

Ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Ομοσπονδιακής Δημοκρατίας της Γερμανίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2018 εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος.

Αριθμός 14(ΙΙΙ) του 2018

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

Προοίμιο. ΕΠΕΙΔΗ το Υπουργικό Συμβούλιο με την Απόφασή του υπ' αριθμό 2/2009 και ημερομηνία 20 Μαΐου 2009, μεταξύ άλλων, ενέκρινε την έναρξη διαπραγματεύσεων με τη Γερμανία, για τη σύναψη συμφωνίας ασφαλείας για την ανταλλαγή και την αμοιβαία προστασία διαβαθμισμένων πληροφοριών· και

ΕΠΕΙΔΗ το Υπουργικό Συμβούλιο με την Απόφασή του υπ' αριθμό 74.069 και ημερομηνία 5 Οκτωβρίου 2012, ενέκρινε τη Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών και εξουσιοδότησε τον Υπουργό Άμυνας να υπογράψει την εν λόγω Συμφωνία· και

ΕΠΕΙΔΗ το Υπουργικό Συμβούλιο με την Απόφασή του υπ' αριθμό Α81.278 και ημερομηνία 13 Σεπτεμβρίου 2016, ενέκρινε το τροποποιημένο κείμενο της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών· και

ΕΠΕΙΔΗ στις 27 Απριλίου 2017 υπογράφηκε στη Μάλτα Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Ομοσπονδιακής Δημοκρατίας της Γερμανίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών·

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 Ομοσπονδιακής Δημοκρατίας της Γερμανίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2018.

Ερμηνεία. 2. Στον παρόντα Νόμο –

«Συμφωνία» σημαίνει τη Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Ομοσπονδιακής Δημοκρατίας της Γερμανίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών, η διαπραγμάτευση της οποίας εγκρίθηκε με την Απόφαση του Υπουργικού Συμβουλίου με αρ. 2/2009 και ημερομηνία 20 Μαΐου 2009, η υπογραφή της οποίας εγκρίθηκε με τις Αποφάσεις του Υπουργικού Συμβουλίου με αρ. 74.069 και ημερομηνία 5.10.2012 και με αρ. Α81.278 και ημερομηνία 13 Σεπτεμβρίου 2016 και η οποία Συμφωνία, εν συνεχεία, υπογράφηκε στη Μάλτα στις 27 Απριλίου 2017.

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

Πίνακας.
Μέρος Ι,
Μέρος ΙΙ,
Μέρος ΙΙΙ.

Νοείται ότι, σε περίπτωση διαφοράς και/ή αντίφασης μεταξύ των κειμένων του Πίνακα, υπερισχύει το κείμενο που εκτίθεται στο Μέρος ΙΙΙ αυτού.

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

ΠΙΝΑΚΑΣ
(άρθρο 3)

ΜΕΡΟΣ Ι

(Κείμενο της Σύμβασης στην Ελληνική Γλώσσα)

ΜΕΡΟΣ ΙΙ

(Κείμενο της Σύμβασης στην Γερμανική Γλώσσα)

ΜΕΡΟΣ ΙΙΙ

(Κείμενο της Σύμβασης στην Αγγλική Γλώσσα)

**ΠΙΝΑΚΑΣ
(Άρθρο 3)**

**Μέρος Ι
(Ελληνική Γλώσσα)**

Συμφωνία

μεταξύ

της Κυβέρνησης της Κυπριακής Δημοκρατίας

και

της Κυβέρνησης της Ομοσπονδιακής Δημοκρατίας της Γερμανίας

για την

Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών

-

Η Κυβέρνηση της Κυπριακής Δημοκρατίας

και

η Κυβέρνηση της Ομοσπονδιακής Δημοκρατίας της Γερμανίας

(εφεξής καλούμενες τα «Συμβαλλόμενα Μέρη»)

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία των διαβαθμισμένων πληροφοριών, οι οποίες ανταλλάσσονται μεταξύ των αρμόδιων αρχών της Κυπριακής Δημοκρατίας και της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, καθώς και με αναδόχους στην επικράτεια του άλλου Συμβαλλόμενου Μέρους ή μεταξύ αναδόχων των δύο Συμβαλλομένων Μερών,

Επιθυμώντας να θεσπίσουν κανόνες για την αμοιβαία προστασία των Διαβαθμισμένων Πληροφοριών, οι οποίοι θα εφαρμόζονται σε όλες τις συμφωνίες συνεργασίας, οι οποίες πρόκειται να υπογραφούν μεταξύ των Συμβαλλομένων Μερών και στα συμβόλαια, που αφορούν στην ανταλλαγή διαβαθμισμένων πληροφοριών,

Συμφώνησαν τα ακόλουθα:

Άρθρο I

Ορισμοί

(1) Για τους σκοπούς της παρούσας Συμφωνίας

I. «διαβαθμισμένες πληροφορίες» σημαίνει

- (α) στην Ομοσπονδιακή Δημοκρατία της Γερμανίας γεγονότα, αντικείμενα ή πληροφορίες ασφαλείας που, ανεξαρτήτως του τρόπου παρουσίασής τους, πρέπει να παραμείνουν απόρρητα προς όφελος του δημοσίου συμφέροντος. Διαβαθμίζονται από κάποια επίσημη αρχή, ή με την υπόδειξη αυτής, ανάλογα με την ανάγκη προστασίας τους.

(β) στην Κυπριακή Δημοκρατία
κάθε πληροφορία ή υλικό, ανεξαρτήτως τύπου, μορφής ή φύσεως, που χρήζει προστασίας από μη εξουσιοδοτημένη γνωστοποίηση και/ή χρήση και διαβαθμίστηκε σύμφωνα με την εθνική νομοθεσία.

2. «διαβαθμισμένη σύμβαση» σημαίνει κάθε σύμβαση η οποία συνάπτεται μεταξύ κάποιας αρχής ή επιχείρησης από το κράτος του ενός Συμβαλλόμενου Μέρους (αναθέτων φορέας) και κάποιας επιχείρησης από το κράτος του άλλου Συμβαλλόμενου Μέρους (ανάδοχος). Στο πλαίσιο μιας τέτοιας σύμβασης, διαβαθμισμένες πληροφορίες από το κράτος του αναθέτοντος φορέα δίνονται στον ανάδοχο, δημιουργούνται από τον ανάδοχο ή γίνονται προσβάσιμες σε νομίμως εξουσιοδοτημένα μέλη του προσωπικού του ανάδοχου, τα οποία πρόκειται να εκτελέσουν εργασίες σε εγκαταστάσεις του αναθέτοντος φορέα.
3. «Αρμόδια Αρχή Ασφαλείας» σημαίνει την αρχή ή τις αρχές ασφαλείας κάθε Συμβαλλόμενου Μέρους, που ευθύνεται ή ευθύνονται για την εφαρμογή και εποπτεία της παρούσας Συμφωνίας.
4. «ανάδοχος» σημαίνει το φυσικό ή νομικό πρόσωπο που διαθέτει την απαραίτητη νομική ικανότητα σύναψης διαβαθμισμένων συμβάσεων.
5. «Εξουσιοδότηση Ασφάλειας Φορέα» σημαίνει την πιστοποίηση της Αρμόδιας Αρχής Ασφαλείας ότι το νομικό ή φυσικό πρόσωπο πληροί τα προσωπικά κριτήρια ασφαλείας και έχει τη φυσική και οργανωτική ικανότητα να χειρίζεται, να φυλάσσει και να προστατεύει διαβαθμισμένες πληροφορίες σύμφωνα με την εκάστοτε εθνική νομοθεσία.
6. «ανάγκη για γνώση» σημαίνει η ανάγκη πρόσβασης σε διαβαθμισμένες πληροφορίες στο πλαίσιο συγκεκριμένου καθήκοντος ή εργασίας.
7. «Πιστοποιητικό Ελέγχου Ασφαλείας» σημαίνει το πιστοποιητικό της Αρμόδιας Αρχής Ασφαλείας, το οποίο πιστοποιεί σύμφωνα με την αντίστοιχη εθνική νομοθεσία, ότι κάποιον φυσικό πρόσωπο δικαιούται να έχει πρόσβαση σε διαβαθμισμένες πληροφορίες συγκεκριμένων επιπέδων διαβάθμισης.

8. «τρίτο μέρος» σημαίνει κράτος, οργανισμό, νομικό ή φυσικό πρόσωπο, το οποίο δεν είναι Συμβαλλόμενο Μέρος στην παρούσα Συμφωνία.

(2) Τα επίπεδα διαβάθμισης ασφαλείας ορίζονται ως ακολούθως:

1. Στην Ομοσπονδιακή Δημοκρατία της Γερμανίας οι διαβαθμισμένες πληροφορίες χαρακτηρίζονται ως
 - α) STRENG GEHEIM εάν η αποκάλυψή τους σε μη εξουσιοδοτημένο άτομο ενδέχεται να αποτελέσει απειλή για την ύπαρξη ή τα ζωτικά συμφέροντα της Ομοσπονδιακής Δημοκρατίας της Γερμανίας ή κάποιου κρατιδίου της,
 - β) GEHEIM εάν η αποκάλυψή τους σε μη εξουσιοδοτημένο άτομο ενδέχεται να αποτελέσει απειλή για την ασφάλεια της Ομοσπονδιακής Δημοκρατίας της Γερμανίας ή κάποιου κρατιδίου της, ή να επιφέρει σοβαρή βλάβη στα συμφέροντά τους,
 - γ) VS-VERTRAULICH εάν η αποκάλυψή τους σε μη εξουσιοδοτημένο άτομο ενδέχεται να επιφέρει βλάβη στα συμφέροντα της Ομοσπονδιακής Δημοκρατίας της Γερμανίας ή κάποιου κρατιδίου της,
 - δ) VS-NUR FÜR DEN DIENSTGEBRAUCH εάν η αποκάλυψή τους σε μη εξουσιοδοτημένο άτομο ενδέχεται να αντιβαίνει στα συμφέροντα της Ομοσπονδιακής Δημοκρατίας της Γερμανίας ή κάποιου κρατιδίου της.
2. Στην Κυπριακή Δημοκρατία οι διαβαθμισμένες πληροφορίες χαρακτηρίζονται ως:
 - α) ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ: πληροφορίες και υλικό, του οποίου η μη εξουσιοδοτημένη αποκάλυψη θα μπορούσε να επιφέρει εξαιρετικά σοβαρή βλάβη στα ουσιώδη συμφέροντα της Κυπριακής Δημοκρατίας,

- β) ΑΠΟΡΡΗΤΟ: πληροφορίες και υλικό, του οποίου η μη εξουσιοδοτημένη αποκάλυψη θα μπορούσε να επιφέρει σοβαρή βλάβη στα ουσιώδη συμφέροντα της Κυπριακής Δημοκρατίας.
- γ) ΕΜΠΙΣΤΕΥΤΙΚΟ: πληροφορίες και υλικό, του οποίου η μη εξουσιοδοτημένη αποκάλυψη θα μπορούσε να επιφέρει βλάβη στα ουσιώδη συμφέροντα της Κυπριακής Δημοκρατίας.
- δ) ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ: πληροφορίες και υλικό, του οποίου η μη εξουσιοδοτημένη αποκάλυψη ενδέχεται να αντιβαίνει στα συμφέροντα της Κυπριακής Δημοκρατίας.

Άρθρο 2

Πίνακας Ισοδυναμίας

Τα Συμβαλλόμενα Μέρη συμφωνούν ότι τα ακόλουθα επίπεδα διαβάθμισης ασφαλείας είναι ισοδύναμα:

Για την Κυπριακή Δημοκρατία	Για την Ομοσπονδιακή Δημοκρατία της Γερμανίας	Αντίστοιχη αγγλική ορολογία
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STRENG GEHEIM	TOP SECRET
ΑΠΟΡΡΗΤΟ	GEHEIM	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	VS-VERTRAULICH	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTRICTED

Άρθρο 3

Επίσημανση Διαβάθμισης Ασφάλειας

(1) Οι διαβαθμισμένες πληροφορίες που ανταλλάσσονται θα φέρουν επίσημανση διαβάθμισης ασφαλείας που θα αντιστοιχεί συγκριτικά στο επίπεδο διαβάθμισης ασφαλείας, η οποία ορίζεται στην εθνική νομοθεσία των Συμβαλλομένων Μερών, σύμφωνα με το Άρθρο 2 από, ή εκ μέρους των αρμοδίων αρχών. Το αντισυμβαλλόμενο μέρος-παραλήπτης θα επισημαίνει τις πληροφορίες αυτές

αναλόγως.

(2) Διαβαθμισμένες πληροφορίες οι οποίες παράγονται από το αντισυμβαλλόμενο μέρος-παραλήπτη σε σχέση με διαβαθμισμένες συμβάσεις καθώς και αντίγραφα που γίνονται από το αντισυμβαλλόμενο μέρος-παραλήπτη, θα επισημαίνονται και αυτές.

(3) Οι διαβαθμίσεις ασφαλείας, κατόπιν αιτήματος της αρμόδιας αρχής του αντισυμβαλλόμενου μέρους αποστολέα, θα τροποποιούνται ή θα ακυρώνονται από ή εκ μέρους της αρμόδιας αρχής του μέρους παραλήπτη. Η αρμόδια αρχή του αντισυμβαλλόμενου μέρους αποστολέα οφείλει να ενημερώνει αμέσως την αρμόδια αρχή του αντισυμβαλλόμενου μέρους παραλήπτη για τροποποιήσεις ή ακυρώσεις κάποιας διαβάθμισης ασφαλείας.

Άρθρο 4

Μέτρα σε Εθνικό Επίπεδο

(1) Μέσα στα πλαίσια της εθνικής τους νομοθεσίας, τα Συμβαλλόμενα Μέρη λαμβάνουν όλα τα απαραίτητα μέτρα για την εγγύηση της προστασίας της ασφάλειας των διαβαθμισμένων πληροφοριών οι οποίες παράγονται, ανταλλάσσονται ή φυλάσσονται βάσει της παρούσας Συμφωνίας. Παρέχουν σε αυτές τις διαβαθμισμένες πληροφορίες τουλάχιστον το ίδιο επίπεδο προστασίας που προβλέπεται για τις εθνικές διαβαθμισμένες πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας.

(2) Οι διαβαθμισμένες πληροφορίες θα χρησιμοποιούνται αποκλειστικά για τον καθορισμένο σκοπό. Το Αντισυμβαλλόμενο Μέρος-Παραλήπτης υποχρεούται να μην αποκαλύπτει, να μην χρησιμοποιεί, ούτε να επιτρέπει την αποκάλυψη ή χρήση διαβαθμισμένων πληροφοριών, παρά μόνον για τους σκοπούς και εντός των περιορισμών που έχουν υποδειχθεί από ή εκ μέρους του Αντισυμβαλλόμενου Μέρους-Πάροχου. Το μέρος που παρέχει τις διαβαθμισμένες πληροφορίες θα πρέπει να δώσει την έγγραφη συγκατάθεσή του για τυχόν αντίθετες διευθετήσεις.

(3) Πρόσβαση σε διαβαθμισμένες πληροφορίες επιτρέπεται να έχουν μόνο πρόσωπα, τα οποία πληρούν λόγω των καθηκόντων τους την προϋπόθεση της «ανάγκης για γνώση» και τα οποία είναι – εκτός της περίπτωσης διαβαθμισμένων πληροφοριών «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH»,

εξουσιοδοτημένα να έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας. Η εξουσιοδότησή τους προϋποθέτει έναν έλεγχο ασφαλείας, ο οποίος πρέπει να είναι τουλάχιστον τόσο αυστηρός όσο ο έλεγχος που διενεργείται για την πρόσβαση σε εθνικές διαβαθμισμένες πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης.

(4) Η πρόσβαση σε διαβαθμισμένες πληροφορίες επιπέδου «ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH» ή υψηλότερο, από άτομο που έχει την υπηκοότητα ενός εκ των Συμβαλλομένων Μερών, θα δίδεται χωρίς την εκ των προτέρων έγκριση του αντισυμβαλλόμενου μέρους-πάρoχου.

(5) Ο Έλεγχος Ασφαλείας Προσωπικού για πρόσωπα υπηκόους του Συμβαλλόμενου Μέρους, τα οποία διαμένουν στην χώρα τους και χρειάζονται εκεί πρόσβαση σε διαβαθμισμένες πληροφορίες, θα διεξάγεται από τις οικείες Εθνικές Αρχές Ασφαλείας ή τις Καθορισθείσες Αρχές Ασφαλείας ή άλλες αρμόδιες εθνικές αρχές.

(6) Ωστόσο, ο Έλεγχος Ασφαλείας Προσωπικού για υπηκόους ενός εκ των Συμβαλλομένων Μερών, οι οποίοι διαμένουν νόμιμα στη χώρα του Αντισυμβαλλόμενου Μέρους και υποβάλλουν εκεί υποψηφιότητα για κάποια θέση εργασίας που απαιτεί πρόσβαση σε διαβαθμισμένες πληροφορίες επιπέδου «ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH» ή υψηλότερο, θα διεξάγεται από την Αρμόδια Αρχή Ασφαλείας του εν λόγω κράτους, η οποία ενδέχεται να αναζητήσει πληροφορίες ασφαλείας και στο εξωτερικό.

(7) Τα Συμβαλλόμενα Μέρη θα διασφαλίζουν, το κάθε ένα στην επικράτειά του, να διεξάγονται οι απαραίτητες επιθεωρήσεις ασφαλείας και ότι τηρείται η παρούσα Συμφωνία.

(8) Τα Άρθρα 5 και 6 της παρούσας Συμφωνίας δεν εφαρμόζονται για διαβαθμισμένες πληροφορίες επιπέδου «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH».

Άρθρο 5

Ανάθεση Διαβαθμισμένων Συμβάσεων

(1) Πριν από την ανάθεση διαβαθμισμένης σύμβασης, ο αναθέτων φορέας, μέσω της αρμόδιας αρχής του, εξασφαλίζει Εξουσιοδότηση Ασφάλειας Φορέα από την αρμόδια αρχή του αναδόχου, ώστε να διασφαλίσει ότι ο πιθανός ανάδοχος υπόκειται σε έλεγχο ασφαλείας από την αρμόδια αρχή αυτού του Συμβαλλόμενου Μέρους και ότι έχει λάβει τα προβλεπόμενα μέτρα ασφαλείας για την εκτέλεση της σύμβασης. Σε περίπτωση που κάποιος ανάδοχος δεν υπόκειται ακόμα σε έλεγχο ασφαλείας, θα πρέπει να υποβληθεί η σχετική αίτηση.

(2) Θα πρέπει επίσης να εξασφαλιστεί Εξουσιοδότηση Ασφάλειας Φορέα εάν ζητηθεί από κάποια εταιρεία να υποβάλει προσφορά και εάν διαβαθμισμένες πληροφορίες πρέπει να δημοσιοποιηθούν πριν από την ανάθεση της σύμβασης στο πλαίσιο της διαδικασίας προσφορών.

(3) Στις περιπτώσεις που αναφέρονται στις ανωτέρω παραγράφους (1) και (2), εφαρμόζεται η ακόλουθη διαδικασία:

1. Οι αιτήσεις για την έκδοση Εξουσιοδότησης Ασφάλειας Φορέα για ανάδοχους από το κράτος του άλλου Συμβαλλόμενου Μέρους, θα περιλαμβάνουν πληροφορίες για το έργο, καθώς και για τη φύση, το εύρος και το επίπεδο ασφαλείας διαβάθμισης των διαβαθμισμένων πληροφοριών που πρόκειται να γνωστοποιηθούν στον ανάδοχο ή να παραχθούν από αυτόν.
2. Εκτός από την πλήρη επωνυμία της εταιρίας, την ταχυδρομική της διεύθυνση, το όνομα του εξουσιοδοτημένου υπεύθυνου ασφαλείας της, το τηλέφωνο, το φαξ και την ηλεκτρονική διεύθυνση του, οι Εξουσιοδοτήσεις Ασφάλειας Φορέα θα πρέπει να περιλαμβάνουν και πληροφορίες σχετικά με τον βαθμό και το επίπεδο διαβάθμισης στο οποίο έχουν ληφθεί μέτρα ασφαλείας από τη συγκεκριμένη εταιρία βάσει των εθνικών κανονισμών ασφαλείας.
3. Οι αρμόδιες αρχές των Συμβαλλομένων Μερών θα αλληλοενημερώνονται για τυχόν αλλαγές στα στοιχεία στα οποία βασίζονται οι εκδοθείσες

Εξουσιοδοτήσεις Ασφάλειας Φορέα.

4. Η ανταλλαγή τέτοιων πληροφοριών μεταξύ των αρμοδίων αρχών των Συμβαλλομένων Μερών θα γίνεται είτε στην επίσημη γλώσσα της αρμόδιας αρχής που πρόκειται να λάβει την ενημέρωση, είτε στην αγγλική γλώσσα.
5. Οι Εξουσιοδοτήσεις Ασφάλειας Φορέα και οι αιτήσεις που απευθύνονται στις αντίστοιχες αρμόδιες αρχές των Συμβαλλομένων Μερών για την έκδοση εξουσιοδοτήσεων ασφάλειας φορέα, θα διαβιβάζονται εγγράφως.

Άρθρο 6

Εκτέλεση Διαβαθμισμένων Συμβάσεων

(1) Οι διαβαθμισμένες συμβάσεις πρέπει να περιέχουν ρήτρα απαίτησης ασφαλείας βάσει της οποίας ο ανάδοχος υποχρεούται να λάβει όλα τα μέτρα που απαιτούνται για την προστασία διαβαθμισμένων πληροφοριών σύμφωνα με τους εθνικούς κανονισμούς ασφαλείας του κράτους του.

(2) Επιπλέον, η ρήτρα απαίτησης ασφαλείας θα περιέχει και τις ακόλουθες διατάξεις:

1. τον ορισμό του όρου «διαβαθμισμένες πληροφορίες» και των αντίστοιχων επιπέδων προστατευτικής επισήμανσης και διαβάθμισης ασφαλείας των δύο Συμβαλλομένων Μερών σύμφωνα με τις διατάξεις της παρούσας Συμφωνίας.
2. τα ονόματα της αρμόδιας αρχής των Συμβαλλομένων Μερών, η οποία είναι εξουσιοδοτημένη να επιτρέπει τη γνωστοποίηση και να συντονίζει τη διαφύλαξη των διαβαθμισμένων πληροφοριών που αφορούν στην εν λόγω σύμβαση.
3. τις οδούς που πρόκειται να χρησιμοποιηθούν για τη διαβίβαση διαβαθμισμένων πληροφοριών μεταξύ των αρμοδίων αρχών και των εμπλεκόμενων ιναδόχων.

4. τις διαδικασίες και τους μηχανισμούς για τη γνωστοποίηση αλλαγών, οι οποίες ενδέχεται να προκύψουν σε σχέση με διαβαθμισμένες πληροφορίες είτε λόγω αλλαγών στις προστατευτικές τους επισημάνσεις, είτε επειδή η προστασία δεν είναι πλέον απαραίτητη,
5. τις διαδικασίες για την έγκριση επισκέψεων ή την πρόσβαση του προσωπικού των ανάδοχων,
6. τις διαδικασίες για τη διαβίβαση διαβαθμισμένων πληροφοριών σε ανάδοχους, οι οποίοι πρόκειται να χρησιμοποιήσουν ή να φυλάξουν τις πληροφορίες αυτές.
7. την απαίτηση ότι ο ανάδοχος θα παρέχει πρόσβαση σε διαβαθμισμένες πληροφορίες μόνο σε πρόσωπο, το οποίο έχει ανάγκη για γνώση και στο οποίο έχει ανατεθεί η εκτέλεση της σύμβασης ή συμμετέχει σε αυτήν και – εκτός στην περίπτωση διαβαθμισμένων πληροφοριών επιπέδου ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /VS-NUR FÜR DEN DIENSTGEBRAUCH– έχει υποβληθεί εκ των προτέρων σε έλεγχο ασφάλειας προσωπικού στο κατάλληλο επίπεδο,
8. την απαίτηση ότι οι διαβαθμισμένες πληροφορίες θα αποκαλύπτονται σε τρίτους ή ότι η διαβίβασή τους σε τρίτους θα επιτρέπεται μόνο εφόσον αυτό εγκριθεί από το αντισυμβαλλόμενο μέρος-πάροχο,
9. την απαίτηση ότι ο ανάδοχος θα ειδοποιεί αμέσως την οικεία αρμόδια αρχή για κάθε πραγματική απώλεια, ή διαρροή ή υπόνοια απώλειας ή διαρροής, ή μη εξουσιοδοτημένη αποκάλυψη των διαβαθμισμένων πληροφοριών που καλύπτονται από τη σύμβαση,
10. την υποχρέωση του ανάδοχου να ενημερώνει την οικεία Αρμόδια Αρχή Ασφαλείας για την ανάληψη εκτέλεσης μιας διαβαθμισμένης σύμβασης,
11. την υποχρέωση του υπεργολάβου να πληροί τις ίδιες υποχρεώσεις ασφαλείας με τον ανάδοχο.

(3) Η αρμόδια για τον αναθέτοντα φορέα αρχή κατονομάζει στον ανάδοχο σε μια ξεχωριστή κατάσταση (κατάλογο διαβάθμισης) όλα τα αρχεία εγγράφων που απαιτούν διαβάθμιση ασφάλειας, καθορίζει το απαιτούμενο επίπεδο διαβάθμισης και φροντίζει ώστε ο κατάλογος αυτός να επισυνάπτεται ως παράρτημα στη διαβαθμισμένη σύμβαση. Η αρμόδια για τον αναθέτοντα φορέα αρχή διαβιβάζει τον κατάλογο αυτό στην αρμόδια αρχή του ανάδοχου ή φροντίζει για τη διαβίβασή του σε αυτήν.

(4) Η αρμόδια για τον αναθέτοντα φορέα αρχή διασφαλίζει ότι ο ανάδοχος θα έχει πρόσβαση σε διαβαθμισμένες πληροφορίες μόνο εφόσον περιέλθει σε αυτήν η Εξουσιοδότηση Ασφάλειας Φορέα από την αρμόδια αρχή του ανάδοχου.

Άρθρο 7

Διαβίβαση Διαβαθμισμένων Πληροφοριών

(1) Επί της αρχής, οι διαβαθμισμένες πληροφορίες επιπέδου «ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH» και «ΑΠΟΡΡΗΤΟ/GEHEIM» διαβιβάζονται από τη μία χώρα στην άλλη με επίσημο υπηρεσιακό ταχυδρομείο σύμφωνα με τους εθνικούς νόμους και κανονισμούς. Οι Εθνικές Αρχές Ασφαλείας ή αντίστοιχα οι καθορισθείσες Αρχές Ασφαλείας των Συμβαλλομένων Μερών δύνανται να συμφωνήσουν εναλλακτικές οδούς διαβίβασης. Η λήψη διαβαθμισμένων πληροφοριών επιβεβαιώνεται από ή εκ μέρους της αρμόδιας αρχής και οι διαβαθμισμένες πληροφορίες θα προωθούνται στον παραλήπτη σύμφωνα με την εθνική νομοθεσία περί ασφαλείας.

(2) Οι αρμόδιες αρχές μπορούν για ένα επακριβώς χαρακτηρισμένο εγχείρημα, να συμφωνήσουν – γενικά ή θεσπίζοντας περιορισμούς – ότι οι διαβαθμισμένες πληροφορίες επιπέδου «ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH» και «ΑΠΟΡΡΗΤΟ/GEHEIM» μπορούν να διαβιβάζονται μέσω μιας άλλης οδού αντί του επίσημου υπηρεσιακού ταχυδρομείου, εφόσον η τήρηση του επίσημου ταχυδρομείου θα δυσχέραινε δυσανάλογα τη μεταφορά ή την εκτέλεση μιας σύμβασης. Στις περιπτώσεις αυτές:

1. ο κοιμιστής πρέπει να είναι εξουσιοδοτημένος με την πρόσβαση σε πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης ασφάλειας,

2. ο φορέας αποστολής οφείλει να διατηρεί κατάλογο με τις διαβαθμισμένες πληροφορίες που έχει διαβιβάσει. Αντίγραφο της κατάστασης αυτής θα παραδίδεται στον παραλήπτη για να τον προωθήσει στην αρμόδια αρχή.
3. οι διαβαθμισμένες πληροφορίες συσκευάζονται σύμφωνα με τους κανονισμούς που διέπουν τη μεταφορά εντός των εθνικών συνόρων,
4. οι διαβαθμισμένες πληροφορίες παραδίδονται έναντι απόδειξης παραλαβής,
5. ο κομιστής πρέπει να έχει ένα πιστοποιητικό ταχυδρομείου το οποίο εκδίδεται από την αρμόδια αρχή του φορέα αποστολής ή παραλαβής.

(3) Όταν πρόκειται να διαβιβαστούν μεγάλοι όγκοι διαβαθμισμένων πληροφοριών, τα μέσα διαβίβασης, η οδός και η συνοδεία θα καθορίζονται ανάλογα με την περίπτωση και βάσει λεπτομερούς σχεδίου μεταφοράς από τις αρμόδιες αρχές.

(4) Η ηλεκτρονική διαβίβαση διαβαθμισμένων πληροφοριών επιπέδου «ΕΜΠΙΣΤΕΥΤΙΚΟ/ VS-VERTRAULICH» και άνω δεν πρέπει να γίνεται χωρίς κρυπτογράφηση. Οι διαβαθμισμένες πληροφορίες αυτού του επιπέδου διαβάθμισης, πρέπει να κρυπτογραφούνται με κρυπτογραφικά μέσα, τα οποία έχουν εγκριθεί με αμοιβαία συμφωνία των αρμοδίων αρχών ασφαλείας των Συμβαλλομένων Μερών.

(5) Οι διαβαθμισμένες πληροφορίες επιπέδου «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ VS-NUR FÜR DEN DIENSTGEBRAUCH» διαβιβάζονται σύμφωνα με τους εθνικούς νόμους και κανονισμούς.

(6) Οι διαβαθμισμένες πληροφορίες επιπέδου «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/ VS-NUR FÜR DEN DIENSTGEBRAUCH» δύνανται να διαβιβάζονται ηλεκτρονικά ή να διατίθενται με εμπορικές συσκευές κρυπτογράφησης εγκεκριμένες από την αρμόδια αρχή ασφαλείας των Συμβαλλομένων Μερών. Οι διαβαθμισμένες πληροφορίες αυτού του επιπέδου διαβάθμισης δύνανται να διαβιβάζονται χωρίς κρυπτογράφηση μόνο εφόσον αυτό δεν αντιβαίνει τους εθνικούς κανονισμούς ασφαλείας, εφόσον δεν διατίθενται εγκεκριμένα μέσα κρυπτογράφησης, εφόσον η διαβίβαση γίνεται αποκλειστικά εντός συγκεκριμένων σταθερών δικτύων και εφόσον ο αποστολέας και ο παραλήπτης έχουν συμφωνήσει εκ των προτέρων για τον

επικείμενο τρόπο διαβίβασης.

Άρθρο 8 Επισκέψεις

(1) Επί της αρχής, οι επισκέπτες από την επικράτεια του ενός Συμβαλλόμενου Μέρους θα εξασφαλίζουν πρόσβαση σε διαβαθμισμένες πληροφορίες και σε εγκαταστάσεις φύλαξης διαβαθμισμένων πληροφοριών μόνο με την εκ των προτέρων άδεια της αρμόδιας αρχής του Συμβαλλόμενου Μέρους της χώρας υποδοχής. Η εν λόγω άδεια παρέχεται μόνο σε πρόσωπα που πληρούν την προϋπόθεση της ανάγκης για γνώση και είναι - εκτός σε περίπτωση διαβαθμισμένων πληροφοριών «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH»-, που είναι εξουσιοδοτημένα να έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες.

(2) Οι αιτήσεις επισκέψεων θα πρέπει να υποβάλλονται στην αρμόδια αρχή του άλλου Συμβαλλόμενου Μέρους εγκαίρως και σύμφωνα με τους κανονισμούς αυτού του Συμβαλλόμενου Μέρους, στη επικράτεια του οποίου επιθυμεί να ταξιδέψει ο επισκέπτης. Οι αρμόδιες αρχές οφείλουν να ενημερώνουν η μία την άλλη για τις λεπτομέρειες των αιτήσεων επίσκεψης και να διασφαλίζουν την προστασία των προσωπικών δεδομένων.

(3) Οι αιτήσεις επισκέψεων υποβάλλονται στη γλώσσα της χώρας υποδοχής ή στην αγγλική γλώσσα και περιέχουν τις ακόλουθες πληροφορίες:

1. το ονοματεπώνυμο, τον τόπο και ημερομηνία γέννησης και τον αριθμό διαβατηρίου ή ταυτότητας του επισκέπτη,
2. την υπηκοότητα του επισκέπτη,
3. την ιδιότητα του επισκέπτη και την επωνυμία της αρχής ή του φορέα, τον οποίο εκπροσωπεί,
4. το επίπεδο εξουσιοδότησης ασφαλείας του επισκέπτη για πρόσβαση σε διαβαθμισμένες πληροφορίες,
5. τον σκοπό και την προτεινόμενη ημερομηνία επίσκεψης,

6. τους φορείς, τους υπεύθυνους επικοινωνίας και τις εγκαταστάσεις, που επιθυμεί να επισκεφτεί ο αιτών.

Άρθρο 9

Διαβουλεύσεις και Επίλυση Διαφορών

(1) Οι αρμόδιες αρχές των Συμβαλλομένων Μερών λαμβάνουν υπόψη τους τις διατάξεις που διέπουν την προστασία διαβαθμισμένων πληροφοριών, οι οποίες ισχύουν στην επικράτεια του άλλου Συμβαλλόμενου Μέρους.

(2) Για τη διασφάλιση της στενής συνεργασίας στην εφαρμογή της παρούσας Συμφωνίας, οι αρμόδιες αρχές θα διεξάγουν μεταξύ τους διαβουλεύσεις κατόπιν αιτήματος της μίας εκ των δύο αρμοδίων αρχών.

(3) Επιπλέον, κάθε Συμβαλλόμενο Μέρος θα επιτρέπει στην Εθνική ή Καθορισθείσα Αρχή Ασφαλείας του άλλου Συμβαλλόμενου Μέρους ή σε οποιαδήποτε άλλη αρχή καθοριστεί με αμοιβαία συμφωνία, να επισκεφτεί την επικράτειά του για να εξετάσει με τις αρχές ασφαλείας του, τις διαδικασίες και τους μηχανισμούς προστασίας των διαβαθμισμένων πληροφοριών που διατίθενται από το άλλο Συμβαλλόμενο Μέρος. Κάθε Συμβαλλόμενο Μέρος θα βοηθά την αρχή αυτή ώστε να διαπιστώσει εάν οι εν λόγω διαβαθμισμένες πληροφορίες, οι οποίες διατίθενται από το άλλο Συμβαλλόμενο Μέρος, τυχάνουν της κατάλληλης προστασίας. Οι λεπτομέρειες των επισκέψεων αυτών καθορίζονται από τις αρμόδιες αρχές σύμφωνα με τις διατάξεις του Άρθρου 8 της παρούσας Συμφωνίας.

(4) Τυχόν διαφορές μεταξύ των Συμβαλλομένων Μερών, οι οποίες προκύπτουν από την ερμηνεία ή την εφαρμογή της παρούσας Συμφωνίας θα επιλύονται αποκλειστικά μέσω διαβουλεύσεων ή διαπραγματεύσεων μεταξύ των Συμβαλλομένων Μερών και δεν θα παραπέμπονται σε εθνικά ή διεθνή δικαστήρια ή σε τρίτους προς επίλυση.

Άρθρο 10
Παραβίαση των Διατάξεων για
την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών

(1) Σε περίπτωση που η μη εξουσιοδοτημένη αποκάλυψη διαβαθμισμένων πληροφοριών δεν δύναται να αποκλειστεί, υπάρχει υπόνοια ότι συνέβη, ή ακόμα επιβεβαιωθεί, το άλλο Συμβαλλόμενο Μέρος πρέπει αμέσως να ειδοποιηθεί.

(2) Η παραβίαση των διατάξεων που διέπουν την προστασία διαβαθμισμένων πληροφοριών θα ερευνάται και θα λαμβάνονται τα κατάλληλα νομικά μέτρα από τις αρμόδιες αρχές και/ή τα δικαστήρια του Συμβαλλόμενου Μέρους, τα οποία έχουν την αντίστοιχη αρμοδιότητα, σύμφωνα με τη νομοθεσία του Συμβαλλόμενου Μέρους. Το άλλο Συμβαλλόμενο Μέρος οφείλει, εάν του ζητηθεί, να υποστηρίξει την εν λόγω έρευνα και πρέπει να ενημερωθεί για το αποτέλεσμα αυτής.

Άρθρο 11
Έξοδα

Κάθε Συμβαλλόμενο Μέρος αναλαμβάνει τα έξοδα που θα προκύψουν από πλευράς του, για την εφαρμογή των διατάξεων της παρούσας Συμφωνίας.

Άρθρο 12
Αρμόδιες Αρχές

Τα Συμβαλλόμενα Μέρη οφείλουν να αλληλοενημερώνονται για τις αρχές οι οποίες είναι υπεύθυνες για την εφαρμογή της παρούσας Συμφωνίας.

Άρθρο 13
Σχέσεις με άλλες Συμφωνίες, Μνημόνια Συναντίληψης και Διευθετήσεις

Τυχόν υφιστάμενες συμφωνίες, μνημόνια συναντίληψης και διευθετήσεις μεταξύ των Συμβαλλομένων Μερών ή των αρμοδίων αρχών για την προστασία διαβαθμισμένων πληροφοριών δεν επηρεάζονται από την παρούσα Συμφωνία στο βαθμό που δεν

αντιβαίνουν στις διατάξεις της.

Άρθρο 14 Τελικές Διατάξεις

(1) Η παρούσα Συμφωνία θα τεθεί σε ισχύ την ημερομηνία κατά την οποία η Κυβέρνηση της Κυπριακής Δημοκρατίας θα ειδοποιήσει την Κυβέρνηση της Ομοσπονδιακής Δημοκρατίας της Γερμανίας ότι έχουν εκπληρωθεί όλες οι αναγκαίες εθνικές νομικές προϋποθέσεις που απαιτούνται για την έναρξη ισχύος της παρούσας Συμφωνίας. Η εν λόγω ημερομηνία θα είναι η ημερομηνία παραλαβής της ειδοποίησης.

(2) Η Συμφωνία αυτή συνάπτεται για αόριστο χρονικό διάστημα.

(3) Η Συμφωνία αυτή δύναται να τροποποιείται γραπτώς με αμοιβαία συμφωνία μεταξύ των Συμβαλλομένων Μερών. Κάθε Συμβαλλόμενο Μέρος δύναται οποιαδήποτε στιγμή να υποβάλει γραπτό αίτημα για την τροποποίηση της παρούσας Συμφωνίας. Εάν υποβληθεί το εν λόγω αίτημα από το ένα εκ των δύο Συμβαλλομένων Μερών, τα Συμβαλλόμενα Μέρη θα ξεκινήσουν διαπραγματεύσεις για την τροποποίηση της Συμφωνίας.

(4) Κάθε Συμβαλλόμενο Μέρος δύναται, μέσω της διπλωματικής οδού, να καταγγείλει την παρούσα Συμφωνία με γραπτή εξάμηνη ειδοποίηση. Σε περίπτωση καταγγελίας, οι διαβαθμισμένες πληροφορίες που διαβιβάστηκαν ή παράχθηκαν από τον ανάδοχο βάσει της παρούσας Συμφωνίας, θα εξακολουθήσουν να τυγχάνουν χειρισμού σύμφωνα με τις διατάξεις του Άρθρου 4 για όσο διάστημα δικαιολογείται από την ύπαρξη της διαβάθμισης.

(5) Την καταχώρηση της παρούσας Συμφωνίας στη Γραμματεία των Ηνωμένων Εθνών, σύμφωνα με το Άρθρο 102 του Καταστατικού Χάρτη των Ηνωμένων Εθνών, αναλαμβάνει να διεκπεραιώσει το Συμβαλλόμενο Μέρος στην εθνική επικράτεια του οποίου υπεγράφη η παρούσα Συμφωνία αμέσως αφότου αυτή τεθεί σε ισχύ. Το άλλο Συμβαλλόμενο Μέρος ενημερώνεται για την καταχώρηση και τον αριθμό αυτής, μόλις επιβεβαιωθεί η καταχώρηση από τη Γραμματεία των Ηνωμένων Εθνών.

Συντάχθηκε στην.....Μάγδα....., στις ..27..Απρ..2017, σε δύο πρωτότυπα, στη ελληνική, γερμανική και αγγλική γλώσσα και όλα τα κείμενα είναι αυθεντικά. Σε περίπτωση διαφορετικής ερμηνείας του ελληνικού και του γερμανικού κειμένου, το αγγλικό κείμενο υπερισχύει.

Για την Κυβέρνηση της
Κυπριακής Δημοκρατίας



Για την Κυβέρνηση της Ομοσπονδιακής
Δημοκρατίας της Γερμανίας

.....Lübbig.....
Annela e. Qj

Μέρος II
(Γερμανική Γλώσσα)

Abkommen

zwischen

der Regierung der Republik Zypern

und

der Regierung der Bundesrepublik Deutschland

über

den gegenseitigen Schutz von Verschlusssachen

Die Regierung der Republik Zypern
und
die Regierung der Bundesrepublik Deutschland
(im Folgenden als „Vertragsparteien“ bezeichnet) –

in der Absicht, den Schutz von Verschlusssachen zu gewährleisten, die zwischen den zuständigen Behörden der Republik Zypern und der Bundesrepublik Deutschland sowie mit Auftragnehmern im Hoheitsgebiet der anderen Vertragspartei oder zwischen Auftragnehmern beider Vertragsparteien ausgetauscht werden,

von dem Wunsch geleitet, eine Regelung über den gegenseitigen Schutz von Verschlusssachen zu schaffen, die auf alle zwischen den Vertragsparteien zu schließenden Abkommen über Zusammenarbeit und auf Verträge, die einen Austausch von Verschlusssachen mit sich bringen, Anwendung findet –

sind wie folgt übereingekommen:

Artikel 1
Begriffsbestimmungen

(1) Im Sinne dieses Abkommens

1. sind „Verschlusssachen“

- a) in der Bundesrepublik Deutschland:
im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform. Sie werden ent-

sprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft;

b) in der Republik Zypern:

jegliche Informationen oder Materialien, unabhängig von ihrer Form oder Art, die gegen unbefugte Bekanntgabe und/oder Nutzung zu schützen sind und im Einklang mit den innerstaatlichen Rechtsvorschriften eingestuft wurden;

2. ist ein „Verschlussachenauftrag“ ein Vertrag zwischen einer Behörde oder einem Unternehmen aus dem Staat der einen Vertragspartei (Auftraggeber) und einem Unternehmen aus dem Staat der anderen Vertragspartei (Auftragnehmer); im Rahmen eines derartigen Vertrags sind Verschlussachen aus dem Staat des Auftraggebers dem Auftragnehmer zu überlassen, von dem Auftragnehmer zu erstellen oder ordnungsgemäß bevollmächtigten Mitarbeitern des Auftragnehmers, die Arbeiten in Einrichtungen des Auftraggebers durchzuführen haben, zugänglich zu machen;
3. bezeichnet „Zuständige Sicherheitsbehörde“ die Sicherheitsbehörde oder -behörden jeder Vertragspartei, die für die Durchführung und Überwachung dieses Abkommens verantwortlich ist beziehungsweise sind;
4. bezeichnet „Auftragnehmer“ eine natürliche oder juristische Person mit der für den Abschluss von Verschlussachenaufträgen notwendigen Geschäftsfähigkeit;
5. bezeichnet „Sicherheitsbescheid“ die Bescheinigung der Zuständigen Sicherheitsbehörde, die bestätigt, dass die natürliche oder juristische Person die persönlichen Sicherheitsanforderungen erfüllt und über die physischen und organisatorischen Kapazitäten verfügt, Verschlussachen im Einklang mit den jeweiligen innerstaatlichen Rechtsvorschriften zu verwenden, zu verwahren und zu schützen;

6. bedeutet „Kenntnis nur, wenn nötig“ das Erfordernis, im Rahmen einer übertragenen Aufgabe oder Tätigkeit Zugang zu Verschlusssachen zu erhalten;
7. bezeichnet „Sicherheitsüberprüfungsbescheinigung“ die Bescheinigung der zuständigen Sicherheitsbehörde, die im Einklang mit den jeweiligen innerstaatlichen Rechtsvorschriften bestätigt, dass eine Einzelperson geeignet ist, Zugang zu Verschlusssachen bestimmter Geheimhaltungsgrade zu erhalten;
8. bezeichnet „Dritte“ Staaten, Organisationen, juristische oder natürliche Personen, die nicht Vertragspartei dieses Abkommens sind.

(2) Für die Geheimhaltungsgrade gelten die folgenden Begriffsbestimmungen:

1. In der Bundesrepublik Deutschland sind Verschlusssachen
 - a) STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann;
 - b) GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann;
 - c) VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann;
 - d) VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann;

2. in der Republik Zypern sind Verschlussachen
- a) ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ: Informationen und Materialien, deren unbefugte Bekanntgabe zu einer besonders schweren Beeinträchtigung der wesentlichen Interessen der Republik Zypern führen könnte;
 - b) ΑΠΟΡΡΗΤΟ: Informationen und Materialien, deren unbefugte Bekanntgabe den wesentlichen Interessen der Republik Zypern ernsthaft schaden könnte;
 - c) ΕΜΠΙΣΤΕΥΤΙΚΟ: Informationen und Materialien, deren unbefugte Bekanntgabe den wesentlichen Interessen der Republik Zypern schaden könnte;
 - d) ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ: Informationen und Materialien, deren unbefugte Bekanntgabe sich nachteilig auf die Interessen der Republik Zypern auswirken könnte.

Artikel 2

Tabelle der Entsprechungen

Die Vertragsparteien legen fest, dass folgende Geheimhaltungsgrade einander entsprechen:

Für die Republik Zypern	Für die Bundesrepublik Deutschland	Entsprechung auf Englisch
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STRENG GEHEIM	TOP SECRET
ΑΠΟΡΡΗΤΟ	GEHEIM	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	VS-VERTRAULICH	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTRICTED

Artikel 3

Kennzeichnung mit Geheimhaltungsgraden

(1) Ausgetauschte Verschlussachen sind mit einer Kennzeichnung des Geheimhaltungsgrads zu versehen, die dem in Einklang mit den innerstaatlichen Rechtsvorschriften der Vertragsparteien von den zuständigen Behörden oder in ihrem Namen festgelegten, und nach Artikel 2 vergleichbaren Geheimhaltungsgrad entspricht. Die empfangende Vertragspartei kennzeichnet die ausgetauschten Verschlussachen entsprechend.

(2) Die Kennzeichnungspflicht gilt auch für Verschlussachen, die von der empfangenden Vertragspartei im Zusammenhang mit Verschlussachenaufträgen entstehen, und für von der empfangenden Vertragspartei hergestellte Kopien.

(3) Geheimhaltungsgrade werden von der für den Empfänger der betreffenden Verschlussache zuständigen Behörde oder in deren Namen auf Ersuchen der zuständigen Behörde der herausgebenden Vertragspartei geändert oder aufgehoben. Die zuständige Behörde der herausgebenden Vertragspartei teilt der zuständigen Behörde der empfangenden Vertragspartei Änderungen oder Aufhebungen eines Geheimhaltungsgrads unverzüglich mit.

Artikel 4

Innerstaatliche Maßnahmen

(1) Die Vertragsparteien treffen im Rahmen ihrer innerstaatlichen Rechtsvorschriften alle geeigneten Maßnahmen, um den Geheimschutz von Verschlussachen zu gewährleisten, die nach diesem Abkommen entstehen, ausgetauscht oder aufbewahrt werden. Sie gewähren diesen Verschlussachen mindestens den gleichen Geheimschutz, wie er für eigene Verschlussachen des entsprechenden Geheimhaltungsgrads gefordert wird.

(2) Die Verschlussachen werden ausschließlich für den angegebenen Zweck verwendet. Die empfangende Vertragspartei darf Verschlussachen weder bekannt geben oder nutzen noch ihre Bekanntgabe oder Nutzung gestatten, es sei denn, dies geschieht für die Zwecke und mit den etwaigen Beschränkungen, die von oder im Auftrag der herausgebenden Vertragspartei festgelegt worden sind. Einer gegenteiligen Regelung muss der Herausgeber der Verschlussache schriftlich zugestimmt haben.

(3) Die Verschlussachen dürfen nur Personen zugänglich gemacht werden, die auf Grund ihrer Aufgaben die Bedingung „Kenntnis nur, wenn nötig“ erfüllen und die – außer im Fall von „ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuftem Verschlussachen – zum Zugang zu Verschlussachen des entsprechenden Geheimhaltungsgrads ermächtigt sind. Eine Ermächtigung setzt eine Sicherheitsüberprüfung voraus, die mindestens so streng sein muss wie diejenige, die für den Zugang zu innerstaatlichen Verschlussachen des entsprechenden Geheimhaltungsgrads durchgeführt wird.

(4) Der Zugang zu Verschlussachen des Geheimhaltungsgrads „ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH“ und höher durch eine Person mit der Staatsangehörigkeit einer Vertragspartei wird ohne vorherige Genehmigung der herausgebenden Vertragspartei gewährt.

(5) Sicherheitsüberprüfungen bei Staatsangehörigen der Vertragspartei, die ihren Aufenthalt im eigenen Land haben und dort Zugang zu Verschlussachen benötigen, werden von deren Nationalen Sicherheitsbehörden beziehungsweise beauftragten Sicherheitsbehörden oder anderen zuständigen innerstaatlichen Behörden vorgenommen.

(6) Sicherheitsüberprüfungen bei Staatsangehörigen einer Vertragspartei, die ihren rechtmäßigen Aufenthalt im Land der anderen Vertragspartei haben und sich dort um eine Tätigkeit bewerben, die Zugang zu Verschlussachen des Geheimhaltungsgrads „ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH“ und höher erfordert, werden hingegen von der Zuständigen Sicherheitsbehörde dieses Staates durchgeführt, wobei gegebenenfalls Sicherheitsauskünfte im Ausland eingeholt werden.

(7) Die Vertragsparteien sorgen innerhalb ihres Hoheitsgebiets für die Durchführung der erforderlichen Sicherheitsinspektionen und für die Einhaltung dieses Abkommens.

(8) Für Verschlussachen des Geheimhaltungsgrads „ΠΕΠΙΟΠΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH“ finden Artikel 5 und 6 dieses Abkommens keine Anwendung.

Artikel 5

Vergabe von Verschlussachenaufträgen

(1) Vor Vergabe eines Verschlussachenauftrags holt der Auftraggeber über die für ihn zuständige Behörde bei der für den Auftragnehmer zuständigen Behörde einen Sicherheitsbescheid ein, um sich vergewissern zu können, ob der in Aussicht genommene Auftragnehmer der Geheimschutzaufsicht durch die zuständige Behörde dieser Vertragspartei unterliegt und ob er die für die Auftragsdurchführung erforderlichen Geheimschutzvorkehrungen getroffen hat. Ist ein Auftragnehmer noch nicht in der Geheimschutzbetreuung, kann dies beantragt werden.

(2) Ein Sicherheitsbescheid ist auch dann einzuholen, wenn ein Unternehmen zur Abgabe eines Angebots aufgefordert worden ist und im Rahmen des Ausschreibungsverfahrens bereits vor Auftragserteilung Verschlussachen übergeben werden müssen.

(3) In den Fällen der Absätze 1 und 2 wird das folgende Verfahren angewendet:

1. Ersuchen um Ausstellung eines Sicherheitsbescheids für Auftragnehmer aus dem Staat der anderen Vertragspartei enthalten Angaben über das Vorhaben sowie die Art, den Umfang und den Geheimhaltungsgrad der dem Auftragnehmer voraussichtlich zu überlassenden oder bei ihm entstehenden Verschlussachen.

2. Sicherheitsbescheide müssen neben der vollständigen Bezeichnung des Unternehmens, seiner Postanschrift und dem Namen des Sicherheitsbevollmächtigten sowie dessen Telefon- und Faxverbindung und E-Mail-Adresse insbesondere Angaben darüber erhalten, in welchem Umfang und bis zu welchem Geheimhaltungsgrad bei dem betreffenden Unternehmen Geheimschutzmaßnahmen auf der Grundlage innerstaatlicher Geheimschutzvorschriften getroffen worden sind.
3. Die zuständigen Behörden der Vertragsparteien teilen es einander mit, wenn sich die den ausgestellten Sicherheitsbescheiden zugrunde liegenden Sachverhalte ändern.
4. Der Austausch dieser Mitteilungen zwischen den zuständigen Behörden der Vertragsparteien erfolgt in der Landessprache der zu unterrichtenden Behörde oder in englischer Sprache.
5. Sicherheitsbescheide und an die jeweils zuständigen Behörden der Vertragsparteien gerichtete Ersuchen um Ausstellung von Sicherheitsbescheiden sind in Schriftform zu übermitteln.

Artikel 6

Durchführung von Verschlusssachenaufträgen

- (1) Verschlusssachenaufträge müssen eine Geheimschutzklausel enthalten, der zufolge der Auftragnehmer verpflichtet ist, die zum Schutz von Verschlusssachen erforderlichen Vorkehrungen in Übereinstimmung mit den innerstaatlichen Geheimschutzvorschriften seines Landes zu treffen.

(2) Außerdem sind folgende Bestimmungen in die Geheimschutzklausel aufzunehmen:

1. die Bestimmung des Begriffs „Verschlussachen“ und der entsprechenden Geheimschutzkennzeichnungen und Geheimhaltungsgrade der beiden Vertragsparteien in Übereinstimmung mit diesem Abkommen;
2. die Namen der jeweils zuständigen Behörde der Vertragsparteien, die zur Genehmigung der Überlassung von Verschlussachen, die mit dem Auftrag in Zusammenhang stehen, und zur Koordinierung des Schutzes dieser Verschlussachen ermächtigt sind;
3. die Wege, über die Verschlussachen zwischen den zuständigen Behörden und beteiligten Auftragnehmern weiterzugeben sind;
4. die Verfahren und Mechanismen für die Mitteilung von Änderungen, die sich möglicherweise in Bezug auf Verschlussachen aufgrund von Änderungen ihrer Geheimschutzkennzeichnungen oder wegen des Wegfalls der Schutzbedürftigkeit ergeben;
5. die Verfahren für die Genehmigung von Besuchen oder des Zugangs von Personal der Auftragnehmer;
6. die Verfahren für die Übermittlung von Verschlussachen an Auftragnehmer, bei denen solche Verschlussachen verwendet und aufbewahrt werden sollen;
7. die Forderung, dass der Auftragnehmer den Zugang zu einer Verschlussache nur einer Person gewähren darf, welche die Bedingung „Kenntnis nur, wenn nötig“ erfüllt und mit der Durchführung des Auftrags beauftragt worden oder daran beteiligt ist und – außer im Fall von als „ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlussachen – zuvor bis zum entsprechenden Geheimhaltungsgrad sicherheitsüberprüft worden ist;

8. die Forderung, dass eine Verschlussache nur an Dritte weitergegeben beziehungsweise deren Weitergabe an Dritte nur gestattet werden darf, wenn die herausgebende Vertragspartei dem zugestimmt hat;
 9. die Forderung, dass der Auftragnehmer seine zuständige Behörde unverzüglich über jeden erfolgten oder vermuteten Verlust, eine begangene oder vermutete Indiskretion oder unbefugte Bekanntgabe der unter den Auftrag fallenden Verschlussachen zu unterrichten hat;
 10. die Verpflichtung des Auftragnehmers, seine eigene Zuständige Sicherheitsbehörde vom Erhalt eines Verschlussachenauftrags zu unterrichten;
 11. die Verpflichtung des Unterauftragnehmers, den gleichen Sicherheitserfordernissen zu genügen wie der Auftragnehmer.
- (3) Die für den Auftraggeber zuständige Behörde benennt dem Auftragnehmer in einer gesonderten Aufstellung (Einstufungsliste) sämtliche Vorgänge, die einer Verschlussacheneinstufung bedürfen, legt den erforderlichen Geheimhaltungsgrad fest und veranlasst, dass diese Aufstellung dem Verschlussachenauftrag als Anhang beigelegt wird. Die für den Auftraggeber zuständige Behörde hat diese Aufstellung auch der für den Auftragnehmer zuständigen Behörde zu übermitteln oder deren Übermittlung zu veranlassen.
- (4) Die für den Auftraggeber zuständige Behörde stellt sicher, dass dem Auftragnehmer Verschlussachen erst dann zugänglich gemacht werden, wenn der entsprechende Sicherheitsbescheid der für den Auftragnehmer zuständigen Behörde vorliegt.

Artikel 7

Übermittlung von Verschlusssachen

(1) Verschlusssachen der Geheimhaltungsgrade „ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH“ und „ΑΠΟΡΡΗΤΟ/GEHEIM“ werden von einem Staat in den anderen grundsätzlich auf amtlichem Kurierweg im Einklang mit den innerstaatlichen Gesetzen und sonstigen Vorschriften befördert. Die Nationalen Sicherheitsbehörden beziehungsweise die beauftragten Sicherheitsbehörden der Vertragsparteien können alternative Übermittlungswege vereinbaren. Der Empfang einer Verschlusssache wird von der zuständigen Behörde oder in deren Namen bestätigt und die Verschlusssachen nach Maßgabe der innerstaatlichen Geheimschutzvorschriften an den Empfänger weitergeleitet.

(2) Die zuständigen Behörden können für ein genau bezeichnetes Vorhaben – allgemein oder unter Festlegung von Beschränkungen – vereinbaren, dass Verschlusssachen der Geheimhaltungsgrade „ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH“ und „ΑΠΟΡΡΗΤΟ/GEHEIM“ auf einem anderen als dem amtlichen Kurierweg befördert werden dürfen, sofern die Einhaltung des amtlichen Kurierwegs den Transport oder die Ausführung eines Auftrags unangemessen erschweren würde. In derartigen Fällen

1. muss der Beförderer zum Zugang zu Verschlusssachen des entsprechenden Geheimhaltungsgrads ermächtigt sein;
2. muss bei der absendenden Stelle ein Verzeichnis der beförderten Verschlusssachen verbleiben; ein Exemplar dieses Verzeichnisses ist dem Empfänger zur Weiterleitung an die zuständige Behörde zu übergeben;
3. müssen die Verschlusssachen nach den für die Inlandsbeförderung geltenden Bestimmungen verpackt sein;
4. muss die Übergabe der Verschlusssachen gegen Empfangsbescheinigung erfolgen;

5. muss der Beförderer einen Kurierausweis mit sich führen, den die für die absendende oder empfangende Stelle zuständige Behörde ausgestellt hat.
- (3) Für die Beförderung von Verschlussachen von erheblichem Umfang werden Transport, Transportweg und Begleitschutz in jedem Einzelfall durch die zuständigen Behörden auf der Grundlage eines detaillierten Transportplans festgelegt.
- (4) Verschlussachen des Geheimhaltungsgrads „ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH“ und höher dürfen auf elektronischem Weg nicht unverschlüsselt übermittelt werden. Für die Verschlüsselung von Verschlussachen dieser Geheimhaltungsgrade dürfen nur Verschlüsselungssysteme eingesetzt werden, die von den Zuständigen Sicherheitsbehörden der Vertragsparteien in gegenseitigem Einvernehmen zugelassen worden sind.
- (5) Verschlussachen des Geheimhaltungsgrads „ΠΕΠΙΟΠΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH“ werden im Einklang mit den innerstaatlichen Gesetzen und sonstigen Vorschriften übermittelt.
- (6) Verschlussachen des Geheimhaltungsgrads „ΠΕΠΙΟΠΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH“ können mittels handelsüblicher Verschlüsselungsgeräte, die von einer zuständigen innerstaatlichen Behörde der Vertragsparteien zugelassen worden sind, elektronisch übertragen oder zugänglich gemacht werden. Eine unverschlüsselte Übermittlung von Verschlussachen dieses Geheimhaltungsgrads ist nur zulässig, wenn innerstaatliche Geheimschutzvorschriften dem nicht entgegenstehen, ein zugelassenes Verschlüsselungssystem nicht verfügbar ist, die Übermittlung ausschließlich innerhalb von Festnetzen erfolgt und Absender und Empfänger sich zuvor über die beabsichtigte Übertragung geeinigt haben.

Artikel 8

Besuche

(1) Besuchern aus dem Hoheitsgebiet einer Vertragspartei wird im Hoheitsgebiet der anderen Vertragspartei Zugang zu Verschlussachen sowie zu Einrichtungen, in denen an diesen gearbeitet wird, grundsätzlich nur mit vorheriger Erlaubnis der zuständigen Behörde der zu besuchenden Vertragspartei gewährt. Sie wird nur Personen erteilt, die die Bedingung „Kenntnis nur, wenn nötig“ erfüllen und – außer im Fall von als „ΠΕΠΙΟΠΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlussachen – zum Zugang zu Verschlussachen ermächtigt sind.

(2) Besuchsanzeigen sind rechtzeitig und in Übereinstimmung mit den Vorschriften der Vertragspartei, in deren Hoheitsgebiet die Besucher einzureisen wünschen, der zuständigen Behörde dieser Vertragspartei vorzulegen. Die zuständigen Behörden teilen einander die Einzelheiten der Anzeigen mit und stellen den Schutz personenbezogener Daten sicher.

(3) Besuchsanzeigen sind in der Sprache des zu besuchenden Landes oder in englischer Sprache und mit folgenden Angaben versehen vorzulegen:

1. Vor- und Familienname, Geburtsdatum und -ort sowie die Pass- oder Personalausweisnummer des Besuchers;
2. Staatsangehörigkeit des Besuchers;
3. Dienstbezeichnung des Besuchers und Name der Behörde oder Stelle, die er vertritt;
4. Grad der Ermächtigung des Besuchers für den Zugang zu Verschlussachen;
5. Besuchszweck sowie vorgesehene Besuchsdatum;

6. Angabe der Stellen, Ansprechpartner und Einrichtungen, die besucht werden sollen.

Artikel 9

Konsultationen und Beilegung von Streitigkeiten

- (1) Die zuständigen Behörden der Vertragsparteien nehmen von den im Hoheitsgebiet der jeweils anderen Vertragspartei geltenden Bestimmungen über den Schutz von Verschlusssachen Kenntnis.
- (2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die zuständigen Behörden einander auf Ersuchen einer dieser Behörden.
- (3) Jede Vertragspartei erlaubt darüber hinaus der Nationalen oder beauftragten Sicherheitsbehörde der anderen Vertragspartei oder jeder im gegenseitigen Einvernehmen bezeichneten anderen Behörde, Besuche in ihrem Hoheitsgebiet zu machen, um mit ihren Sicherheitsbehörden ihre Verfahren und Einrichtungen zum Schutz von Verschlusssachen, die ihr von der anderen Vertragspartei zur Verfügung gestellt wurden, zu erörtern. Jede Vertragspartei unterstützt diese Behörde bei der Feststellung, ob solche Verschlusssachen, die ihr von der anderen Vertragspartei zur Verfügung gestellt worden sind, ausreichend geschützt werden. Die Einzelheiten der Besuche werden von den zuständigen Behörden im Einklang mit Artikel 8 dieses Abkommens festgelegt.
- (4) Streitigkeiten zwischen den Vertragsparteien, die sich aus der Auslegung oder Anwendung dieses Abkommens ergeben, werden ausschließlich durch Konsultationen oder Verhandlungen der Vertragsparteien beigelegt und nicht an nationale oder internationale Gerichte oder Dritte zur Beilegung verwiesen.

Artikel 10

Verletzung der Bestimmungen über den gegenseitigen Schutz von Verschlusssachen

(1) Wenn eine unbefugte Bekanntgabe von Verschlusssachen nicht auszuschließen ist, vermutet oder festgestellt wird, ist dies der anderen Vertragspartei unverzüglich mitzuteilen.

(2) Verletzungen der Bestimmungen über den Schutz von Verschlusssachen werden von den zuständigen Behörden und/oder Gerichten der Vertragspartei, deren Zuständigkeit jeweils gegeben ist, nach dem Recht dieser Vertragspartei untersucht und verfolgt. Die andere Vertragspartei soll diese Ermittlungen auf Ersuchen unterstützen und ist über das Ergebnis zu unterrichten.

Artikel 11

Kosten

Jede Vertragspartei trägt die ihr bei der Durchführung dieses Abkommens entstehenden Kosten.

Artikel 12

Zuständige Behörden

Die Vertragsparteien unterrichten einander darüber, welche Behörden für die Durchführung dieses Abkommens zuständig sind.

Artikel 13

Verhältnis zu anderen Übereinkünften, Absprachen und Vereinbarungen

Alle bestehenden Abkommen, Absprachen und Vereinbarungen zwischen den Vertragsparteien oder den zuständigen Behörden über den Schutz von Verschlusssachen bleiben von diesem Abkommen unberührt, soweit sie diesem nicht entgegenstehen.

Artikel 14

Schlussbestimmungen

(1) Dieses Abkommen tritt an dem Tag in Kraft, an dem die Regierung der Republik Zypern der Regierung der Bundesrepublik Deutschland notifiziert hat, dass die innerstaatlichen Voraussetzungen für das Inkrafttreten erfüllt sind. Maßgebend ist der Tag des Eingangs der Notifikation.

(2) Dieses Abkommen wird auf unbestimmte Zeit geschlossen.

(3) Dieses Abkommen kann einvernehmlich in Schriftform von den Vertragsparteien geändert werden. Jede Vertragspartei kann jederzeit schriftlich eine Änderung dieses Abkommens beantragen. Stellt eine Vertragspartei einen entsprechenden Antrag, so nehmen die Vertragsparteien Verhandlungen über die Änderung des Abkommens auf.

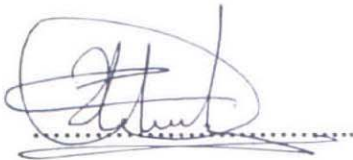
(4) Jede Vertragspartei kann dieses Abkommen unter Einhaltung einer Frist von sechs Monaten auf diplomatischem Wege schriftlich kündigen. Im Fall der Kündigung sind die aufgrund dieses Abkommens übermittelten oder beim Auftragnehmer entstandenen Verschlusssachen weiterhin nach Artikel 4 zu behandeln, solange das Bestehen der Einstufung dies rechtfertigt.

(5) Die Registrierung dieses Abkommens beim Sekretariat der Vereinten Nationen nach Artikel 102 der Charta der Vereinten Nationen wird unverzüglich nach seinem Inkrafttre-

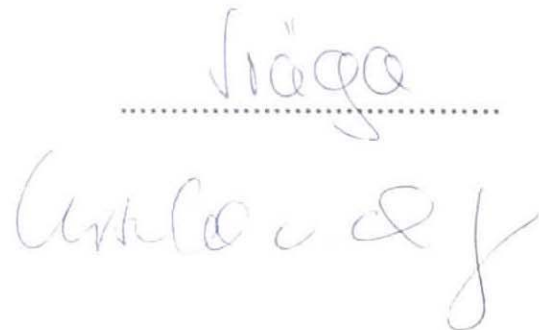
ten von der Vertragspartei veranlasst, in deren Staatsgebiet das Abkommen geschlossen wird. Die andere Vertragspartei wird unter Angabe der VN-Registrierungsnummer von der erfolgten Registrierung unterrichtet, sobald diese vom Sekretariat der Vereinten Nationen bestätigt worden ist.

Geschehen zu ...*Malta* am ...*27.04.2017*... in zwei Urschriften, jede in griechischer, deutscher und englischer Sprache, wobei jeder Wortlaut verbindlich ist. Bei unterschiedlicher Auslegung des griechischen und des deutschen Wortlauts ist der englische Wortlaut maßgebend.

**Für die Regierung
der Republik Zypern**



**Für die Regierung
der Bundesrepublik Deutschland**



**Μέρος III
(Αγγλική Γλώσσα)**

Agreement

between

the Government of the Republic of Cyprus

and

the Government of the Federal Republic of Germany

on the

Mutual Protection of Classified Information

The Government of the Republic of Cyprus

and

the Government of the Federal Republic of Germany

(henceforth the Contracting Parties),

Intending to ensure the protection of classified information that is exchanged between the competent authorities of the Republic of Cyprus and the Federal Republic of Germany as well as with contractors in the territory of the other Contracting Party or between contractors of the two Contracting Parties,

Desirous of laying down an arrangement on the mutual protection of classified information that shall apply to all agreements on cooperation to be concluded between the Contracting Parties and to contracts involving an exchange of classified information,

Have agreed as follows:

Article 1
Definitions

(1) For the purposes of this Agreement

1. "classified information" is

- (a) in the Federal Republic of Germany facts, items or intelligence which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or at the instance of, an official agency in accordance with their need for protection;

- (b) in the Republic of Cyprus
any information or material, irrespective of its form or nature, which requires protection against unauthorized disclosure and/or use and has been classified in accordance with the national legislation;
- 2. a “classified contract” is a contract between an authority or an enterprise from the country of one Contracting Party (contracting entity) and an enterprise from the country of the other Contracting Party (contractor); under such contract, classified information from the country of the contracting entity is to be released to the contractor, is to be established by the contractor or is to be made accessible to duly authorised members of the contractor's staff who are to perform tasks in facilities of the contracting entity;
- 3. “Competent Security Authority” means the security authority or authorities of each Contracting Party responsible for the implementation and supervision of this Agreement;
- 4. “contractor” means an individual or a legal entity possessing the legal capacity to conclude classified contracts;
- 5. “Facility Security Clearance” means the determination by the Competent Security Authority confirming, that the individual or legal entity provides the personal security and has the physical and organizational capability to use, store and protect classified information in accordance with the respective national legislation;
- 6. “need-to-know” means the necessity to have access to classified information in the scope of a given duty or task;
- 7. “Personnel Security Clearance” means the determination by the Competent Security Authority confirming, in accordance with the respective national legislation, that an individual is eligible to have access to certain levels of classified information;

8. "Third Party" means any state, organization, legal entity or individual, which is not a Contracting Party to this Agreement.
- (2) The levels of security classification are defined as follows:
1. In the Federal Republic of Germany, classified information is
 - (a) STRENG GEHEIM if knowledge of it by unauthorized persons may pose a threat to the existence or vital interests of the Federal Republic of Germany or one of its states;
 - (b) GEHEIM if knowledge of it by unauthorized persons may pose a threat to the security of the Federal Republic of Germany or one of its states, or may cause severe damage to their interests;
 - (c) VS-VERTRAULICH if knowledge of it by unauthorized persons may be damaging to the interests of the Federal Republic of Germany or one of its states;
 - (d) VS-NUR FÜR DEN DIENSTGEBRAUCH if knowledge of it by unauthorized persons may be disadvantageous to the interests of the Federal Republic of Germany or one of its states;
 2. in the Republic of Cyprus, classified information is
 - (a) ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the Republic of Cyprus;
 - (b) ΑΠΟΡΡΗΤΟ: information and material the unauthorised disclosure of which could seriously harm the essential interests of the Republic of Cyprus;

- (c) ΕΜΠΙΣΤΕΥΤΙΚΟ: information and material the unauthorised disclosure of which could harm the essential interests of the Republic of Cyprus;
- (d) ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the Republic of Cyprus.

Article 2
Table of Equivalence

The Contracting Parties stipulate that the following security classification levels are equivalent:

For the Republic of Cyprus	For the Federal Republic of Germany	Equivalent in English
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STRENG GEHEIM	TOP SECRET
ΑΠΟΡΡΗΤΟ	GEHEIM	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	VS-VERTRAULICH	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTRICTED

Article 3
Security Classification Markings

(1) Exchanged classified information shall bear a security classification marking corresponding to its security classification level, specified in the national legislation of the Contracting Parties and comparable in accordance with Article 2 by, or on behalf of, the competent authorities. The receiving Contracting party marks the exchanged information accordingly.

(2) Classified information which is generated by the receiving Contracting party in connection with classified contracts as well as copies made by the receiving Contracting party shall also be marked.

(3) Security classifications shall, at the request of the competent authority of the originating Contracting party, be amended or revoked by, or on behalf of, the competent authority of the recipient of the given classified information. The competent authority of the originating Contracting party shall immediately inform the competent authority of the receiving Contracting party of amendments or revocations of a security classification.

Article 4

Measures at the National Level

(1) Within the scope of their national legislation, the Contracting Parties shall take all appropriate measures to guarantee the security protection of classified information generated, exchanged or held under the terms of this Agreement. They shall afford such classified information a degree of security protection at least equal to that required for their own classified information at the equivalent level.

(2) The classified information shall be used solely for the designated purpose. The receiving Contracting party shall not disclose or use, or permit the disclosure or use of, any classified information except for the purposes and within any limitations stated by or on behalf of the originating Contracting party. The originator of the classified information must have given his written consent to any arrangement to the contrary.

(3) Access to classified information may be granted only to persons having a need-to-know on account of their duties and - except in the case of classified information at the "ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ /VS-NUR FÜR DEN DIENSTGEBRAUCH" level - having been authorized to have access to classified information of the equivalent level of security classification. A security clearance shall be granted only after completion of security screening under standards no less stringent than those applied for access to national classified information of the equivalent level of security

classification.

(4) Access to classified information at the "ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH" level or higher by a person holding the nationality of a Contracting Party shall be granted without prior authorization of the originating Contracting party.

(5) Personnel Security Clearances for nationals of the Contracting Party residing, and requiring access to classified information, in their own country shall be undertaken by their National Security Authorities (NSAs)/Designated Security Authorities (DSAs) or other competent national authorities.

(6) However, Personnel Security Clearances for nationals of one Contracting Party who are legally resident in the country of the other Contracting Party and apply for a position that requires access to information classified "ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH" or higher, in that country shall be undertaken by the Competent Security Authority of that country, conducting overseas checks as appropriate.

(7) The Contracting Parties shall, each within its territory, ensure that the necessary security inspections are carried out and that this Agreement is complied with.

(8) Article 5 and Article 6 of this Agreement shall not apply to classified information at the "ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH" level.

Article 5

Award of Classified Contracts

(1) Prior to the award of a classified contract, the contracting entity shall, through his competent authority, obtain a Facility Security Clearance from the competent authority of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the competent authority of this Contracting Party and whether he has taken the security precautions required for discharging the performance of the contract. Where a contractor is not yet subject to security oversight, an application may be made to that end.

(2) A Facility Security Clearance shall also be obtained if an enterprise has been requested to submit a bid and if classified information will have to be released prior to the award of a contract under the bid procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of a Facility Security Clearance for contractors from the country of the other Contracting Party shall contain information on the project as well as the nature, the scope and the level of security classification of the classified information expected to be released to the contractor or to be generated by him.
2. In addition to the full name of the enterprise, its postal address, the name of its security official, its telephone and fax number and its e-mail address, Facility Security Clearances must include information in particular on the extent to which, and the level of security classification up to which, security measures have been taken by the respective enterprise on the basis of national security regulations.
3. The competent authorities of the Contracting Parties shall inform each other of any changes in the facts covered by issued Facility Security Clearances.
4. The exchange of such information between the competent authorities of the Contracting Parties shall be effected either in the national language of the authority to be informed or in English.
5. Facility Security Clearances and requests addressed to the respective competent authorities of the Contracting Parties for the issuance of Facility Security Clearances shall be transmitted in written form.

Article 6
Performance of Classified Contracts

(1) Classified contracts must contain a security requirement clause under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the national security regulations of his country.

(2) In addition, the security requirement clause shall contain the following provisions:

1. the definition of the term "classified information" and of the equivalent levels of protective markings and security classifications of the two Contracting Parties in accordance with the provisions of this Agreement;
2. the names of the competent authority of each of the two Contracting Parties empowered to authorize the release and to coordinate the safeguarding of classified information related to the contract;
3. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;
4. the procedures and mechanisms for communicating changes that may arise in respect of classified information either because of changes in its protective markings or because protection is no longer necessary;
5. the procedures for the approval of visits, or access, by personnel of the contractors;
6. the procedures for transmitting classified information to contractors where such information is to be used or held;
7. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know and has been charged with, or contributes to, the performance of the contract and - except in the case of classified information at the "ΠΕΡΙΟΡΙΣΜΕΝΙΣ

"ΕΜΠΙΣΤΕΥΤΙΚΟ /VS-NUR FÜR DEN DIENSTGEBRAUCH" level - has been security-cleared to the appropriate level in advance:

8. the requirement that classified information shall only be disclosed, or the disclosure of classified information shall only be permitted, to a third party if this has been approved by the originating Contracting party;
9. the requirement that the contractor shall immediately notify his competent authority of any actual or suspected loss, leak or unauthorized disclosure of the classified information covered by the contract;
10. the commitment of the contractor to inform its own Competent Security Authority: of the receipt of a classified contract;
11. the commitment of the subcontractor to fulfill the same security obligations as the contractor.

(3) The competent authority of the contracting entity shall provide the contractor with a separate list (classification guide) of all documentary records requiring security classification, shall determine the required level of security classification and shall arrange for this list to be enclosed as an appendix to the classified contract. The competent authority of the contracting entity shall also transmit, or arrange for the transmission of, the list to the competent authority of the contractor.

(4) The competent authority of the contracting entity shall ensure that the contractor will be given access to classified information only after the pertinent Facility Security Clearance has been received from the competent authority of the contractor.

Article 7

Transmission of Classified Information

(1) As a matter of principle, classified information at the "ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH" and "ΑΠΟΡΡΗΤΟ/GEHEIM" levels shall be transmitted from one country to another by official courier in accordance with national laws and

regulations. The National Security Authorities/Designated Security Authorities of the Contracting Parties may agree on alternative channels of transmission. Receipt of classified information shall be confirmed by, or on behalf of, the competent authority and the classified information shall be forwarded to the recipient in accordance with national security regulations.

(2) For a specifically designated project, the competent authorities may agree - generally or subject to restrictions - that classified information at the "ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH" and "ΑΠΟΡΡΗΤΟ/GEHEIM" levels may be transmitted through channels other than official courier if reliance on the official courier service would cause undue difficulties for such transportation or for the execution of a contract. In such cases

1. the bearer must be authorized to have access to classified information of the equivalent level of security classification;
2. a list of the items of classified information transmitted must be retained by the dispatching agency; a copy of this list shall be handed over to the recipient for forwarding to the competent authority;
3. items of classified information must be packed in accordance with the regulations governing transportation within national boundaries;
4. items of classified information must be delivered against receipt;
5. the bearer must carry a courier certificate issued by the competent authority of the dispatching or the receiving agency.

(3) Where large volumes of classified information are to be transmitted, the means of transportation, the route, and the escort shall be determined on a case-by-case basis and on the basis of a detailed transport plan by the competent authorities.

(4) The electronic transmission of classified information at the "ΕΜΠΙΣΤΕΥΤΙΚΟ/VS-VERTRAULICH" level and higher must not take place in an unencrypted form. Classified information of these levels of security classification may only be encrypted

by encryption means approved by mutual agreement by the Competent Security Authorities of the Contracting Parties.

(5) Classified information at the "ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH" level shall be transmitted according to national laws and regulations.

(6) Classified information at the "ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH" level may be electronically transmitted or made available by means of commercial encryption devices approved by a competent national authority of the Contracting Parties. Classified information of this level of security classification may only be transmitted in an unencrypted form provided that this is not in contradiction with national security regulations, that no approved encryption means are available, transmission is effected within fixed networks only and the sender and the recipient have reached agreement on the proposed transmission in advance.

Article 8 Visits

(1) As a matter of principle, it is only with the prior permission of the competent authority of the Contracting Party the country of which is to be visited that visitors from the territory of one Contracting Party will, on the territory of the other Contracting Party, be granted access to classified information and to facilities in which classified information is being handled. Such permission shall be given only to persons having a need-to-know and - except in the case of classified information at the "ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/VS-NUR FÜR DEN DIENSTGEBRAUCH" level - having been authorized to have access to classified information.

(2) Requests for visits shall be submitted, on a timely basis and in accordance with the regulations of the Contracting State whose territory such visitors wish to enter, to the competent authority of that Contracting Party. The competent authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

(3) Requests for visits shall be submitted in the language of the country to be visited or in English and shall contain the following information:

1. the visitor's first name and surname, date and place of birth, and his/her passport or identity card number;
2. the visitor's nationality;
3. the visitor's service designation, and the name of his/her parent authority or agency;
4. the level of the visitor's security clearance for access to classified information;
5. the purpose of the visit, and the proposed date of the visit;
6. the designation of the agencies, the contact persons and the installations to be visited.

Article 9

Consultations and Dispute Settlements

(1) The competent authorities of the Contracting Parties shall take note of the provisions governing the protection of classified information that apply within the territory of the other Contracting Party.

(2) To ensure close cooperation in the implementation of this Agreement, the competent authorities shall consult each other at the request of one of these authorities.

(3) Each Contracting Party shall, in addition, allow the National or Designated Security Authority of the other Contracting Party or any other authority designated by mutual agreement to visit its territory in order to discuss, with its security authorities, its procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that authority in

ascertaining whether such classified information which has been made available by the other Contracting Party is adequately protected. The details of the visits shall be laid down by the competent authorities in accordance with the provisions of Article 8 of this Agreement.

(4) Any dispute between the Contracting Parties arising out of the interpretation or implementation of this Agreement shall be settled solely through consultations or negotiations between the Contracting Parties and shall not be referred to any national or international tribunal or third party for settlement.

Article 10
Violations of Provisions Governing the
Mutual Protection of Classified Information

(1) Whenever unauthorized disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed.

(2) Violations of provisions governing the protection of classified information shall be investigated, and pertinent legal action shall be taken, by the competent authorities and/or courts of the Contracting Party having jurisdiction respectively, according to that Contracting Party's law. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

Article 11
Costs

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

Article 12
Competent Authorities

The Contracting Parties shall inform each other of the authorities to be responsible for the implementation of this Agreement.

Article 13
Relationship with Other Agreements, Memoranda of Understanding
and Arrangements

Any existing Agreements, Memoranda of Understanding and Arrangements between the Contracting Parties or the competent authorities on the protection of classified information shall be unaffected by the present Agreement in so far as they do not conflict with its provisions.

Article 14
Final Provisions

(1) This Agreement shall enter into force on the date on which the Government of the Republic of Cyprus has notified the Government of the Federal Republic of Germany that the national requirements for such entry into force have been fulfilled. The relevant date shall be the date of receipt of the notification.

(2) This Agreement is concluded for an indefinite period of time.

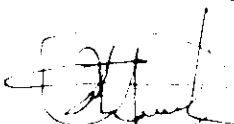
(3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall initiate negotiations on the amendment of the Agreement.

(4) Either Contracting Party may, through diplomatic channels, denounce this Agreement by giving six months' written notice. In the event of denunciation, classified information transmitted, or generated by the contractor, on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 4 above for as long as is justified by the existence of the security classification.

(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 Contracting Party on whose national territory the Agreement is concluded immediately following its entry into force. The other Contracting Party shall be informed of registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat.

Done at Malta on 27 April 2017 in two originals, in the Greek, German and English languages, all three texts being authentic. In case of divergent interpretations of the German and Greek texts, the English text shall prevail.

**For the Government of the
Republic of Cyprus**


.....

**For the Government of the
Federal Republic of Germany**


.....

