protection of Classified Information in accordance with the national law of the 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 Parties.

Article 2
Definitions

For the purposes of this Agreement:

- a) "Breach of Security" means an act or an omission which is contrary to this Agreement or the national law of the Parties, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromising of Classified Information;
- b) "Classified Contract" means an agreement between two or more Contractors, which contains or the implementation of which requires access to or generation of Classified Information;
- c) "Classified Information" means any information, irrespective of its form or nature, which requires protection against any breach of security, has been granted a security

classification level in accordance with the national law of the Parties and has been marked as such;

- d) "Competent Security Authority" means the National Security Authority and any other competent entity which, according to the national law of the Parties, is responsible for the implementation of this Agreement;
- e) "Contractor" means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;
- f) "Facility Security Clearance" means the determination by the Competent Security Authority confirming, that the legal entity or and individual has the physical and organizational capability to handle and store Classified Information in accordance with the respective national law;
- g) "National Security Authority" means the state authority of each Party, which in accordance with its national law is responsible for the general implementation and supervision of this Agreement;
- h) "Need-to-know" means the necessity to have access to specific Classified Information in the scope of a given official position and for the performance of a specific task;
- i) "Originator" means the Party as well as any legal entity or individual under its jurisdiction which releases Classified Information;
- j) "Personnel Security Clearance" means the determination by the Competent Security Authority confirming, in accordance with the respective national law, that the individual is eligible to have access to Classified Information;
- k) "Receiver" means the Party as well as any legal entity or individual under its jurisdiction which receives Classified Information;
- l) "Third Party" means a legal entity or an individual which is not an Originator or Receiver of the Classified Information exchanged in accordance with this Agreement, a government not Party to this Agreement or an international organisation.

Article 3 Security Classification Levels

The Parties agree that the following security classification levels and markings are equivalent and correspond to the security classification levels and markings specified in their national law:

Republic of Cyprus	Republic of Austria	Republic of Greece
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STRENG GEHEIM	TOP SECRET
ΑΠΟΡΡΗΤΟ	GEHEIM	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	VERTRAULICH	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	EINGESCHRÄNKT	RESTRICTED

Article 4
Competent Security Authorities

1. The Parties shall notify each other through diplomatic channels of the Competent Security Authorities responsible for the implementation of this Agreement.
2. The National Security Authorities shall inform each other of respective national law on Classified Information and of any significant amendments thereto 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 law, the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. At least 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 Article 3.
2. The Originator shall inform the Receiver 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 authorised in accordance with the national law of the Parties to have access to Classified Information of the equivalent security classification level.
4. Within the scope of this Agreement, each Party shall recognise the Personnel Security Clearances and Facility Security Clearances granted in accordance with the national law of the other Party.
5. The Competent Security Authorities shall, in accordance with the national law, 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 of the Parties 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 Receiver shall:
 - a) submit Classified Information to any Third Party only upon prior written consent of the Originator;
 - b) mark the received Classified Information in accordance with 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 by the National Security Authorities. The Receiver shall confirm the receipt of Classified Information in writing.
2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed by the National 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 law applicable to the Receiver and the following procedures:
 - a) the translations and the reproductions shall be marked and protected as the original Classified Information;
 - b) the translations and the number of copies shall be limited to that required for official purposes;
 - c) the translations shall bear an appropriate note in the language of the translation indicating that it contains Classified Information received from the Originator.
2. Classified Information shall only be translated by persons duly authorized.
3. Classified Information marked ΑΠΟΡΡΗΤΟ/ GEHEIM / SECRET or above shall be translated or reproduced only upon prior written consent of the Originator.

Article 8 Destruction of Classified Information

1. Classified Information shall be destroyed in a manner that prevents its partial or total reconstruction.
2. Classified Information marked up to ΑΠΟΡΡΗΤΟ/GEHEIM /SECRET shall be destroyed in accordance with the national law. A report on destruction of Classified Information marked ΑΠΟΡΡΗΤΟ/GEHEIM /SECRET shall be made and its translation in English shall be delivered to the Competent Security Authority of the Originator.
3. Classified Information marked ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ STRENG GEHEIM /TOP SECRET shall not be destroyed. It shall be returned to the Competent Security Authority of the Originator.
4. In case of a crisis situation in which it is impossible to protect or return Classified Information it shall be destroyed immediately. The Receiver shall inform the Competent Security Authority of the Originator about this destruction as soon as possible.

Article 9 Classified Contracts

1. The Competent Security Authority of a Party, wishing to place a Classified Contract with a Contractor of the other Party, or wishing to authorise one of its own Contractors to place a Classified Contract in the territory of the other Party shall obtain prior written assurance from the Competent Security Authority of the other Party that the proposed Contractor is granted a Facility Security Clearance of the appropriate security classification level.
2. The Contractor shall submit information about potential sub-contractors for approval to the Competent Security Authority, in whose territory the work is to be performed.
3. 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 the appropriate security classification level;
 - b) commitment of the Contractor to ensure that persons who perform duties requiring access to Classified Information are authorised in accordance with the national law to have access to Classified Information of the equivalent security classification level;
 - c) requirement that the Contractor shall ensure that all persons authorised to have access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national law;
 - d) list of Classified Information and list of areas in which Classified Information can arise;
 - e) procedure for communication of changes in the security classification level of Classified Information;
 - f) communication means and electronic means for transmission;
 - g) procedure for the transmission of Classified Information;
 - h) commitment of the Contractor to notify any actual or suspected Breach of Security;
 - i) commitment of the Contractor to forward a copy of the Classified Contract to its own Competent Security Authority;
 - j) commitment of the subcontractor to fulfil the same security obligations as the Contractor.
4. As soon as pre-contractual negotiations begin between potential Contractors, the Competent Security Authority of the Originator shall inform the Competent Security Authority of the other Party of the security classification level given to the Classified Information related to those pre-contractual negotiations.
5. A copy of each Classified Contract shall be forwarded to the Competent Security Authority of the Party where the work is to be performed, to allow adequate security supervision and control.

Article 10 Visits

1. Visits involving access to Classified Information are subject to prior written approval of the Competent Security Authority of the host Party.
2. The Competent Security Authority of the host Party shall receive a request for visit at least ten days in advance. The Competent Security Authorities shall inform each other about the details of the visit and ensure the protection of personal data.
3. In urgent cases, the request for visit can be transmitted in shorter time.
4. The request for visit shall include:
 - a) visitor's name and surname, place and date of birth, citizenship, passport and/or identification document number;
 - b) name of the legal entity represented by the visitor and position of the visitor in the legal entity;
 - c) name, address and contact information of the legal entity to be visited;
 - d) confirmation of the visitor's Personnel Security Clearance, its validity and level;
 - 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 the official seal of the Competent Security Authority.
5. Once the visit has been approved, the Competent Security Authority of the host Party shall provide a copy of the request for visit to the security officers of the legal entity to be visited.
6. The validity of visit approval shall not exceed one year.
7. The Competent Security Authorities of the Parties may draw up lists of individuals authorised 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 a Breach of Security the Competent Security Authorities shall inform each other as soon as possible, and consult on the further steps to be undertaken in particular in relation to the investigation to be conducted in accordance with national law.
2. The Competent Security Authorities shall, upon request, co-operate in the investigation in accordance with Paragraph 1.
3. The Competent Security Authorities shall inform each other of the results of the investigation, proceedings and measures taken.

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 Parties.

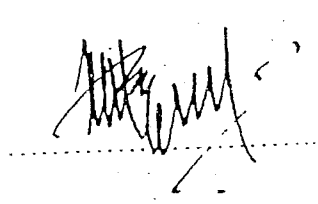
Article 14 Final Provisions

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. The amendments shall enter into force in accordance with paragraph 1.
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.

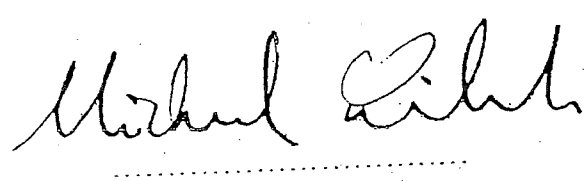
4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Originator dispenses the Receiver from this obligation.
5. Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the United Nations Charter, shall be initiated by the Party on whose national territory the Agreement is signed immediately following its entry into force. The other Party shall be informed of the registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat.

Done at VIENNA... on 17/7/2014..... in two originals, each in the Greek, German 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**



**For the Austrian Federal
Government**



(Ελληνική γλώσσα)

ΣΥΜΦΩΝΙΑ ΜΕΤΑΞΥ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΚΑΙ
ΤΗΣ ΟΜΟΣΠΟΝΔΙΑΚΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΑΥΣΤΡΙΑΣ ΓΙΑ ΤΗΝ ΑΜΟΙΒΑΙΑ
ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ.

Η Κυβέρνηση της Κυπριακής Δημοκρατίας και
η Ομοσπονδιακή Κυβέρνηση της Αυστρίας
(στο εξής τα «Μέρη»).

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία όλων των Διαβαθμισμένων Πληροφοριών που κατατάσσονται ως διαβαθμισμένες από ένα Μέρος και έχουν διαβιβασθεί στο άλλο Μέρος ή που παράγονται από κοινού, κατά τη διάρκεια της συνεργασίας μεταξύ των Μερών,

Επιθυμώντας να θεσπίσουν κανόνες για την αμοιβαία προστασία Διαβαθμισμένων Πληροφοριών που ανταλλάσσονται μεταξύ των Μερών,

Λαμβάνοντας υπόψη το αμοιβαίο συμφέρον για την προστασία Διαβαθμισμένων Πληροφοριών, σύμφωνα με την εθνική νομοθεσία των Μερών.

Συμφώνησαν τα ακόλουθα:

Άρθρο 1
Σκοπός

Σκοπός της παρούσας Συμφωνίας είναι να διασφαλισθεί η προστασία των Διαβαθμισμένων Πληροφοριών που παράγονται από κοινού ή ανταλλάσσονται μεταξύ των Μερών.

Άρθρο 2
Ερμηνεία

Για τους σκοπούς της παρούσας Συμφωνίας:

α) «Παράβαση Ασφαλείας» σημαίνει πράξη ή παράλειψη η οποία είναι αντίθετη με την παρούσα Συμφωνία ή την εθνική νομοθεσία των Μερών, το αποτέλεσμα της οποίας δύναται να οδηγήσει σε αποκάλυψη, απώλεια, καταστροφή, υπεξάιρεση ή οποιαδήποτε άλλη διαρροή Διαβαθμισμένων Πληροφοριών

β) «Διαβαθμισμένη Σύμβαση» σημαίνει συμφωνία μεταξύ δύο ή περισσότερων Ανάδοχων, η οποία περιέχει ή η υλοποίηση της οποίας απαιτεί την πρόσβαση σε Διαβαθμισμένες Πληροφορίες ή την παραγωγή τέτοιων Πληροφοριών

γ) «Διαβαθμισμένες Πληροφορίες» σημαίνει οποιεσδήποτε πληροφορίες, ανεξάρτητα από τη μορφή ή τη φύση τους, οι οποίες χρήζουν προστασίας. Επίσης, οποιεσδήποτε παράβασης ασφαλείας, οι οποίες έχουν επισημανθεί με κατάλληλη σήμανση διαβάθμισης σύμφωνα με την εθνική νομοθεσία των Μερών.

δ) «Αρμόδια Αρχή Ασφαλείας» σημαίνει την Εθνική Αρχή Ασφαλείας και οποιαδήποτε άλλη αρμόδια οντότητα η οποία, σύμφωνα με την εθνική νομοθεσία των Μερών, είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας.

ε) «Ανάδοχος» σημαίνει το πρόσωπο ή την νομική οντότητα που διαθέτει την νομική ικανότητα να συνάπτει Διαβαθμισμένες Συμβάσεις.

στ) «Διαβάθμιση Ασφαλείας Εγκαταστάσεων» σημαίνει τον προσδιορισμό από την Αρμόδια Αρχή Ασφαλείας που βεβαιώνει ότι η νομική οντότητα και το πρόσωπο έχει τη φυσική και την οργανωτική ικανότητα να χειρίζεται και να αποθηκεύει Διαβαθμισμένες Πληροφορίες σύμφωνα με την αντίστοιχη εθνική νομοθεσία.

ζ) «Εθνική Αρχή Ασφαλείας» σημαίνει τη κρατική αρχή έκαστου Μέρους, η οποία, σύμφωνα με την εθνική του νομοθεσία, είναι υπεύθυνη για την γενική εφαρμογή και εποπτεία τήρησης της παρούσας Συμφωνίας.

η) «Αρχή της «Ανάγκης για γνώση» σημαίνει την ανάγκη για πρόσβαση σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες στο πλαίσιο συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας.

θ) «Εντολέας» σημαίνει το Μέρος καθώς και οποιαδήποτε νομική οντότητα ή πρόσωπο που υπάγεται στη δικαιοδοσία του που διαβιβάζει Διαβαθμισμένες Πληροφορίες.

ι) «Διαβάθμιση Ασφαλείας Πρόσωπικού» σημαίνει τον προσδιορισμό της Αρμόδιας Αρχής Ασφαλείας βεβαιώνοντας ότι, σύμφωνα με την αντίστοιχη εθνική νομοθεσία, το πρόσωπο είναι εξουσιοδοτημένο όπως έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες.

κ) «Παραλήπτης» σημαίνει το Μέρος καθώς και οποιαδήποτε νομική οντότητα που υπάγεται στην δικαιοδοσία του που λαμβάνει Διαβαθμισμένες Πληροφορίες.

λ) «Τρίτο Πρόσωπο» σημαίνει οποιαδήποτε νομική οντότητα ή πρόσωπο που δεν είναι ο Εντολέας ή ο Παραλήπτης των Διαβαθμισμένων Πληροφοριών που ανταλλάσσονται σύμφωνα με την παρούσα Συμφωνία, κυβέρνηση που δεν είναι Συμβαλλόμενο Μέρος στην παρούσα Συμφωνία ή διεθνή οργανισμό.

Άρθρο 3 Επισημάνσεις Διαβάθμισης Ασφαλείας

Τα Μέρη συμφωνούν όπως οι ακόλουθες επισημάνσεις διαβάθμισης ασφαλείας είναι ισοδύναμες και αντίστοιχες με τις επισημάνσεις διαβάθμισης ασφαλείας που προσδιορίζονται στην εθνική τους νομοθεσία:

Για την Κυπριακή Δημοκρατία	Για την Ομοσπονδία της Αυστρίας	Αντίστοιχη Αγγλική ορολογία
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STRENG GEHEIM	TOP SECRET
ΑΠΟΡΡΗΤΟ	GEHEIM	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	VERTRAULICH	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	EINGESCHRÄNKT	RESTRICTED

Άρθρο 4 Αρμόδιες Αρχές Ασφαλείας

1. Τα Μέρη ενημερώνονται αμοιβαία μέσω της διπλωματικής οδού για τις Αρμόδιες Αρχές Ασφαλείας που είναι υπεύθυνες για την εφαρμογή της παρούσας Συμφωνίας.
2. Οι Εθνικές Αρχές Ασφαλείας ενημερώνονται αμοιβαία για την αντίστοιχη εθνική νομοθεσία περί Διαβαθμισμένων Πληροφοριών και για οποιεσδήποτε σημαντικές τροποποιήσεις σε αυτή και θα ανταλλάσσουν πληροφορίες για τὰ πρότυπα ασφαλείας, τις διαδικασίες και τις πρακτικές που εφαρμόζονται για την προστασία Διαβαθμισμένων Πληροφοριών.

Άρθρο 5 Προστατευτικά Μέτρα και Πρόσβαση σε Διαβαθμισμένες Πληροφορίες

1. Σύμφωνα με την εθνική τους νομοθεσία, τα Μέρη θα λαμβάνουν όλα τα αναγκαία μέτρα για την προστασία Διαβαθμισμένων Πληροφοριών, που ανταλλάσσονται ή παράγονται δυνάμει της παρούσας Συμφωνίας. Αποδίδεται τουλάχιστον ο ίδιος βαθμός προστασίας στις εν λόγω Διαβαθμισμένες Πληροφορίες όπως προβλέπεται για την εθνική Διαβαθμισμένη Πληροφορία, βάσει του ισοδύναμου βαθμού διαβάθμισης ασφαλείας σύμφωνα με το Άρθρο 3.

2. Η Εντολέας ενημερώνει γραπτώς τον Παραλήπτη για οποιαδήποτε αλλαγή στο βαθμό διαβάθμισης ασφαλείας των Διαβαθμισμένων Προσωπικών που έχουν διαβιβασθεί.
3. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται σε πρόσωπα που έχουν εξουσιοδοτηθεί σύμφωνα με την εθνική νομοθεσία των Μερών να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες του αντίστοιχου βαθμού διαβάθμισης ασφαλείας, σύμφωνα με την αρχή της ανάγκης για γνώση.
4. Στο πλαίσιο εφαρμογής της παρούσας Συμφωνίας, έκαστο των Μερών θα αναγνωρίζει τη Διαβάθμιση Ασφαλείας Εγκαταστάσεων και τη Διαβάθμιση Ασφαλείας Προσωπικού που έχει χορηγηθεί σύμφωνα με την εθνική νομοθεσία του άλλου Μέρους.
5. Οι Αρμόδιες Αρχές Ασφαλείας, θα συνεργάζονται μεταξύ τους, [σύμφωνα με την εθνική νομοθεσία], κατόπιν αιτήματος, στη διενέργεια διαδικασιών ελέγχου που απαιτούνται για την εφαρμογή της παρούσας Συμφωνίας.
6. Στο πλαίσιο εφαρμογής της παρούσας Συμφωνίας, οι Αρμόδιες Αρχές Ασφαλείας των Μερών θα ενημερώνονται αμοιβαία, χωρίς καθυστέρηση, για οποιαδήποτε αλλαγή όσον αφορά τη Διαβάθμιση Ασφαλείας Εγκαταστάσεων και Προσωπικού, και ειδικότερα όσον αφορά την αφαίρεση ή την υποβάθμιση της διαβάθμισης τους.
7. Ο Παραλήπτης θα:
 - α) διαβιβάσει Διαβαθμισμένες Πληροφορίες σε οποιοδήποτε Τρίτο Μέρος μόνο με την προηγούμενη γραπτή συγκατάθεσή του Εντολέα.
 - β) επισημαίνει τις Διαβαθμισμένες Πληροφορίες που έχουν ληφθεί σύμφωνα με το Άρθρο 3.
 - γ) χρησιμοποιεί τις Διαβαθμισμένες Πληροφορίες μόνο για το σκοπό που έχει καθορισθεί.

Άρθρο 6
Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται μέσω της διπλωματικής οδού εκτός αν συμφωνηθεί διαφορετικά από τις Εθνικές Αρχές Ασφαλείας. Ο Παραλήπτης επιβεβαιώνει γραπτώς την λήψη των Διαβαθμισμένων Πληροφοριών.

2. Η ηλεκτρονική διαβίβαση Διαβαθμισμένων Πληροφοριών θα πραγματοποιείται μέσω πιστοποιημένων μέσων κρυπτογράφησης όπως συμφωνείται μεταξύ των Εθνικών Αρχών Ασφαλείας.

Άρθρο 7
Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών

1. Η μετάφραση και η αναπαραγωγή Διαβαθμισμένων Πληροφοριών θα γίνεται σύμφωνα με την εθνική νομοθεσία που εφαρμόζεται για τον Παραλήπτη και με βάση τις ακόλουθες διαδικασίες:

α) η μετάφραση και η αναπαραγωγή θα φέρει τη σήμανση και θα έχει την ίδια ιεραρχία όπως η πρωτότυπη Διαβαθμισμένη Πληροφορία.

β) η μετάφραση και ο αριθμός των αντιγράφων θα περιορίζεται στον αριθμό που απαιτείται για καθορισμένους σκοπούς.

γ) η μετάφραση θα περιέχει κατάλληλη σημείωση στη γλώσσα της μετάφρασης ότι περιέχει Διαβαθμισμένες Πληροφορίες που έχουν ληφθεί από τον Εντολέα.

2. Οι Διαβαθμισμένες Πληροφορίες θα μεταφράζονται μόνο από δεόντως εξουσιοδοτημένα πρόσωπα.

3. Διαβαθμισμένες Πληροφορίες με τη σήμανση GEHEIM / ΑΠΟΡΡΗΤΟ / SECRET ή υψηλότερη διάβαθμιση μεταφράζονται ή αναπαράγονται μόνο με την προηγούμενη γραπτή συγκατάθεση του Εντολέα.

Άρθρο 8
Καταστροφή Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες θα καταστρέφονται με τέτοιο τρόπο ώστε να αποτρέπεται ο μερικός ή ο ολικός ανασχηματισμός τους.
2. Διαβαθμισμένες Πληροφορίες με τη σήμανση GEHEIM / ΑΠΟΡΡΗΤΟ / SECRET θα καταστρέφονται σύμφωνα με την εθνική νομοθεσία. Θα συντάσσεται έκθεση για την καταστροφή Διαβαθμισμένων Πληροφοριών με τη σήμανση GEHEIM / ΑΠΟΡΡΗΤΟ / SECRET και η μετάφραση της στην Αγγλική γλώσσα θα παραδοθεί στην Αρμόδια Αρχή Ασφαλείας του Εντολέα.
3. Διαβαθμισμένες Πληροφορίες με τη σήμανση AKRΩΣ ΑΠΟΡΡΗΤΟ/STRENG GEHEIM/TOP SECRET, δεν θα καταστρέφονται. Θα επιστρέφονται στην Αρμόδια Αρχή Ασφαλείας του Εντολέα.
4. Σε περίπτωση κατάστασης κρίσης, στην οποία είναι αδύνατη η προστασία ή η επιστροφή Διαβαθμισμένων Πληροφοριών, τέτοιες πληροφορίες καταστρέφονται αμέσως. Ο Παραλήπτης θα ενημερώσει την Αρμόδια Αρχή Ασφαλείας του Εντολέα αναφορικά με την καταστροφή το συντομότερο δυνατό.

Άρθρο 9
Διαβαθμισμένες Συμβάσεις

1. Η Αρμόδια Αρχή Ασφαλείας ενός Μέρους που επιθυμεί να συνάψει Διαβαθμισμένη Σύμβαση με Ανάδοχο του άλλου Μέρους, ή επιθυμεί όπως εξουσιοδοτήσει έναν από τους δικούς του Ανάδοχους να συνάψει Διαβαθμισμένη Σύμβαση στην επικράτεια του άλλου Μέρους, εξασφαλίζει την προηγούμενη γραπτή βεβαίωση της Αρμόδιας Αρχής Ασφαλείας του άλλου Μέρους ότι ο προτεινόμενος Ανάδοχος έχει εξασφαλίσει Διαβάθμιση Ασφαλείας Εγκαταστάσεων κατάλληλου βαθμού διαβάθμισης ασφαλείας.
2. Ο Ανάδοχος υποβάλλει στοιχεία για τους προτεινόμενους υπεργολάβους για έγκριση προς την Αρμόδια Αρχή Ασφαλείας στην επικράτεια του οποίου θα εκτελεσθεί το έργο.
3. Κάθε Διαβαθμισμένη Σύμβαση που συνάπτεται σύμφωνα με την παρούσα Συμφωνία θα περιέχει:
 - a) δέσμευση του Ανάδοχου ότι θα διασφαλίζει ότι οι εγκαταστάσεις του διαθέτουν τις απαραίτητες προϋποθέσεις για το χειρισμό και την αποθήκευση Διαβαθμισμένων Πληροφοριών του κατάλληλου βαθμού διαβάθμισης ασφαλείας.

β) δέσμευση του Ανάδοχου ότι θα διασφαλίζει ότι τα πρόσωπα που εκτελούν καθήκοντα που απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες έχουν εξουσιοδοτηθεί σύμφωνα με την εθνική νομοθεσία να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες του αντίστοιχου βαθμού διαβάθμισης ασφαλείας.

γ) ρήτρα ότι ο Ανάδοχος διασφαλίζει ότι όλα τα πρόσωπα που έχουν εξουσιοδοτηθεί να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες έχουν ενημερωθεί όσον αφορά την ευθύνη που έχουν για την προστασία των εν λόγω Διαβαθμισμένων Πληροφοριών σύμφωνα με την εθνική νομοθεσία.

δ) κατάλογο των Διαβαθμισμένων Πληροφοριών και κατάλογο των τομέων διαβάθμισης πληροφοριών που δύναται να προκύψουν.

ε) διαδικασία για την ενημέρωση επί αλλαγών στο βαθμό διαβάθμισης ασφαλείας των Διαβαθμισμένων Πληροφοριών.

στ) τα μέσα επικοινωνίας και ηλεκτρονικά μέσα για σκοπούς διαβίβασης.

ζ) τη διαδικασία για τη διαβίβαση Διαβαθμισμένων Πληροφοριών.

η) δέσμευση του Ανάδοχου όπως κοινοποιεί οποιαδήποτε πραγματική ή υποπτευόμενη Παράβαση Ασφαλείας.

θ) δέσμευση του Ανάδοχου να προωθεί αντίγραφο της Διαβαθμισμένης Σύμβασης στη δική του Αρμόδια Αρχή Ασφαλείας.

ι) δέσμευση του υπο-εργολάβου να ακολουθήσει τις ίδιες υποχρεώσεις ασφαλείας όπως ο Ανάδοχος.

4. Μόλις αρχίσουν οι προ-συμβατικές διαβουλεύσεις μεταξύ των προτεινόμενων Συμβαλλόμενων, η Αρμόδια Αρχή Ασφαλείας του Εντολέα θα ενημερώσει την Αρμόδια Αρχή Ασφαλείας του άλλου Μέρους όσον αφορά το βαθμό διαβάθμισης ασφαλείας που έχει δοθεί στις Διαβαθμισμένες Πληροφορίες σε σχέση με τις εν λόγω προ-συμβατικές διαβουλεύσεις.

5. Αντίγραφο κάθε Διαβαθμισμένης Σύμβασης θα αποστέλλεται στην Αρμόδια Αρχή Ασφαλείας του Μέρους όπου θα εκτελεσθεί το έργο ώστε να υπάρχει επαρκής εποπτεία και έλεγχος ασφάλειας.

Άρθρο 10 Επισκέψεις

1. Επισκέψεις που αφορούν την πρόσβαση σε Διαβαθμισμένες Πληροφορίες θα υπόκεινται στην προηγούμενη γραπτή έγκριση της Αρμόδιας Αρχής Ασφαλείας του φιλοξενούντος Μέρους.
2. Η Αρμόδια Αρχή Ασφαλείας του φιλοξενούντος Μέρους θα λαμβάνει αίτημα για επίσκεψη τουλάχιστον δέκα μέρες προηγουμένως. Οι Αρμόδιες Αρχές Ασφαλείας θα ενημερώνονται για τα στοιχεία της επίσκεψης και θα διασφαλίζουν την προστασία προσωπικών δεδομένων.
3. Σε έκτακτες περιπτώσεις, το αίτημα για επίσκεψη δύναται να διαβιβασθεί σε λιγότερο χρόνο.
4. Το αίτημα για επίσκεψη θα περιλαμβάνει:
 - α) το όνομα και επίθετο του επισκέπτη, την ημερομηνία και τον τόπο γεννήσεως, την υπηκοότητα και/η τον αριθμό δελτίου ταυτότητας.
 - β) το όνομα της νομικής οντότητας την οποία αντιπροσωπεύει ο επισκέπτης και τη θέση που κατέχει ο επισκέπτης στην νομική οντότητα.
 - γ) το όνομα, επίθετο, στοιχεία επικοινωνίας και θέση της νομικής οντότητας που θα επισκεφθεί.
 - δ) πιστοποίηση του Ελέγχου Ασφαλείας Προσωπικού που κατέχει ο επισκέπτης, της εγκυρότητας και του επιπέδου ασφαλείας του.
 - ε) το αντικείμενο και τον σκοπό της επίσκεψης.
 - στ) την αναμενόμενη ημερομηνία και διάρκεια της αιτούμενης επίσκεψης. Στην περίπτωση επαναλαμβανόμενων επισκέψεων, θα αναφέρεται η συνολική περίοδος που καλύπτεται από τις επισκέψεις.
 - ζ) την ημερομηνία, υπογραφή και την επίσημη σφραγίδα της Αρμόδιας Αρχής Ασφαλείας.
5. Εφ' όσον η επίσκεψη έχει εγκριθεί, η Αρμόδια Αρχή Ασφαλείας του φιλοξενούν Μέρους προσκομίζει αντίγραφο του αιτήματος για την επίσκεψη στους αξιωματικούς ασφαλείας της νομικής οντότητας που θα δεχθεί την επίσκεψη.

6. Η ισχύς της έγκρισης για επίσκεψη δεν θα υπερβαίνει το ένα έτος.

7. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών δύνανται να καταρτίσουν κατάλογο των προσώπων που έχουν εξουσιοδοτηθεί να προβαίνουν σε επαναλαμβανόμενες επισκέψεις. Ο κατάλογος θα ισχύει αρχικά για περίοδο δώδεκα μηνών. Οι όροι των αντίστοιχων επισκέψεων θα διευθετούνται απευθείας με τα σημεία επαφής της εν λόγω νομικής οντότητας που θα δέχεται την επίσκεψη από τα εν λόγω πρόσωπα, σύμφωνα με τους όρους και τις προϋποθέσεις που θα συμφωνηθούν.

Άρθρο 11 Παράβαση Ασφαλείας

1. Σε περίπτωση Παράβασης Ασφαλείας οι Αρμόδιες Αρχές Ασφαλείας ενημερώνουν η μία την άλλη το συντομότερο δυνατό και διαβουλεύονται σχετικά με τα περαιτέρω μέτρα που θα λάβουν και ειδικότερα σε σχέση με την διερεύνηση που θα διεξαχθεί σύμφωνα με την εθνική νομοθεσία.

2. Οι Αρμόδιες Αρχές Ασφαλείας, κατόπιν αιτήματος, συνεργάζονται στην διερεύνηση σύμφωνα με την παράγραφο 1.

3. Οι Αρμόδιες Αρχές Ασφαλείας ενημερώνουν η μία την άλλη για το αποτέλεσμα της έρευνας, τις διαδικασίες και τα μέτρα που έχουν ληφθεί.

Άρθρο 12 Δαπάνες

Έκαστο των Μερών καλύπτει τις δαπάνες του οι οποίες προκύπτουν από την εφαρμογή και εποπτεία εφαρμογής, της παρούσας Συμφωνίας.

Άρθρο 13 Επίλυση Διαφορών

Οποιαδήποτε διαφορά που αφορά την ερμηνεία ή την εφαρμογή της παρούσας Συμφωνίας θα επιλύεται με διαβουλεύσεις μεταξύ των Μερών.

Άρθρο 14 Τελικές Διατάξεις

1. Η παρούσα Συμφωνία συνομολογήθηκε για απεριόριστο χρόνο και τίθεται σε ισχύ την πρώτη μέρα του δεύτερου μήνα που έπεται της ημερομηνίας κατά την οποία τα Μέρη θα έχουν κοινοποιήσει εκατέρωθεν μέσω της διπλωματικής οδού, την ολοκλήρωση των εσωτερικών νομικών

διαδικασιών που απαιτούνται για την έναρξη ισχύος της παρούσας Συμφωνίας.

2. Η παρούσα Συμφωνία δύναται να τροποποιηθεί οποτεδήποτε με την αμοιβαία γραπτή συμφωνία των Μερών. Οι τροποποιήσεις τίθενται σε ισχύ σύμφωνα με τις πρόνοιες της Παραγράφου 1.

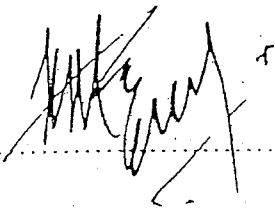
3. Έκαστο των Μερών δύναται οποτεδήποτε να τερματίσει την παρούσα Συμφωνία κατόπιν γραπτής ειδοποίησης προς το άλλο Μέρος που δίδεται μέσω της διπλωματικής οδού. Σε τέτοια περίπτωση ο τερματισμός τίθεται σε ισχύ έξι μήνες μετά την ημερομηνία λήψης της ειδοποίησης τερματισμού.

4. Ανεξάρτητα από τον τερματισμό της παρούσας Συμφωνίας, τα Μέρη διασφαλίζουν ότι όλες οι Διαβαθμισμένες Πληροφορίες εξακολουθούν να προστατεύονται μέχρι ο Εντολέας να απαλλάξει τον Παραλήπτη από την υποχρέωση αυτή.

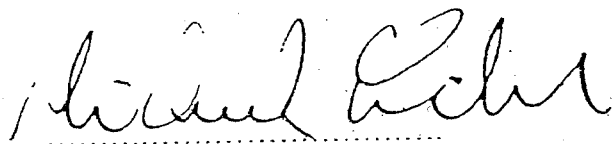
5. Η εγγραφή της παρούσας Συμφωνίας στη Γραμματεία των Ηνωμένων Εθνών, σύμφωνα με το Άρθρο 102 του Καταστατικού Χάρτη των Ηνωμένων Εθνών, θα προωθηθεί από το Μέρος στην εθνική επικράτεια του οποίου υπογράφεται η Συμφωνία αμέσως μετά την έναρξη ισχύος της. Το άλλο Μέρος θα ενημερωθεί για την εγγραφή και για τον αριθμό εγγραφής της Συμφωνίας, μόλις αυτό επιβεβαιωθεί από τη Γραμματεία των Ηνωμένων Εθνών.

Έγινε στην Βιέννη στις 17/7/2004 και συντάχθηκε σε δύο αντίτυπα, το κάθε ένα στα Γερμανικά, στα Ελληνικά και στην Αγγλική γλώσσα, όλα δε τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση απόκλισης στην ερμηνεία υπερισχύει το Αγγλικό κείμενο.

Εκ Μέρους της Κυβέρνησης
της Κυπριακής Δημοκρατίας



Εκ Μέρους της Ομοσπονδιακής
Κυβέρνησης της Αυστρίας



(Γερμανική γλώσσα)

**ABKOMMEN ZWISCHEN DER REGIERUNG DER REPUBLIK ZYPERN UND DER
ÖSTERREICHISCHEN BUNDESREGIERUNG ÜBER DEN GEGENSEITIGEN
SCHUTZ KLASSIFIZIERTER INFORMATIONEN**

Die Regierung der Republik Zypern und die Österreichische Bundesregierung (im Weiteren „die Parteien“ genannt),

In der Absicht, den gegenseitigen Schutz aller klassifizierten Informationen, die von einer Partei als klassifiziert eingestuft und an die andere Partei übermittelt oder im Zuge der Zusammenarbeit zwischen den Parteien gemeinsam erstellt wurden, zu gewährleisten,

Von dem Wunsch geleitet, ein Regelwerk über den gegenseitigen Schutz der zwischen den Parteien ausgetauschten klassifizierten Informationen zu schaffen,

In Erwägung des gemeinsamen Interesses des Schutzes klassifizierter Informationen, in Übereinstimmung mit dem innerstaatlichen Recht der Parteien,

Sind wie folgt übereingekommen.

**ARTIKEL 1
ZIEL**

Ziel dieses Abkommens ist es, den Schutz der im Zuge der Zusammenarbeit zwischen den Parteien gemeinsam erstellten oder ausgetauschten klassifizierten Informationen zu gewährleisten.

**ARTIKEL 2
BEGRIFFSBESTIMMUNGEN**

Für die Zwecke dieses Abkommens bedeutet:

a) "Sicherheitsverletzung" eine Handlung oder eine Unterlassung, die gegen dieses Abkommen oder das innerstaatliche Recht der Parteien verstößt, deren Ergebnis zu Offenlegung, Verlust, Zerstörung, Veruntreuung oder einer anderen Art von Beeinträchtigung klassifizierter Informationen führen kann;

b) „Klassifizierter Vertrag“ ein Vertrag zwischen zwei oder mehreren Auftragnehmern bzw. Auftragnehmern, der klassifizierte Informationen enthält oder dessen Erfüllung den Zugang zu oder die Erstellung von klassifizierten Informationen erfordert;

c) "Klassifizierte Informationen" Informationen, unabhängig von ihrer Form oder Art, die des Schutzes gegen jegliche Sicherheitsverletzung bedürfen, denen gemäß dem innerstaatlichen Recht der Parteien eine Sicherheitsklassifizierungsstufe zugeordnet wurden und die als solche gekennzeichnet wurden.

d) "Zuständige Sicherheitsbehörde" die nationale Sicherheitsbehörde und jede andere zuständige Stelle, die nach dem innerstaatlichen Recht der Parteien für die Umsetzung dieses Abkommens verantwortlich ist;

e) "Aufnahmenehmer bzw. Auftraggeber" eine natürliche oder juristische Person, die über die rechtliche Fähigkeit verfügt, klassifizierte Verträge abzuschließen;

f) "Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen" die Feststellung durch eine zuständige Sicherheitsbehörde, dass eine juristische oder natürliche Person zum Umgang mit und zur Aufbewahrung von klassifizierten Informationen gemäß dem jeweiligen innerstaatlichen Recht physisch und organisatorisch in der Lage ist;

g) "Nationale Sicherheitsbehörde" die staatliche Behörde einer der Parteien, die gemäß ihrem innerstaatlichen Recht für die allgemeine Umsetzung und Aufsicht über dieses Abkommens verantwortlich ist;

h) "Need-to-know" die Notwendigkeit, Zugang zu bestimmten klassifizierten Informationen im Rahmen einer vorgegebenen offiziellen Stellung und für die Erfüllung einer bestimmten Aufgabe zu haben;

i) "Herausgeber" die Partei sowie jede ihrer Hoheitsgewalt unterstehende juristische oder natürliche Person, die klassifizierte Informationen herausgibt;

j) "Sicherheitsunbedenklichkeitsbescheinigung für Personen" die Feststellung durch die zuständige Sicherheitsbehörde, dass eine Person zum Zugang zu klassifizierten Informationen gemäß dem innerstaatlichen Recht berechtigt ist;

k) "Empfänger" die Partei sowie jede ihrer Hoheitsgewalt unterstehende juristische oder natürliche Person, die klassifizierte Informationen erhält;

l) „Dritter“ eine juristische oder natürliche Person, die nicht Herausgeber oder Empfänger der klassifizierten Informationen ist, die gemäß diesem Abkommen ausgetauscht wurden, eine Regierung, die nicht Partei dieses Abkommens ist, oder eine internationale Organisation.

ARTIKEL 3 SICHERHEITSKLASSIFIZIERUNGSSTUFEN

Die Parteien legen fest, dass folgende Sicherheitsklassifizierungsstufen und Kennzeichnungen gleichwertig sind und sie den Sicherheitsklassifizierungsstufen und Kennzeichnungen nach dem jeweiligen innerstaatlichen Recht entsprechen:

ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STRENG GEHEIM	TOP SECRET
ΑΠΟΡΡΗΤΟ	GEHEIM	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	VERTRAULICH	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	EINGESCHRÄNKΤ	RESTRICTED

ARTIKEL 4 ZUSTÄNDIGE SICHERHEITSBEHÖRDEN

1. Die Parteien informieren einander auf diplomatischem Wege über die für die Durchführung dieses Abkommens zuständigen Sicherheitsbehörden.
2. Die nationalen Sicherheitsbehörden informieren einander über das jeweilige innerstaatliche Recht über klassifizierte Informationen und über alle diesbezügliche maßgebliche Änderungen und tauschen Informationen über die Sicherheitsstandards, Verfahren und Praktiken des Schutzes klassifizierter Informationen aus.

ARTIKEL 5 SCHUTZMAßNAHMEN UND ZUGANG ZU KLASSIFIZIERTEN INFORMATIONEN

1. Gemäß ihrem innerstaatlichen Recht treffen die Parteien alle geeigneten Maßnahmen zum Schutz der klassifizierten Informationen, die im Rahmen dieses Abkommens ausgetauscht oder erstellt wurden. Solchen klassifizierten Informationen wird mindestens der gleiche Schutzstandard, wie es für innerstaatliche klassifizierte Informationen vorgesehen ist, mit der gemäß Artikel 3 gleichwertigen Sicherheitsklassifizierungsstufe gewährt.
2. Der Herausgeber informiert den Empfänger schriftlich über jede Änderung der Sicherheitsklassifizierungsstufe der übermittelten klassifizierten Informationen.
3. Der Zugang zu Klassifizierten Informationen wird nach dem Grundsatz des Need-to-know auf Personen beschränkt, die gemäß dem innerstaatlichen Recht der Parteien zum Zugang zu klassifizierten Informationen der gleichwertigen Sicherheitsklassifizierungsstufe ermächtigt sind.
4. Im Rahmen dieses Abkommens anerkennt jede Partei die Sicherheitsunbedenklichkeitsbescheinigungen für Personen und Unternehmen, die gemäß dem innerstaatlichen Recht der anderen Partei ausgestellt wurden.
5. Die zuständigen Sicherheitsbehörden unterstützen sich gegenseitig gemäß ihrem innerstaatlichen Recht auf Anfrage bei der Durchführung der Sicherheitsüberprüfung der für die Anwendung dieses Abkommens erforderlichen Verfahren.
6. Im Rahmen dieses Abkommens informieren die zuständigen Sicherheitsbehörden der Parteien einander unverzüglich über jede Änderung bezüglich der Sicherheitsunbedenklichkeitsbescheinigungen für Personen und Unternehmen, insbesondere über ihren Widerruf oder ihre Herabstufung.
7. Der Empfänger
 - a) gibt klassifizierte Informationen nur nach vorheriger schriftlicher Zustimmung des Herausgebers an Dritte heraus;
 - b) kennzeichnet empfangene klassifizierte Informationen gemäß Artikel 3;
 - c) verwendet klassifizierte Informationen nur für die dafür vorgesehenen Zwecke.

ARTIKEL 6 ÜBERMITTLUNG KLASSIFIZIERTER INFORMATIONEN

1. Klassifizierte Informationen werden auf diplomatischem Weg, sofern von der zuständigen Sicherheitsbehörde nicht anders gewünscht, übermittelt. Der Empfänger bestätigt den Empfang der klassifizierten Informationen in schriftlicher Form.
2. Elektronische Übermittlung von klassifizierten Informationen wird mit von den innerstaatlichen Sicherheitsbehörden vereinbarten zertifizierten kryptografischen Mitteln durchgeführt.

ARTIKEL 7 VERVIELFÄLTIGUNG UND ÜBERSETZUNG KLASSIFIZIERTER INFORMATIONEN

1. Übersetzungen und Vervielfältigungen klassifizierter Informationen erfolgen in Übereinstimmung mit dem für den Empfänger geltenden innerstaatlichen Recht und gemäß den folgenden Verfahren:
 - a) Übersetzungen und Vervielfältigungen werden wie die ursprünglichen klassifizierten Informationen gekennzeichnet und geschützt;
 - b) Übersetzungen und die Anzahl der Kopien werden auf die für amtliche Zwecke notwendigen beschränkt;
 - c) Übersetzungen tragen einen entsprechenden Hinweis in der Übersetzungssprache; der anzeigt, dass sie klassifizierte Informationen des Herausgebers enthalten.
2. Klassifizierte Informationen werden nur von befugten Personen übersetzt.
3. Als ΑΠΟΡΡΗΤΟ / GEHEIM / SECRET oder mit einer höheren Sicherheitsklassifizierungsstufe gekennzeichnete klassifizierte Informationen werden nur nach vorheriger schriftlicher Zustimmung des Herausgebers übersetzt oder vervielfältigt.

ARTIKEL 8 VERNICHUNG KLASSIFIZIERTER INFORMATIONEN

1. Klassifizierte Informationen werden auf einer Weise vernichtet, die ihre teilweise oder vollständige Wiederherstellung verhindert.
2. Als bis zu ΑΠΟΡΡΗΤΟ / GEHEIM / SECRET gekennzeichnete klassifizierte Informationen werden in Übereinstimmung mit dem innerstaatlichen Recht vernichtet. Über die Vernichtung von als ΑΠΟΡΡΗΤΟ / GEHEIM / SECRET gekennzeichneten klassifizierten Informationen wird ein Bericht verfasst und dessen Übersetzung in die englische Sprache wird der zuständigen Sicherheitsbehörde des Herausgebers übermittelt.

3. Als ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / STRENG GEHEIM / TOP SECRET gekennzeichnete klassifizierte Informationen dürfen nicht vernichtet werden. Sie werden an die zuständige Sicherheitsbehörde des Herausgebers rückübermittelt.

4. Im Falle einer Krisensituation, in der es unmöglich ist, klassifizierte Informationen zu schützen oder rückzuübermitteln, werden diese umgehend vernichtet. Der Empfänger informiert die zuständige Sicherheitsbehörde des Herausgebers sobald wie möglich über diese Vernichtung.

ARTIKEL 9 KLASSIFIZIERTE VERTRÄGE

1. Die zuständige Sicherheitsbehörde einer Partei, die einen klassifizierten Vertrag mit einem Auftragnehmer der anderen Partei abschließen möchte, oder einen seiner eigenen Auftragnehmer ermächtigen möchte, einen klassifizierten Vertrag im Hoheitsgebiet der anderen Partei abzuschließen, holt die vorherige schriftliche Zustimmung der zuständigen Sicherheitsbehörde der anderen Partei ein, dass dem vorgeschlagene Auftragnehmer eine Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen der entsprechenden Sicherheitsklassifizierungsstufe gewährt wurde.

2. Der Auftragnehmer legt Informationen über potenzielle Subunternehmer der zuständigen Sicherheitsbehörde, in deren Hoheitsgebiet die Arbeit durchgeführt werden soll, zur Genehmigung vor.

3. Jeder gemäß diesem Abkommen abgeschlossene klassifizierte Vertrag enthält:

a) die Verpflichtung des Auftragnehmers sicherzustellen, dass seine Räumlichkeiten die notwendigen Voraussetzungen für die Handhabung und Lagerung von klassifizierten Informationen der angemessenen Sicherheitsklassifizierungsstufe haben;

b) die Verpflichtung des Auftragnehmers sicherzustellen, dass Personen, die Aufgaben erfüllen, die den Zugang zu klassifizierten Informationen erfordern, gemäß dem innerstaatlichen Recht zum Zugang zu klassifizierten Informationen der entsprechenden Sicherheitsklassifizierungsstufe berechtigt sind;

c) das Erfordernis, dass der Auftragnehmer sicherstellt, dass alle Personen, die Zugang zu klassifizierten Informationen haben, über ihre Verantwortung für den Schutz klassifizierter Informationen gemäß ihrem innerstaatlichen Recht informiert sind;

d) eine Liste der klassifizierten Informationen und eine Liste der Bereiche, in der klassifizierte Informationen entstehen können;

e) das Verfahren für die Mitteilung von Veränderungen der Sicherheitsklassifizierungsstufe klassifizierter Informationen;

f) Kommunikationsmittel und elektronische Übermittlungsmittel;

g) das Verfahren für die Übermittlung von klassifizierten Informationen;

h) die Verpflichtung des Auftragnehmers, jede tatsächliche oder vermutete Sicherheitsverletzung bekanntzugeben;

i) die Verpflichtung des Auftragnehmers, eine Kopie des klassifizierten Vertrags an seine eigene zuständige Sicherheitsbehörde zu übermitteln;

j) die Verpflichtung der Subunternehmer, die gleichen Sicherheitsverpflichtungen wie der Auftragnehmer zu erfüllen.

4. Sobald vorvertraglichen Verhandlungen zwischen potenziellen Auftragnehmern bzw. Auftraggebern beginnen, informiert die zuständige Sicherheitsbehörde des Auftragnehmers die zuständige Sicherheitsbehörde der anderen Partei über die Sicherheitsklassifizierungsstufe, die den klassifizierten Informationen im Zusammenhang mit diesen vorvertraglichen Verhandlungen gegeben wurden.

5. Eine Kopie jedes klassifizierten Vertrags wird an die zuständige Sicherheitsbehörde der Partei, wo die Arbeit durchgeführt werden soll, weitergeleitet, um eine ausreichende Sicherheitsüberwachung und Kontrolle zu ermöglichen.

ARTIKEL 10 BESUCHE

1. Besuche, die den Zugang zu klassifizierten Informationen betreffen, unterliegen der vorherigen Genehmigung durch die zuständige Behörde der gastgebenden Partei.

2. Die zuständige Sicherheitsbehörde der gastgebenden Partei erhält mindestens zehn Tage im Voraus einen Besuchs Antrag. Die zuständigen Sicherheitsbehörden informieren einander über die Einzelheiten des Besuchs und gewährleisten den Schutz der persönlichen Daten.

3. In dringenden Fällen kann der Besuchs Antrag in kürzerer Zeit übermittelt werden.

4. Der Antrag soll Folgendes enthalten:

a) Vor- und Familienname, Geburtsdatum und -ort, Staatsangehörigkeit, Pass und / oder Personalausweisnummer des Besuchers;

b) Name der juristischen Person, die durch den Besucher vertreten wird und die Funktion des Besuchers in der juristischen Person;

c) Name, Anschrift und Kontaktdaten der juristischen Person, die besucht wird;

d) eine Bestätigung der Sicherheitsunbedenklichkeitsbescheinigung des Besuchers, ihrer Gültigkeit und Sicherheitsstufe;

e) Ziel und Zweck des Besuchs;

f) voraussichtlicher Termin und Dauer des beantragten Besuchs. Im Fall wiederholter Besuche ist der gesamte von den Besuchen abgedeckte Zeitraum, anzugeben,

g) Datum, Unterschrift und Amtssiegel der zuständigen Sicherheitsbehörde.

5. Sobald der Besuch genehmigt wurde, stellt die zuständige Sicherheitsbehörde der gastgebenden Partei eine Kopie des Besucherantrags dem Sicherheitsbeamten der juristischen Person, die besucht wird, zur Verfügung.

6. Die Gültigkeit der Besuchsgenehmigung darf ein Jahr nicht überschreiten.

7. Die zuständigen Sicherheitsbehörden der Parteien können Listen von Personen ausarbeiten, die berechtigt sind wiederkehrende Besuche zu machen. Die Listen gelten zunächst für einen Zeitraum von zwölf Monaten. Die Bedingungen der jeweiligen Besuche werden unmittelbar mit den entsprechenden Anlaufstellen in der juristischen Person vereinbart, die in Übereinstimmung mit den vereinbarten Bestimmungen und Bedingungen von diesen Personen besucht werden.

ARTIKEL 11 SICHERHEITSVERLETZUNGEN

1. Im Falle einer Sicherheitsverletzung informieren die zuständigen Sicherheitsbehörden einander gegenseitig so schnell wie möglich und beraten über die weiteren Schritte, die insbesondere bezüglich der Untersuchung unternommen werden, die in Übereinstimmung mit dem innerstaatlichen Recht durchgeführt wird.

2. Die zuständigen Sicherheitsbehörden arbeiten auf Anfrage bei der Untersuchung gemäß Absatz 1 zusammen.

3. Die zuständigen Sicherheitsbehörden informieren einander über die Ergebnisse der Untersuchung, der Verfahren und der eingeleiteten Maßnahmen.

ARTIKEL 12 KOSTEN

Jede Partei trägt die Kosten, die ihr im Zusammenhang mit der Durchführung dieses Abkommens entstehen.

ARTIKEL 13 STREITBEILEGUNG

Jegliche Streitigkeit über die Auslegung oder Anwendung dieses Abkommens wird durch Verhandlungen zwischen den Parteien beigelegt.

ARTIKEL 14 SCHLUSSBESTIMMUNGEN

1. Dieses Abkommen wird auf unbestimmte Zeit geschlossen und tritt am ersten Tag des zweiten Monats nach dem Tag des Eingangs der letzten schriftlichen Mitteilung in Kraft, an dem die Parteien einander auf diplomatischem Wege den Abschluss der für das Inkrafttreten des Abkommens erforderlichen innerstaatlichen Verfahren mitgeteilt haben.

2. Dieses Abkommen kann jederzeit im gegenseitigen schriftlichen Einvernehmen beider Vertragsparteien geändert werden. Änderungen treten gemäß Absatz 1 in Kraft.

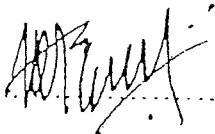
3. Jede Partei kann dieses Abkommen jederzeit durch schriftliche Mitteilung an die andere Partei auf diplomatischem Wege kündigen. In diesem Fall wird die Kündigung sechs Monate nach Erhalt der entsprechenden Mitteilung wirksam.

4. Ungeachtet der Beendigung dieses Abkommens gewährleisten die Parteien, dass alle klassifizierten Informationen weiterhin geschützt werden, bis der Herausgeber den Empfänger von dieser Verpflichtung entbindet.

5. Die Registrierung dieses Abkommens beim Sekretariat der Vereinten Nationen gemäß Artikel 102 der Satzung der Vereinten Nationen wird unmittelbar nach seinem Inkrafttreten von der Partei eingeleitet, auf deren Hoheitsgebiet das Abkommen unterzeichnet wurde. Die andere Partei wird über die Registrierung und die UN-Registrierungsnummer informiert, sobald diese vom Sekretariat bestätigt wurde.

Geschehen in WIEN am 7/7/2014..... in zwei Urschriften, jede in griechischer, deutscher und englischer Sprache, wobei jeder Text gleichermaßen authentisch ist. Im Falle unterschiedlicher Auslegung geht der englische Text vor.

Für die Regierung der Republik Zypern:



Für die Österreichische Bundesregierung:

