



**ΕΠΙΣΗΜΗ ΕΦΗΜΕΡΙΔΑ  
ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ  
ΠΑΡΑΡΤΗΜΑ ΠΡΩΤΟ  
ΝΟΜΟΘΕΣΙΑ - ΜΕΡΟΣ ΙΙΙ**

Αριθμός 4287	Δευτέρα, 12 Δεκεμβρίου 2022	455
--------------	-----------------------------	-----

Ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Κροατίας για την Ανταλλαγή και Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2022 εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος.

Αριθμός 14(III) του 2022

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

Η Βουλή των Αντιπροσώπων ψηφίζει ως ακολούθως:

Συνοπτικός τίτλος.

1. Ο παρών Νόμος θα αναφέρεται ως ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Κροατίας για την Ανταλλαγή και Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2022.

Ερμηνεία.

2. Στον παρόντα Νόμο «Συμφωνία» σημαίνει τη Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Κροατίας για την Ανταλλαγή και Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών, η διαπραγμάτευση της οποίας εγκρίθηκε με την υπ' αριθμόν 84.779 Απόφαση του Υπουργικού Συμβουλίου, ημερομηνίας 24 Απριλίου 2018, και υπεγράφη στο Ζάγκρεμπ στις 4 Οκτωβρίου 2021 από τον Γενικό Διευθυντή του Υπουργείου Εξωτερικών εκ μέρους της Κυπριακής Δημοκρατίας.

Κύρωση της Συμφωνίας. Πίνακας, Μέρος I, Μέρος II, Μέρος III.

3. Με τον παρόντα Νόμο κυρώνεται η Συμφωνία το κείμενο της οποίας εκτίθεται στο Μέρος I του Πίνακα στην ελληνική γλώσσα, στο Μέρος II του Πίνακα στην κροατική γλώσσα και στο Μέρος III του Πίνακα στην αγγλική γλώσσα:

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

Αρμόδια αρχή.

4. Αρμόδια αρχή για την εφαρμογή της Συμφωνίας ορίζεται ο Υπουργός Άμυνας.

ΠΙΝΑΚΑΣ  
(Άρθρο 3)

ΜΕΡΟΣ I  
(Κείμενο στην ελληνική γλώσσα)

ΜΕΡΟΣ II  
(Κείμενο στην κροατική γλώσσα)

ΜΕΡΟΣ III  
(Κείμενο στην αγγλική γλώσσα)

ΜΕΡΟΣ Γ  
(Κείμενο στην ελληνική γλώσσα)  
ΣΥΜΦΩΝΙΑ

ΜΕΤΑΞΥ

ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΚΑΙ

ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΚΡΟΑΤΙΑΣ

ΓΙΑ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΚΑΙ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ  
ΠΛΗΡΟΦΟΡΙΩΝ

Η κυβέρνηση της Κυπριακής Δημοκρατίας και η κυβέρνηση της Δημοκρατίας της Κροατίας (εφεξής καλούμενες «τα Μέρη»),

Αναγνωρίζοντας, την ανάγκη για τον καθορισμό κανόνων σχετικά με τη προστασία Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάσσουν προς το συμφέρον της εθνικής ασφαλείας, στα πλαίσια πολιτικής, στρατιωτικής, οικονομικής, νομικής, επιστημονικής και τεχνολογικής ή άλλης συνεργασίας, καθώς και Διαβαθμισμένων Πληροφοριών που προκύπτουν από την εν λόγω συνεργασία,

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία όλων των Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάσσουν μεταξύ τους ή που παράγονται από κοινού στα πλαίσια συνεργασίας μεταξύ των Μερών,

Επιθυμώντας να θεσπίσουν κανόνες για τη ρύθμιση της αμοιβαίας προστασίας των Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάσσουν τα Μέρη μεταξύ τους ή που παράγονται από κοινού στα πλαίσια συνεργασίας μεταξύ των Μερών,

Λαμβάνοντας υπόψη το αμοιβαίο συμφέρον της προστασίας των Διαβαθμισμένων Πληροφοριών, σύμφωνα με την εθνική νομοθεσία των Μερών

Συμφώνησαν τα ακόλουθα

Άρθρο 1  
Σκοπός

Σκοπός της παρούσας Συμφωνίας είναι η διασφάλιση της προστασίας των Διαβαθμισμένων Πληροφοριών τις οποίες παράγουν ή ανταλλάσσουν μεταξύ τους τα Μέρη ή οι εργολάβοι, υπεργολάβοι ή οποιοδήποτε νομικό πρόσωπο ιδιωτικού ή δημοσίου δικαίου, το οποίο εξουσιοδοτείται να χειρίζεται και να αποθηκεύει Διαβαθμισμένες Πληροφορίες.

## Άρθρο 2 Ορισμοί

Για τους σκοπούς της παρούσας Συμφωνίας:

1. «Πάραβιαση Ασφαλείας» σημαίνει πράξη ή παράλειψη η οποία αντιβαίνει στην παρούσα Συμφωνία ή στην εθνική νομοθεσία των Μερών και το αποτέλεσμα της οποίας ενδέχεται να οδηγήσει σε μη εξουσιοδοτημένη γνωστοποίηση, απώλεια, καταστροφή, παράνομη χρήση ή οποιαδήποτε άλλη διαρροή των Διαβαθμισμένων Πληροφοριών,
2. «Διαβαθμισμένη Σύμβαση» σημαίνει κάθε συμφωνία που υπογράφεται μεταξύ δύο ή περισσότερων Εργολάβων και η οποία περιέχει ή περιλαμβάνει πρόσβαση σε Διαβαθμισμένες Πληροφορίες ή η εκτέλεση της οποίας απαιτεί πρόσβαση σε Διαβαθμισμένες Πληροφορίες,
3. «Διαβαθμισμένες Πληροφορίες» σημαίνει κάθε πληροφορία, ανεξαρτήτως τύπου ή φύσεως, η οποία χρήζει προστασίας από μη εξουσιοδοτημένη πρόσβαση ή χειρισμό και διαβαθμίστηκε με κάποιο επίπεδο διαβάθμισης ασφαλείας, σύμφωνα με την εθνική νομοθεσία των Μερών,
4. «Αρμόδια Αρχή Ασφαλείας» σημαίνει οποιαδήποτε αρμόδια αρχή των Μερών εκτός των Εθνικών Αρχών Ασφαλείας, η οποία, σύμφωνα με την εθνική νομοθεσία των Μερών, είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας,
5. «Εργολάβος» σημαίνει το φυσικό ή νομικό πρόσωπο, το οποίο έχει τη νομική ικανότητα σύναψης ή ανάληψης διαβαθμισμένων συμβάσεων,
6. «Εξουσιοδότηση Ασφαλείας Φορέα» σημαίνει τη θετική απόφαση της Εθνικής Αρχής Ασφαλείας, η οποία επιβεβαιώνει, σύμφωνα με την εθνική νομοθεσία των Μερών, ότι κάποιο φυσικό ή νομικό πρόσωπο εξουσιοδοτείται να έχει πρόσβαση σε και να χειρίζεται Διαβαθμισμένες Πληροφορίες έως ένα συγκεκριμένο επίπεδο διαβάθμισης,
7. «Εθνική Αρχή Ασφαλείας» σημαίνει την αρχή κάθε Μέρους, που αναφέρεται στο Άρθρο 4 της παρούσας συμφωνίας και η οποία είναι υπεύθυνη για την εφαρμογή και επίσημη της παρούσας Συμφωνίας,
8. «Ανάγκη για γνώση» σημαίνει την αρχή βάσει της οποίας παρέχεται πρόσβαση σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες αποκλειστικά στα πλαίσια συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας,

9. «Εξουσιοδότηση Ασφαλείας Προσωπικού» σημαίνει τη θετική απόφαση της Εθνικής Αρχής Ασφαλείας, η οποία επιβεβαιώνει, σύμφωνα με την εθνική νομοθεσία των Μερών, ότι το φυσικό πρόσωπο εξουσιοδοτείται να έχει πρόσβαση σε και να χειρίζεται Διαβαθμισμένες Πληροφορίες έως κάποιο συγκεκριμένο επίπεδο διαβάθμισης.

10. «Μέρος Αποστολέας» σημαίνει το Μέρος το οποίο δημιουργεί και παρέχει Διαβαθμισμένες Πληροφορίες στο Μέρος Παραλήπτη.

11. «Μέρος Παραλήπτης» σημαίνει το Μέρος στο οποίο διαβιβάζονται Διαβαθμισμένες Πληροφορίες από το Μέρος Αποστολέα.

12. «Επίπεδο Διαβάθμισης Ασφαλείας» σημαίνει την κατηγορία η οποία, σύμφωνα με την εθνική νομοθεσία των Μερών, αντιστοιχεί στο επίπεδο περιορισμού της πρόσβασης σε Διαβαθμισμένες Πληροφορίες και στο ελάχιστο επίπεδο προστασίας.

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

### Άρθρο 3 Επίπεδα Διαβάθμισης Ασφαλείας

Τα Μέρη συμφωνούν ότι τα ακόλουθα Επίπεδα Διαβάθμισης Ασφαλείας και διαβαθμίσεις ισοδυναμούν και αντιστοιχούν στα Επίπεδα Διαβάθμισης Ασφαλείας, τα οποία ορίζονται από την εθνική τους νομοθεσία:

Για την Κυπριακή Δημοκρατία	Για τη Δημοκρατία της Κροατίας	Αντιστοιχη αγγλική αρολογία
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	VRLO TAJNO	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	POUJERLJIVO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	OGRANICENO	RESTRICTED

### Άρθρο 4 Εθνικές Αρχές Ασφαλείας

1. Οι Εθνικές Αρχές Ασφαλείας των μερών είναι:

Για την Κυπριακή Δημοκρατία:  
Εθνική Αρχή Ασφαλείας (ΕΑΑ)  
Υπουργείο Άμυνας της Κυπριακής Δημοκρατίας.

Για τη Δημοκρατία της Κροατίας:  
Γραφείο Συμβουλίου Εθνικής Ασφαλείας.

2. Τα Μέρη αλληλοενημερώνονται μέσω της διπλωματικής οδού για τυχόν αλλαγές που αφορούν στις Εθνικές Αρχές Ασφαλείας.

3. Οι Εθνικές Αρχές Ασφαλείας αλληλοενημερώνονται για την αντίστοιχη εθνική νομοθεσία περί Διαβαθμισμένων Πληροφοριών και για τυχόν σημαντικές τροποποιήσεις σε αυτή και ανταλλάσσουν πληροφορίες σχετικά με τα πρότυπα ασφαλείας, τις διαδικασίες και πρακτικές που αφορούν στην προστασία Διαβαθμισμένων Πληροφοριών.

4. Κατόπιν αιτήματος, οι Εθνικές Αρχές Ασφαλείας αλληλοενημερώνονται σχετικά με άλλες αρμόδιες Αρχές.

#### Άρθρο 5

#### Μέτρα Προστασίας και Πρόσβαση σε Διαβαθμισμένες Πληροφορίες

1. Σύμφωνα με την εθνική τους νομοθεσία, τα Μέρη λαμβάνουν όλα τα απαραίτητα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών τις οποίες παράγουν ή ανταλλάσσουν βάσει της παρούσας Συμφωνίας. Τα Μέρη θα παρέχουν στις Διαβαθμισμένες Πληροφορίες, οι οποίες παράγονται και/ή παρέχονται βάσει της παρούσας Συμφωνίας, το ίδιο επίπεδο ασφαλείας, όπως προβλέπεται για τις εθνικές τους Διαβαθμισμένες Πληροφορίες του αντίστοιχου Επιπέδου Διαβάθμισης Ασφαλείας, σύμφωνα με το Άρθρο 3 της παρούσας Συμφωνίας.

2. Το Μέρος Αποστολέας ενημερώνει:

- α) το Μέρος Παραλήπτη για τυχόν προϋποθέσεις διάθεσης ή περιορισμούς στη χρήση των Διαβαθμισμένων Πληροφοριών,
- β) το Μέρος Παραλήπτη γραπτώς για τυχόν αλλαγή στο Επίπεδο Διαβάθμισης Ασφαλείας των διαβιβασθέντων Διαβαθμισμένων Πληροφοριών.

3. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες στο Επίπεδο Διαβάθμισης Ασφαλείας ΕΜΓΙΣΤΕΥΤΙΚΟ / ΡΟΥΒΕΡΛΙΝΟ / CONFIDENTIAL και άνω περιορίζεται σε φυσικά και νομικά πρόσωπα που κατέχουν κατάλληλο πιστοποιητικό ασφαλείας του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας και βάσει της αρχής της ανάγκης για γνώση, σύμφωνα με την εθνική νομοθεσία των Μερών.

4. Δεν απαιτείται Εξουσιοδότηση Ασφαλείας Προσωπικού για πρόσβαση σε Διαβαθμισμένες Πληροφορίες στο Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / ΟΓΡΑΝΙΩΕΝΟ / RESTRICTED. Η πρόσβαση αυτή περιορίζεται σε φυσικά πρόσωπα βάσει της αρχής της ανάγκης για

γνώση και τα οποία έχουν δεόντως ενημερωθεί για τις ευθύνες και υποχρεώσεις τους που αφορούν στην πρακτική τέτοιων Διαβαθμισμένων Πληροφοριών.

5. Στο πλαίσιο της παρούσας Συμφωνίας, κάθε Μέρος αναγνωρίζει τις Εξουσιοδοτήσεις Ασφαλείας Προσωπικού και Εξουσιοδοτήσεις Ασφαλείας Φορέα, οι οποίες παρέχονται σύμφωνα με την εθνική νομοθεσία του κράτους του άλλου Μέρους. Οι εν λόγω Εξουσιοδοτήσεις Ασφαλείας θα είναι ισοδύναμες με τα Επίπεδα Διαβάθμισης Ασφαλείας που προβλέπονται στο Άρθρο 3 της παρούσας Συμφωνίας.

6. Οι Εθνικές Αρχές Ασφαλείας, κατόπιν αιτήματος και σύμφωνα με την αντίστοιχη εθνική νομοθεσία τους, αλληλοβοηθούνται στη διεξαγωγή των διαδικασιών ελέγχου ασφαλείας, οι οποίες απαιτούνται για την εφαρμογή της παρούσας Συμφωνίας.

7. Στο πλαίσιο της παρούσας Συμφωνίας, οι Εθνικές Αρχές Ασφαλείας των Μερών αλληλοενημερώνονται χωρίς καθυστέρηση σχετικά με τυχόν αλλαγές στις Εξουσιοδοτήσεις Ασφαλείας Προσωπικού και Εξουσιοδοτήσεις Ασφαλείας Φορέα, και πιο συγκεκριμένα όταν πρόκειται για την απόσυρση ή την υποβάθμιση του Επιπέδου Διαβάθμισης Ασφαλείας.

8. Το Μέρος Παραλήπτης:

- α) Υποβάλλει Διαβαθμισμένες Πληροφορίες σε τυχόν Τρίτο Μέρος μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα,
- β) Διαβαθμίζει την παραληφθείσα πληροφορία σύμφωνα με το Επίπεδο Διαβάθμισης Ασφαλείας, όπως καθορίζεται στο Άρθρο 3 της παρούσας Συμφωνίας,
- γ) Χρησιμοποιεί Διαβαθμισμένες Πληροφορίες μόνο για τους σκοπούς για τους οποίους προβλέπονται.

#### Άρθρο 6

#### Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Διαβαθμισμένες Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO ΤΑΙΝΟ / TOP SECRET διαβιβάζονται μέσω



κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών. Ως ελάχιστο επίπεδο ασφαλείας τέτοιες Διαβαθμισμένες Πληροφορίες μεταφέρονται από και υπό τον αποκλειστικό έλεγχο Κυβερνητικού ταχυμεταφορέα ο οποίος κατέχει Εξουσιοδότηση Ασφαλείας Προσωπικού στο Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO ΤΑΙΝΟ / TOP SECRET. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη των Διαβαθμισμένων Πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO ΤΑΙΝΟ / TOP SECRET.

2. Διαβαθμισμένες Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ / SECRET διαβιβάζονται μέσω κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών ή μέσω άλλης ασφαλούς οδού την οποία έχουν εγκρίνει αμοιβαία οι Αρχές Ασφαλείας και των δύο μερών. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη των Διαβαθμισμένων Πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ / SECRET.

3. Διαβαθμισμένες Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΕΜΠΙΣΤΕΥΤΙΚΟ / ΡΟΝΤΕΡΛΙΝΟ / CONFIDENTIAL διαβιβάζονται μέσω κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών ή μέσω άλλης ασφαλούς οδού την οποία έχουν εγκρίνει αμοιβαία οι Αρχές Ασφαλείας και των δύο μερών. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΕΜΠΙΣΤΕΥΤΙΚΟ / ΡΟΝΤΕΡΛΙΝΟ / CONFIDENTIAL.

4. Διαβαθμισμένες Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / ΟΓΡΑΝΙΩΕΝΟ / RESTRICTED διαβιβάζονται μέσω ασφαλούς οδού σύμφωνα με την εθνική νομοθεσία των Μερών.

5. Οι διαδικασίες για τη μεταφορά μεγάλων φορτίων που περιέχουν Διαβαθμισμένες Πληροφορίες αξιολογούνται και συμφωνούνται από κοινού από τις Εθνικές Αρχές Ασφαλείας, για κάθε περίπτωση ξεχωριστά.

6. Εάν Διαβαθμισμένες Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / ΟΓΡΑΝΙΩΕΝΟ / RESTRICTED, ΕΜΠΙΣΤΕΥΤΙΚΟ / ΡΟΝΤΕΡΛΙΝΟ / CONFIDENTIAL ή ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ / SECRET πρόκειται να διαβιβαστούν ηλεκτρονικά μεταξύ των Μερών, δεν αποστέλλονται υπό μορφή απλού κειμένου. Η ηλεκτρονική διαβίβαση Διαβαθμισμένων Πληροφοριών των συγκεκριμένων Επιπέδων Διαβάθμισης



Ασφαλείας γίνεται μέσω πιστοποιημένων κρυπτογραφικών μέσων, τα οποία έχουν εγκριθεί αραιβαία από τις Εθνικές Αρχές Ασφαλείας:

7. Τα κύρια σημεία εισόδου και εξόδου Διαβαθμισμένων Πληροφοριών τις οποίες ανταλλάτουν τα Μέρη στο πλαίσιο της παρούσας Συμφωνίας είναι:

Για την Κυπριακή Δημοκρατία:

Η Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ του Υπουργείου Εξωτερικών,

Για την Δημοκρατία της Κροατίας:

Η Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ στο Γραφείο του Εθνικού Συμβουλίου Ασφαλείας.

8. Χωρίς επηρεασμό των διατάξεων της Παραγράφου 7 του παρόντος Άρθρου, όποτε κρίνεται αναγκαία η ανταλλαγή Διαβαθμισμένων Πληροφοριών από τις Δυνάμεις Ασφαλείας, η ανταλλαγή αυτή γίνεται σύμφωνα με την εθνική τους νομοθεσία.

9. Τα κύρια σημεία εισόδου και εξόδου για αυτή την κατηγορία Διαβαθμισμένων Πληροφοριών συμφωνούνται από τις Δυνάμεις Ασφαλείας και η ανταλλαγή γίνεται κατόπιν γραπτής συγκατάθεσης και έγκρισης σύμφωνα με την εθνική νομοθεσία των Μερών.

10. Εάν είναι αναγκαία, οι υπηρεσίες πληροφοριών των Μερών δύνανται, σύμφωνα με την εθνική νομοθεσία, να ανταλλάζουν επιχειρησιακές πληροφορίες και πληροφορίες ασφαλείας απευθείας μεταξύ τους.

### **Άρθρο 7**

#### **Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών**

1. Οι μεταφράσεις και οι αναπαραγωγές Διαβαθμισμένων Πληροφοριών γίνονται σύμφωνα με την εθνική νομοθεσία του Μέρους Παραλήπτη.

2. Οι πληροφορίες που φέρουν τα Επίπεδα Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ / SECRET ή ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLIO ΤΑΙΝΟ / TOP SECRET μεταφράζονται ή αναπαραγόμενοι μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα.

3. Όλα τα αντίγραφα Διαβαθμισμένων Πληροφοριών διαβαθμίζονται σε

Επίπεδο Διαβάθμισης Ασφαλείας και προστατεύονται όπως και οι πρωτότυπες Διαβαθμισμένες Πληροφορίες.

4. Τέτοιες αναπαραχθείσες Διαβαθμισμένες Πληροφορίες προστατεύονται με τον ίδιο τρόπο όπως και οι πρωτότυπες Διαβαθμισμένες Πληροφορίες.

5. Ο αριθμός των αντιγράφων Διαβαθμισμένων Πληροφοριών περιορίζεται στον αριθμό που απαιτείται για επίσημους σκοπούς.

6. Οι μεταφράσεις διαβαθμίζονται με το Επίπεδο Διαβάθμισης Ασφαλείας του πρωτότυπου και φέρουν κατάλληλη σημείωση στη γλώσσα μετάφρασης, υποδεικνύοντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες που λήφθηκαν από το Μέρος Αποστολέα.

#### **Άρθρο 8** **Καταστροφή Διαβαθμισμένων Πληροφοριών**

1. Οι Διαβαθμισμένες Πληροφορίες καταστρέφονται ώστε να αποφευχθεί η μερική ή ολική ανακατασκευή τους.

2. Οι πληροφορίες που έχουν διαβαθμιστεί έως το Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ / SECRET καταστρέφονται σύμφωνα με την εθνική νομοθεσία των Μερών.

3. Οι πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO ΤΑΙΝΟ / TOP SECRET δεν καταστρέφονται. Επιστρέφονται στο Μέρος Αποστολέα.

4. Η έκθεση για την καταστροφή των Διαβαθμισμένων Πληροφοριών, η οποία συντάσσεται στην αγγλική γλώσσα, παραδίδεται στην Εθνική Αρχή Ασφαλείας ή σε οποιαδήποτε άλλη Αρμόδια Αρχή Ασφαλείας του Μέρους Αποστολέα.

5. Σε περίπτωση κατάστασης κρίσης κατά την οποία δεν είναι δυνατή η προστασία ή η επιστροφή Διαβαθμισμένων Πληροφοριών τις οποίες αντάλλαξαν ή παρήγαγαν τα Μέρη βάσει της παρούσας Συμφωνίας, αυτές καταστρέφονται αμέσως. Το Μέρος Παραλήπτης ενημερώνει την Εθνική Αρχή Ασφαλείας ή οποιαδήποτε Αρμόδια Αρχή Ασφαλείας του Μέρους Αποστολέα σχετικά με την εν λόγω καταστροφή το συντομότερο δυνατόν.

**Άρθρο 9**  
**Διαβαθμισμένες Συμβάσεις**

1. Οι Διαβαθμισμένες Συμβάσεις συμφωνούνται και εκτελούνται σύμφωνα με την εθνική νομοθεσία κάθε Μέρους.

2. Η Εθνική Αρχή Ασφαλείας του ενός Μέρους παρέχει, εκ των προτέρων, στην Εθνική Αρχή Ασφαλείας του άλλου Μέρους γραπτή επιβεβαίωση ότι ο εργολάβος ή ο υπεργολάβος που επιθυμεί να συνάψει σύμβαση με Επίπεδο Διαβάθμισης Ασφαλείας ΕΜΠΙΣΤΕΥΤΙΚΟ / ΡΟΥΒΕΡΛΙΝΟ / CONFIDENTIAL ή/και ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ / SECRET με αυτό το άλλο Μέρος, διαθέτει ή για την εξασφάλιση Εξουσιοδότησης Ασφαλείας Φορέα για το κατάλληλο Επίπεδο Διαβάθμισης Ασφαλείας.

3. Ένα παράρτημα ασφαλείας με το οποίο το Μέρος Αποστολέας υποδεικνύει ποιες Διαβαθμισμένες Πληροφορίες πρόκειται να αποσταλούν στο Μέρος Παραλήπτη, σε ποιο Επίπεδο Διαβάθμισης Ασφαλείας έχουν διαβαθμιστεί οι συγκεκριμένες πληροφορίες και τις υποχρεώσεις του Εργολάβου να προστατέψει τις Διαβαθμισμένες Πληροφορίες, αποτελεί αναπόσπαστο μέρος κάθε Διαβαθμισμένης Σύμβασης ή σύμβασης υπεργολαβίας.

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

- α) Δέσμευση του Εργολάβου ή του υπεργολάβου με την οποία διασφαλίζεται ότι τα υποστατικά του πληρούν τις απαραίτητες προϋποθέσεις για χειρισμό και αποθήκευση Διαβαθμισμένων Πληροφοριών ενός συγκεκριμένου Επιπέδου Διαβάθμισης Ασφαλείας,
- β) Δέσμευση του Εργολάβου ή του υπεργολάβου με την οποία διασφαλίζεται ότι όλα τα άτομα που εκτελούν καθήκοντά τα οποία απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες είναι θεόντως εξουσιοδοτημένα, σύμφωνα με την εθνική τους νομοθεσία, να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες με το αντίστοιχο Επίπεδο Διαβάθμισης Ασφαλείας και ότι ενημερώνονται τακτικά σε θέματα ασφαλείας,
- γ) Δέσμευση γνωστοποίησης τυχόν αλλαγής στο Επίπεδο Διαβάθμισης Ασφαλείας των Διαβαθμισμένων Πληροφοριών σύμφωνα με την εθνική τους νομοθεσία,
- δ) Κατάλογο με τις Διαβαθμισμένες Πληροφορίες και τους χώρους χειρισμού και αποθήκευσης των Διαβαθμισμένων Πληροφοριών.

- ε) Τη διαδικασία διαβίβασης Διαβαθμισμένων Πληροφοριών,
- στ) Δέσμευση του Εργολάβου ή του υπεργολάβου να ενημερώνει τις αντίστοιχες Εθνικές Αρχές Ασφαλείας του για τυχόν πραγματική ή ενδεχόμενη Παραβίαση Ασφαλείας, σύμφωνα με την εθνική τους νομοθεσία,
- ζ) Δέσμευσή του Εργολάβου ή του υπεργολάβου να προωθήσει αντίγραφο της Διαβαθμισμένης Σύμβασης στις Εθνικές Αρχές Ασφαλείας και των δύο Μερών,
- η) Δέσμευση του υπεργολάβου να τηρήσει τις ίδιες υποχρεώσεις ασφαλείας με τον εργολάβο.

6. Μόλις ξεκινήσουν οι προ-συμβατικές διαπραγματεύσεις της σύμβασης μεταξύ των πιθανών Εργολάβων, η Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα ενημερώνει την Εθνική Αρχή Ασφαλείας του Μέρους Παραλήπτη σχετικά με το Επίπεδο Διαβάθμισης Ασφαλείας που δόθηκε στις Διαβαθμισμένες Πληροφορίες οι οποίες σχετίζονται με τις διαπραγματεύσεις αυτές.

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

#### **Άρθρο 10 Επισκέψεις**

1. Οι επισκέψεις που αφορούν σε Διαβαθμισμένες Σύμβασεις και προϋποθέτουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες υπόκεινται στην εκ των προτέρων γραπτή έγκριση την οποία παρέχει η Αρμόδια Αρχή Ασφαλείας του Μέρους υποδοχής.
2. Η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής θα πρέπει να λάβει αίτηση επίσκεψης τουλάχιστον δέκα ημέρες νωρίτερα.
3. Σε έκτακτες περιπτώσεις η αίτηση επίσκεψης μπορεί να διαβιβαστεί εντός συντομότερης προθεσμίας.
4. Η αίτηση επίσκεψης περιλαμβάνει:

- α) Το ονοματεπώνυμο του επισκέπτη, τον τόπο και την ημερομηνία γέννησης, την υπηκοότητα και τον αριθμό διαβατηρίου ή ταυτότητας.
- β) Την επωνυμία του νομικού προσώπου το οποίο εκπροσωπεί ο επισκέπτης και τη θέση του επισκέπτη στο νομικό πρόσωπο.
- γ) Την επωνυμία, τη διεύθυνση και τα στοιχεία επικοινωνίας του νομικού προσώπου και των εγκαταστάσεων που πρόκειται να δεχθούν την επίσκεψη.
- δ) Επιβεβαίωση της Εξουσιοδότησης Ασφαλείας Προσωπικού του επισκέπτη, της εγκυρότητάς και του Επιπέδου Διαβάθμισης Ασφαλείας αυτής.
- ε) Το σκοπό και τους λόγους της επίσκεψης, καθώς και το υψηλότερο Επίπεδο Διαβάθμισης Ασφαλείας των Διαβαθμισμένων Πληροφοριών στις οποίες αφορά η επίσκεψη.
- στ) Την αναμενόμενη ημερομηνία και διάρκεια της επίσκεψης. Σε περίπτωση επαναλαμβανόμενων επισκέψεων, αναφέρεται η συνολική διάρκεια των επισκέψεων.
- ζ) Την ημερομηνία, την υπογραφή και την επίσημη σφραγίδα της σχετικής Εθνικής Αρχής Ασφαλείας.

5. Μόλις εγκριθεί η επίσκεψη, η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής παρέχει αντίγραφο της αίτησης επίσκεψης στους λειτουργούς ασφαλείας του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη.

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

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

### **Άρθρο 11** **Παραβίαση Ασφαλείας**

1. Σε περίπτωση πραγματικής ή εικαζόμενης παραβίασης ασφαλείας, η Εθνική Αρχή Ασφαλείας του Μέρους Παραλήπτη ενημερώνει την Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα το συντομότερα δυνατόν, σύμφωνα με την εθνική της νομοθεσία, και ξεκινά κατάλληλη έρευνα για τη διαπίστωση των περιστάσεων της παραβίασης ασφαλείας. Τα αποτελέσματα των ερευνών και η τελική έκθεση για τις αιτίες και την έκταση της ζημιάς προωθούνται στην Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα.
2. Εάν η παραβίαση ασφαλείας επέλθει σε τρίτη χώρα, η Εθνική Αρχή Ασφαλείας του Μέρους τα οποία κοινοποιήσει τις πληροφορίες στην τρίτη χώρα λαμβάνει όλα τα απαραίτητα μέτρα για να διασφαλίσει ότι οι ενέργειες που περιγράφονται στην Παράγραφο 1 του παρόντος Άρθρου έχουν τεθεί σε εφαρμογή.
3. Το Μέρος Αποστολέας, κατόπιν αιτήματος, συνεργάζεται στην έρευνα σύμφωνα με την Παράγραφο 1 του παρόντος Άρθρου.

### **Άρθρο 12** **Έξοδα**

Κάθε Μέρος αναλαμβάνει τα δικά του έξοδα τα οποία προκύπτουν από την εφαρμογή και επίσημο της παρούσας Συμφωνίας.

### **Άρθρο 13** **Διευθέτηση Διαφορών**

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

### **Άρθρο 14** **Τελικές Πρόνοιες**

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

2. Η παρούσα Συμφωνία δύναται να τροποποιηθεί με αμοιβαία γραπτή συγκατάθεση των Μερών. Οι τροποποιήσεις τίθενται σε ισχύ σύμφωνα με την Παράγραφο 1 του παρόντος Άρθρου.

3. Κάθε Μέρος δύναται, ανά πάσα στιγμή, να τερματίσει τη Συμφωνία δίδοντας στο άλλο Μέρος γραπτή ειδοποίηση μέσω της διπλωματικής οδού. Στην περίπτωση αυτή, η λήξη της Συμφωνίας τίθεται σε ισχύ έξι (6) μήνες μετά την ημερομηνία παραλαβής της αντίστοιχης ανακοίνωσης τερματισμού από το άλλο Μέρος.

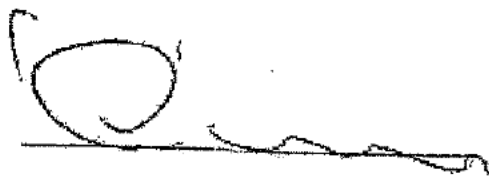
4. Σε περίπτωση τερματισμού της παρούσας Συμφωνίας όλες οι Διαβαθμισμένες Πληροφορίες τις οποίες αντάλλαξαν τα Μέρη δυνάμει της παρούσας Συμφωνίας συνεχίζουν να προστατεύονται σύμφωνα με τις πρόνοιες που ορίζονται ανωτέρω και επιστρέφονται στο Μέρος Αποσταλέα.

5. Το Μέρος στο κράτος του οποίου συνάφθηκε η παρούσα Συμφωνία κινεί τη διαδικασία που αφορά στην καταχώρηση της Συμφωνίας στη Γραμματεία των Ηνωμένων Εθνών, σύμφωνα με το Άρθρο 102 της Χάρτας των Ηνωμένων Εθνών, μόλις τεθεί σε ισχύ. Το άλλο Μέρος ενημερώνεται για την καταχώρηση και τον αριθμό καταχώρησης, μόλις η Γραμματεία των Ηνωμένων Εθνών επιβεβαιώσει την καταχώρηση αυτή.

Συντάχθηκε στην Ζάγκρεμπ, στις 4. Οκτωβρίου 2001 σε δύο πρωτότυπα, στην Ελληνική, Κροατική και Αγγλική γλώσσα, και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση διαφωνίας στην ερμηνεία, το αγγλικό κείμενο υπερισχύει.

ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΗΣΗ ΤΗΣ  
ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΗΣΗ ΤΗΣ  
ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΚΡΟΑΤΙΑΣ






ΜΕΡΟΣ ΙΙ  
(Κείμενο στην κροατική γλώσσα)

UGOVOR

IZMEĐU

VLADE REPUBLIKE CIPRA

I

VLADE REPUBLIKE HRVATSKE

O RAZMJENI I UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

Vlada Republike Cipra i Vlada Republike Hrvatske (u daljnjem tekstu „stranke“),

prepoznajući potrebu za utvrđivanjem pravila o zaštiti klasificiranih podataka koji se u okviru političke, vojne, gospodarske, pravne, znanstvene i tehnološke ili bilo koje druge suradnje uzajamno razmjenjuju u interesu nacionalne sigurnosti, kao i klasificiranih podataka koji nastaju u postupku takve suradnje,

s namjerom da osigureju uzajamnu zaštitu svih klasificiranih podataka koji se razmjenjuju ili zajednički nastaju tijekom suradnje između stranaka,

želeći uspostaviti skup pravila koja uređuju uzajamnu zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju tijekom suradnje između stranaka,

uzimajući u obzir uzajamne interese u zaštiti klasificiranih podataka, u skladu sa zakonodavstvom stranaka,

sporazumjele su se kako slijedi:

**Članak 1.**  
**Predmet**

Predmet ovog Ugovora je osigurati zaštitu klasificiranih podataka koji nastaju ili se uzajamno razmjenjuju između stranaka, ili ugovaratelja, podugovaratelja ili bilo koje druge javne ili privatne pravne osobe ovlaštene za postupanje i pohranu klasificiranih podataka.

## Članak 2. Definicije

Za potrebe ovog Ugovora:

1. „povreda sigurnosti“ označava svaki postupak ili propust koji je u suprotnosti s ovim Ugovorom ili nacionalnim zakonodavstvom stranaka, posljedica kojega može dovesti do neovlaštenog otkrivanja, gubitka, uništenja, pronevjere ili bilo kojeg drugog oblika povrede sigurnosti klasificiranih podataka;
2. „klasificirani ugovor“ označava ugovor između dva ili više ugovaratelja koji sadrži ili uključuje pristup ili čija provedba zahtijeva pristup klasificiranim podacima;
3. „klasificirani podaci“ označava sve podatke, bez obzira na njihov oblik ili prirodu, koje treba zaštititi od neovlaštenog pristupa ili postupanja i kojima je dodijeljen stupanj tajnosti, u skladu s nacionalnim zakonodavstvom stranaka;
4. „nadležno sigurnosno tijelo“ označava svako nadležno tijelo stranaka osim nacionalnih sigurnosnih tijela koje je, u skladu s njihovim nacionalnim zakonodavstvom, odgovorno za provedbu ovog Ugovora;
5. „ugovaratelj“ označava fizičku osobu ili pravnu osobu koja posjeduje pravnu sposobnost sklapanja ili provedbe klasificiranih ugovora;
6. „uvjerenje o sigurnosnoj provjeri pravne osobe“ označava pozitivnu odluku nacionalnog sigurnosnog tijela koja potvrđuje, u skladu s nacionalnim zakonodavstvom stranaka, da fizička osoba ili pravna osoba ima ovlašten za pristup i postupanje s klasificiranim podacima do određenog stupnja tajnosti;
7. „nacionalno sigurnosno tijelo“ označava tijelo svake stranke iz članka 4. ovog Ugovora koje je odgovorno za provedbu i nadzor ovog Ugovora;
8. „nužnost pristupa podacima za obavljanje poslova iz djelokruga“ označava načelo prema kojem je pristup određenom klasificiranom podatku omogućen isključivo u okviru određenog radnog mjesta i za obavljanje određenog zadatka;
9. „uvjerenje o sigurnosnoj provjeri osobe“ označava pozitivnu odluku nacionalnog sigurnosnog tijela koja potvrđuje, u skladu s nacionalnim zakonodavstvom stranaka, da fizička osoba ispunjava uvjete za pristup i postupanje s klasificiranim podacima do određenog stupnja tajnosti;

10. „stranka pošiljateljica“ označava stranku koja stvara i ustupa klasificirane podatke stranci primateljici;

11. „stranka primateljica“ označava stranku kojoj se prenose klasificirani podaci stranke pošiljateljice;

12. „stupanj tajnosti“ označava kategoriju koja, u skladu s nacionalnim zakonodavstvom stranaka, odgovara stupnju ograničenja pristupa klasificiranim podacima i minimalnom stupnju njihove zaštite;

13. „treća strana“ označava bilo koju državu, organizaciju, fizičku ili pravnu osobu koja nije stranka ovog Ugovora;

### Članak 3. Stupnjevi tajnosti

Stranke su suglasne da su sljedeći stupnjevi tajnosti i oznake istoznačni i odgovaraju stupnjevima tajnosti u njihovom nacionalnom zakonodavstvu:

Za Republiku Cipar	Za Republiku Hrvatsku	Istoznačnica na engleskom jeziku
ΑΚΡΟΣ ΑΠΟΡΡΗΤΟ	VRLO TAJNO	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	POVJERLJIVO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	OGRANIČENO	RESTRICTED

### Članak 4. Nacionalna sigurnosna tijela

1. Nacionalna sigurnosna tijela stranaka su:

za Republiku Cipar:  
Nacionalno sigurnosno tijelo (NSA)  
Ministarstvo obrane Republike Cipra;

za Republiku Hrvatsku:  
Ured Vijeća za nacionalnu sigurnost.

2. Stranke obavješćuju jedna drugu diplomatskim putem o svim promjenama nacionalnih sigurnosnih tijela.

3. Nacionalna sigurnosna tijela obavješćuju jedno drugo o svom nacionalnom zakonodavstvu vezano uz klasificirane podatke i o bilo kojim njegovim značajnim izmjenama i dopunama te razmjenjuju informacije o sigurnosnim standardima, postupcima i praksama za zaštitu klasificiranih podataka.

4. Na zahtjev, nacionalna sigurnosna tijela obavješćuju jedno drugo o drugim nadležnim sigurnosnim tijelima.

### Članak 5.

#### Mjera zaštite i pristup klasificiranim podacima

1. U skladu sa svojim nacionalnim zakonodavstvom, stranke poduzimaju sve potrebne mjere za zaštitu klasificiranih podataka koji su nastali ili su razmijenjeni u skladu s ovim Ugovorom. Klasificiranim podacima nastalim ili ustupljenim u skladu s ovim Ugovorom stranke pružaju jednaku razinu zaštite koju bi pružili vlastitim klasificiranim podacima istoznačnog stupnja tajnosti, kako je utvrđeno u članku 3. ovog Ugovora.

2. Stranka pošiljateljica obavješćuje:

- a) stranku primateljicu o svim uvjetima ustupanja ili ograničenjima korištenja klasificiranih podataka;
- b) stranku primateljicu, pisanim putem, o svakoj promjeni stupnja tajnosti ustupljenih ili prenesenih klasificiranih podataka.

3. Pristup klasificiranim podacima označenim kao ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO / CONFIDENTIAL i više ograničava se na fizičke osobe i pravne osobe koje posjeduju odgovarajuće uvjerenje o sigurnosnoj provjeri i temeljem nužnosti pristupa podacima za obavljanje poslova iz djelokruga, u skladu s nacionalnim zakonodavstvom stranaka.

4. Uvjerenje o sigurnosnoj provjeri osobe nije potrebno za pristup klasificiranim podacima označenim kao ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / OGRANIČENO / RESTRICTED. Pristup takvim podacima ograničava se na fizičke osobe temeljem nužnosti pristupa podacima za obavljanje poslova iz djelokruga i koje su primjereno informirane o svojoj odgovornosti i obvezi zaštite takvih klasificiranih podataka.

5. U okviru područja primjene ovog Ugovora, svaka stranka priznaje uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe izdana u skladu s nacionalnim zakonodavstvom druge stranke. Uvjerenja o sigurnosnoj provjeri istovjetna su razinama predviđenim u članku 3. ovog Ugovora.

6. Nacionalna sigurnosna tijela, na zahtjev, pomažu jedno drugom u skladu sa svojim nacionalnim zakonodavstvom u provođenju postupaka sigurnosne provjere potrebnih za primjenu ovog Ugovora.

7. U okviru područja primjene ovog Ugovora, nacionalna sigurnosna tijela stranaka bez odgode obavješćuju jedno drugo o svakoj (zmjeni u vezi) s uvjerenjima o sigurnosnoj provjeri osobe i uvjerenjima o sigurnosno provjeri pravne osobe, posebice o povlačenju ili snižavanju stupnja tajnosti.

8. Stranka primateljica:

- a) ustupa klasificirane podatke trećoj strani samo temeljem prethodnog pisanog pristanka stranke pošiljateljice;
- b) označava zaprimljene klasificirane podatke u skladu sa stupnjem tajnosti utvrđenim u članku 3. ovog Ugovora;
- c) koristi klasificirane podatke samo u svrhe za koje su dostavljeni.

#### Članak 6.

#### Prijenos klasificiranih podataka

1. Klasificirani podaci označeni kao ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO / TOP SECRET prenose se putem ovlaštenih državnih tijela u skladu s nacionalnim zakonodavstvom stranaka. Minimalna sigurnosna mjera je da takve klasificirane podatke prenosi, i pod njegovim su isključivim nadzorom, službeni dostavljač koji posjeduje uvjerenje o sigurnosnoj provjeri osobe stupnja ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO / TOP SECRET. Stranka primateljica pisano potvrđuje primitak klasificiranih podataka stupnja tajnosti ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO / TOP SECRET.

2. Klasificirani podaci označeni kao ΑΠΟΡΡΗΤΟ / TAJNO / SECRET prenose se putem ovlaštenih državnih tijela u skladu s nacionalnim zakonodavstvom stranaka, ili na druge sigurne načine koje su uzajamno odobrila sigurnosna tijela objiju stranaka. Stranka primateljica pisanim putem potvrđuje primitak klasificiranih podataka stupnja tajnosti ΑΠΟΡΡΗΤΟ / TAJNO / SECRET.

3. Klasificirani podaci označeni kao ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO / CONFIDENTIAL prenose se putem ovlaštenih državnih tijela u skladu s nacionalnim zakonodavstvom stranaka, ili na druge sigurne načine koje su uzajamno odobrila sigurnosna tijela objiju stranaka. Stranka primateljica pisanim putem potvrđuje primitak klasificiranih podataka stupnja tajnosti ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO / CONFIDENTIAL.

4. Klasificirani podaci označeni kao ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / OGRANIČENO / RESTRICTED prenose se sigurnim načinom u skladu s nacionalnim zakonodavstvom stranaka.

5. Postupak za prijevoz velikih pošiljki koje sadrže klasificirane podatke zajednički procjenjuju i dogovaraju, za svaki pojedini slučaj, nacionalna sigurnosna tijela obiju stranaka.

6. Kada je među strankama potreban prijenos klasificiranih podataka označenih kao ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / OGRANIČENO / RESTRICTED, ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO / CONFIDENTIAL ili ΑΠΟΡΡΗΤΟ / TAJNO / SECRET elektroničkim putem, oni se prenose kriptirani. Elektronički prijenos ovih specifičnih stupnjeva tajnosti provodi se certificiranim kriptografskim sredstvima koja su uzajamno odobrila nacionalna sigurnosna tijela.

7. Glavne točke ulaza i izlaza za razmjenu klasificiranih podataka u skladu s ovim Ugovorom su:

za Republiku Cipar:

Središnji registar VRLO TAJNO u Ministarstvu vanjskih poslova;

za Republiku Hrvatsku:

Središnji registar VRLO TAJNO u Uredu Vijeća za nacionalnu sigurnost.

8. Ne dovodeći u pitanje stavak 7. ovog članka, kada god snage sigurnosti razmjenu klasificiranih podataka smatraju nužnom, ta se razmjena provodi u skladu s njihovim nacionalnim zakonodavstvom.

9. Glavne točke prijema i slanja za ovu kategoriju klasificiranih podataka dogovaraju snage sigurnosti, a razmjena se provodi na temelju prethodnog pisanog pristanka i odobrenja u skladu s nacionalnim zakonodavstvom stranaka.

10. Ako postoji potreba, obavještajne službe stranaka mogu, u skladu s nacionalnim zakonodavstvom, neposredno razmjenjivati operativne i obavještajne informacije.

#### **Članak 7.**

##### **Umnožavanje i prevođenje klasificiranih podataka**

1. Prevođenje i umnožavanje klasificiranih podataka provodi se u skladu s nacionalnim zakonodavstvom stranke primateljice.

2. Klasificirani podaci označeni kao ΑΠΟΡΡΗΤΟ / TAJNO / SECRET ili ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO / TOP SECRET prevode se ili umnožavaju samo uz prethodni pisani pristanak stranke pošiljateljice.

3. Svi umnoženi primjerci klasificiranih podataka označavaju se kao izvorni klasificirani podaci.

4. Takvi umnoženi klasificirani podaci štite se na isti način kao izvorni klasificirani podaci.

5. Broj umnoženih primjeraka klasificiranih podataka ograničen je na broj potreban za službene svrhe.

6. Prijevod se označava izvornom oznakom stupnja tajnosti i nosi primjerenu bilješku na jeziku prijevoda koja ukazuje na to da prijevod sadrži klasificirane podatke primljene od stranke pošiljateljice.

#### Članak 8.

##### Uništavanje klasificiranih podataka

1. Klasificirani podaci uništavaju se na način koji onemogućava njihovo djelomično ili potpuno obnavljanje.

2. Klasificirani podaci označeni do stupnja tajnosti ΑΠΟΡΡΗΤΟ / TAJNO / SECRET uništavaju se u skladu s nacionalnim zakonodavstvom stranaka.

3. Klasificirani podaci označeni stupnjem tajnosti ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO / TOP SECRET ne uništavaju se. Oni se vraćaju stranici pošiljateljici.

4. Izvješće o uništavanju klasificiranih podataka sastavljeno na engleskom jeziku dostavlja se nacionalnom sigurnosnom tijelu ili bilo kojem drugom nadležnom sigurnosnom tijelu stranke pošiljateljice.

5. U kriznoj situaciji u kojoj nije moguće zaštititi ili vratiti klasificirane podatke razmijenjene ili nastale u skladu s ovim Ugovorom, klasificirani podaci se odmah uništavaju. Stranka primateljica, što je prije moguće, obavješćuje nacionalno sigurnosno tijelo ili bilo koje drugo nadležno sigurnosno tijelo stranke pošiljateljice o tom uništavanju.



## Članak 9. Klasificirani ugovori

1. Klasificirani ugovori sklapaju se i provode u skladu s nacionalnim zakonodavstvom svake stranke.

2. Nacionalno sigurnosno tijelo jedne stranke dostavlja nacionalnom sigurnosnom tijelu druge stranke prethodnu pisanu potvrdu da ugovaratelj ili podugovaratelj koji želi sklopiti klasificirani ugovor s drugom strankom označen stupnjem tajnosti ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO / CONFIDENTIAL ili/ ΑΠΟΡΡΗΤΟ / TAJNO / SECRET, posjeduje ili je u postupku dobivanja uvjerenja o sigurnosnoj provjeri pravne osobe odgovarajućeg stupnja tajnosti.

3. Sigurnosni prilog kojim stranka pošiljateljica pobliže određuje koji klasificirani podaci se ustupaju stranci primateljici, koji je stupanj tajnosti dodijeljen tim podacima i koje su obveze ugovaratelja u vezi zaštite klasificiranih podataka, sastavni je dio svakog klasificiranog ugovora ili podugovora.

4. Svaki klasificirani ugovor sklopljen u skladu s ovim Ugovorom uključuje:

- a) obvezu ugovaratelja ili podugovaratelja da osigura da njegovi prostori zadovoljavaju potrebne uvjete za postupanje i pohranu klasificiranih podataka određenog stupnja tajnosti;
- b) obvezu ugovaratelja ili podugovaratelja da osigura da su osobe koje obavljaju poslove koji zahtijevaju pristup klasificiranim podacima propisno ovlaštene za pristup klasificiranim podacima odgovarajućeg stupnja tajnosti u skladu sa svojim nacionalnim zakonodavstvom i da su redovito sigurnosno informirane;
- c) obvezu obavješćivanja o svakoj promjeni stupnja tajnosti klasificiranih podataka u skladu sa svojim nacionalnim zakonodavstvom;
- d) popis klasificiranih podataka i popis prostora u kojima se s klasificiranim podacima može postupati i pohranjivati ih;
- e) postupak za prijenos klasificiranih podataka;
- f) obvezu ugovaratelja ili podugovaratelja da obavijesti svoje nadležno nacionalno sigurnosno tijelo o svakoj stvarnoj povredi sigurnosti ili sumnji u povredu sigurnosti, u skladu sa svojim nacionalnim zakonodavstvom;

- g) obvezu ugovaratelja ili podugovaratelja da proslijedi primjerak klasificiranog ugovora nacionalnom sigurnosnom tijelu objiju stranaka;
- h) obvezu podugovaratelja da ispuni iste sigurnosne obveze kao i ugovaratelj.

5. Čim između mogućih ugovaratelja započinu pregovori koji prethode ugovoru, nacionalno sigurnosno tijelo stranke pošiljateljice obavješćuje nacionalno sigurnosno tijelo druge stranke o stupnju tajnosti koji je dodijeljen klasificiranim podacima koji se odnose na te pregovore koji prethode ugovoru.

6. Primjerak svakog klasificiranog ugovora prosjeđuje se nacionalnom sigurnosnom tijelu stranke gdje će se posao obavljati, kako bi se omogućio primjereni sigurnosni nadzor i kontrola.

#### Članak 10. Posjeti

1. Posjeti vezani uz klasificirane ugovore i koji uključuju pristup klasificiranim podacima podliježu prethodnom pisanom odobrenju nacionalnog sigurnosnog tijela stranke domaćina.
2. Nacionalno sigurnosno tijelo stranke domaćina prima zahtjev za posjet najmanje deset dana unaprijed.
3. U žurnim slučajevima, zahtjev za posjet može se podnijeti u kraćem vremenu.
4. Zahtjev za posjet uključuje:
  - a) ime i prezime posjetitelja, mjesto i datum rođenja, državljanstvo, broj putovnice ili druge identifikacijske isprave;
  - b) ime pravne osobe koju posjetitelj predstavlja i radno mjesto posjetitelja u pravnoj osobi;
  - c) ime, adresu i kontakt podatke pravne osobe i objekata koji se žele posjetiti;
  - d) potvrdu o posjedovanju uvjerenja o sigurnosnoj provjeri posjetitelja, njegov rok valjanosti i stupanj;

- e) cilj i svrhu posjete i najviši stupanj tajnosti klasificiranih podataka koji će biti uključeni;
- f) očekivani datum i trajanje zatražene posjete. U slučaju višekratnih posjeta, navodi se ukupno razdoblje pokriveno posjetima;
- g) datum, potpis i otisak službenog pečata mjerodavnog nacionalnog sigurnosnog tijela.

5. Kada je posjet odobren, nacionalno sigurnosno tijelo stranke domaćina dostavlja primjerak zahtjeva za posjet savjetnicima za informacijsku sigurnost pravne osobe koju će se posjetiti.

6. Valjanost odobrenja za posjet ne smije prelaziti jednu godinu.

7. Nacionalna sigurnosna tijela stranaka mogu sastaviti popise pojedinaca koji imaju ovlast za višekratne posjete. Ti popisi valjani su tijekom početnog razdoblja od dvanaest mjeseci. Uvjeti pojedinih posjeta izravno se dogovaraju s odgovarajućim kontaktima u pravnoj osobi koju pojedinci posjećuju, u skladu s dogovorenim uvjetima.

#### Članak 11.

##### Povreda sigurnosti

1. U slučaju stvarne povrede sigurnosti ili sumnje u povredu sigurnosti nacionalno sigurnosno tijelo stranke primateljice, što je prije moguće, obavješćuje nacionalno sigurnosno tijelo stranke pošiljateljice i, u skladu sa svojim nacionalnim zakonodavstvom, pokreće odgovarajući postupak kako bi se utvrdile okolnosti povrede sigurnosti. Rezultati postupka i završno izvješće o uzrocima i razmjerima štete dostavljaju se nacionalnom sigurnosnom tijelu stranke pošiljateljice.

2. Ako se povreda sigurnosti dogodi u trećoj zemlji, nacionalno sigurnosno tijelo stranke koja je podatak ustupila trećoj zemlji poduzima sve nužne mjere kako bi osigurala pokretanje postupaka propisanih u stavku 1. ovog članka.

3. Stranka pošiljateljica, na zahtjev, surađuje u postupcima u skladu sa stavkom 1. ovog članka.

## Članak 12. Troškovi

Svaka stranka snosi svoje vlastite troškove koji nastanu uslijed provedbe i nadzora ovog Ugovora.

## Članak 13. Rješavanje sporova

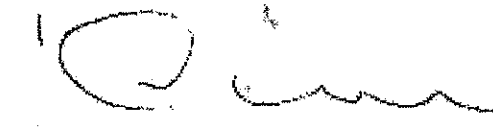
Svaki spor u vezi s tumačenjem ili primjenom ovog Ugovora rješavat će se pregovorima između stranaka.

## Članak 14. Završne odredbe

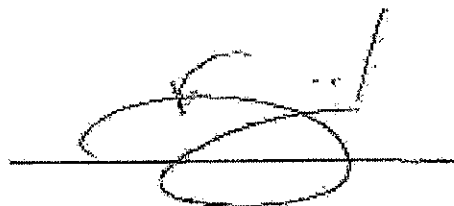
1. Ovaj Ugovor sklapa se na neodređeno vrijeme i stupa na snagu prvog dana drugog mjeseca nakon datuma primitka posljednje pisane obavijesti kojom su stranke obavijestile jedna drugu, diplomatskim putem, da su ispunjeni njihovi unutarnji pravni uvjeti potrebni za njegovo stupanje na snagu.
2. Ovaj Ugovor može se izmijeniti i dopuniti uzajamnim pisanim pristankom stranaka. Izmjene i dopune stupaju na snagu u skladu sa stavkom 1. ovog članka.
3. Svaka stranka može, u bilo koje vrijeme, okončati ovaj Ugovor pisanom obavješću drugoj stranci diplomatskim putem. U tom slučaju, okončanje proizvodi učinak šest (6) mjeseci od datuma na koji je druga stranka primila obavijest o okončanju.
4. U slučaju prestanka ovog Ugovora, svi klasificirani podaci razmijenjeni u skladu s ovim Ugovorom nastavljaju se štiti u skladu s ovdje utvrđenim odredbama i vraćaju se stranci pošiljateljici.
5. Stranka u čijoj je državi ovaj Ugovor sklopljen započinje postupak u vezi s registracijom ovog Ugovora pri Tajništvu Ujedinjenih naroda, u skladu s člankom 102. Povelje Ujedinjenih naroda, odmah po njegovom stupanju na snagu. Druga stranka obavješćuje se o registraciji i o broju registracije pri UN-u, čim Tajništvo Ujedinjenih naroda potvrdi registraciju.

Sastavljeno u Zagrebu dana 4. listopada 2001. u dva izvornika, svaki na grčkom, hrvatskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

ZA VLADU  
REPUBLIKE CIPRA



ZA VLADU  
REPUBLIKE HRVATSKE



ΜΕΡΟΣ ΙΙΙ  
(Κείμενο στην αγγλική γλώσσα)

**AGREEMENT  
BETWEEN  
THE GOVERNMENT OF THE REPUBLIC OF CYPRUS  
AND  
THE GOVERNMENT OF THE REPUBLIC OF CROATIA  
ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED  
INFORMATION**

The Government of the Republic of Cyprus and the Government of the Republic of Croatia (hereinafter referred to as "the Parties").

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

Intending to ensure the mutual protection of all Classified Information, which has been exchanged or jointly generated in the course of cooperation between the Parties,

Desiring to establish a set of rules regulating the mutual protection of Classified Information exchanged or generated in the course of the cooperation between the Parties,

Considering the mutual interests in the protection of Classified Information, in accordance with the legislation 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 generated or mutually exchanged between the Parties, or contractors, sub-contractors or any other public or private legal entity authorised to handle and store Classified Information.

## Article 2 Definitions

For the purposes of this Agreement:

1. **"Breach of Security"** means any act or an omission which is contrary to this Agreement or to the national legislation of the Parties, the result of which may lead to an unauthorised disclosure, loss, destruction, misappropriation or any other type of breach of Classified Information;
2. **"Classified Contract"** means an agreement between two or more Contractors which contains or involves access to, or the execution of which requires access to Classified Information;
3. **"Classified Information"** means any information, regardless of its form or nature, which requires protection against unauthorised access or manipulation and for which a Security Classification Level has been assigned, in accordance with the national legislation of the Parties;
4. **"Competent Security Authority"** means any competent authority of the Parties other than the National Security Authorities that, in accordance with their national legislation, is responsible for the implementation of this Agreement;
5. **"Contractor"** means a natural person or a legal entity possessing the legal capacity to conclude or undertake classified contracts;
6. **"Facility Security Clearance"** means the positive decision of the National Security Authority confirming, in accordance with the national legislation of the Parties, that a natural person or a legal entity is authorised to have access to and handle Classified Information up to a specific classification level;
7. **"National Security Authority"** means the authority of each Party referred to in Article 4 of this Agreement which is responsible for the implementation and supervision of this Agreement;
8. **"Need-to-Know"** means the principle whereby access to specific Classified Information is granted exclusively in the scope of a given official position and for the performance of a specific task;
9. **"Personnel Security Clearance"** means the positive decision by the National Security Authority confirming, in accordance with the national



legislation of the Parties, that the natural person is authorized to have access to and handle Classified Information up to a specific classification level;

10. "Providing Party" means the Party that creates and provides the Classified Information to the Receiving Party;

11. "Receiving Party" means the Party to which Classified Information of the Providing Party is transmitted;

12. "Security Classification Level" means a category, which, in accordance with the national legislation of the Parties, corresponds to the level of restriction of access to Classified Information and to the minimum level of protection;

13. "Third Party" means any state, organization, natural person or legal entity that is not a party to this Agreement.

### 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 specified in their national legislation:

For the Republic of Cyprus	For the Republic of Croatia	Equivalent in English
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	VRLO TAJNO	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	POVJERLJIVO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	OGRANICENO	RESTRICTED

### Article 4 National Security Authorities

1. The National Security Authorities of the Parties are:

For the Republic of Cyprus:  
National Security Authority (NSA)  
Ministry of Defence of the Republic of Cyprus;

For the Republic of Croatia:  
Office of the National Security Council.

2. The Parties shall inform each other through diplomatic channels of any modification of the National Security Authorities.

3. The National Security Authorities shall inform each other of their respective national legislation 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.

4. Upon request, the National Security Authorities shall notify each other about the other Competent Security Authorities.

#### Article 5

##### Protection Measures and Access to Classified Information

1. In accordance with their national legislation, the Parties shall take all necessary measures for the protection of Classified Information that is created or exchanged under this Agreement. The Parties shall afford to Classified Information created and/or provided under this Agreement the same level of protection as they would to their own Classified Information of the equivalent Security Classification Level, as set forth in Article 3 of this Agreement.

2. The Providing Party shall inform:

a) The Receiving Party of any conditions of release or limitations on the use of the Classified Information;

b) The Receiving Party in writing about any change of the Security Classification Level of the released or transmitted Classified Information.

3. Access to Classified Information marked as CONFIDENTIAL / ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO and above shall be limited to natural persons and legal entities holding an adequate security clearance and on a Need-to-know basis in accordance with the national legislation of the Parties.

4. A Personnel Security Clearance is not required for access to Classified Information marked as RESTRICTED / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / OGRANICENO. Such access shall be limited to natural persons on a Need-to-Know basis and who have been appropriately briefed on their responsibilities and obligations to protect such Classified Information.

5. Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearances and Facility Security Clearances granted in

accordance with the national legislation of the other Party. The security clearances shall be equivalent to the levels provided in Article 3 of this Agreement.

6. The National Security Authorities shall assist each other upon request in accordance with their respective national legislation in carrying out vetting procedures necessary for the application of this Agreement.

7. Within the scope of this Agreement, the National Security Authorities of the Parties shall inform each other without delay about any alteration with regard to Personnel Security Clearances and Facility Security Clearances, in particular about withdrawal or downgrading of the Security Classification Level.

8. The Receiving Party shall:

- a) Release Classified Information to a Third Party only upon prior written consent of the Providing Party;
- b) Mark the received Classified Information in accordance with the Security Classification Level as set forth in Article 3 of this Agreement;
- c) Use Classified Information solely for the purposes that it has been provided for.

#### Article 6 Transmission of Classified Information

1. Classified Information marked as TOP SECRET / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO shall be transmitted through Government to Government channels in accordance with the national legislation of the Parties. As a minimum security level such Classified Information shall be carried by and under the sole control of an official courier holding a Personnel Security Clearance to TOP SECRET / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO level. The Receiving Party shall confirm the receipt of TOP SECRET / ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / VRLO TAJNO Classified Information in writing.

2. Classified Information marked as SECRET / ΑΠΟΡΡΗΤΟ / TAJNO shall be transmitted through Government to Government channels in accordance with the national legislation of the Parties, or through other secure channels mutually approved by the Security Authorities of both Parties. The Receiving

Party shall confirm the receipt of SECRET / ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ Classified Information in writing.

3. Classified Information marked as CONFIDENTIAL / ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO shall be transmitted through Government to Government channels in accordance with the national legislation of the Parties, or through other secure channels mutually approved by the Security Authorities of both Parties. The Receiving Party shall confirm the receipt of CONFIDENTIAL / ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO Classified Information in writing.

4. Classified Information marked as RESTRICTED / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / OGRANIČENO shall be transmitted through secure channels in accordance with the national legislation of the Parties.

5. The procedures for the carriage of large consignments containing Classified Information shall be jointly evaluated and agreed, on a case-by-case basis, by the National Security Authorities of both Parties.

6. If Classified Information marked as RESTRICTED / ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / OGRANIČENO, CONFIDENTIAL / ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO or SECRET / ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ is to be transmitted electronically between the Parties, it shall not be sent in clear text. Electronic transmission of these specific classification levels shall be carried out through certified cryptographic means mutually approved by the National Security Authorities.

7. The main points of entry and exit for the exchange of Classified Information under this Agreement shall be:

For the Republic of Cyprus:  
The Central TOP SECRET Registry at the Ministry of Foreign Affairs;

For the Republic of Croatia:  
The Central TOP SECRET Registry at the Office of the National Security Council;

8. Without prejudice to Paragraph 7 of this Article, whenever deemed necessary by the Security Forces, to exchange Classified Information, this exchange shall be done in accordance with their national legislation.

9. The main points of entry and exit for this category of Classified Information shall be agreed by the Security Forces and the exchange done upon a prior written consent and approval in accordance with the national legislation of the Parties.

10. If necessary, the intelligence services of the Parties may, in accordance with national legislation, exchange operative and intelligence information directly with each other.

#### Article 7

##### Reproduction and Translation of Classified Information

1. Translations and reproductions of Classified Information shall be made in accordance with the national legislation of the Receiving Party.
2. Classified Information marked as SECRET / ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ or TOP SECRET / ΑΚΡΟΣ ΑΠΟΡΡΗΤΟ / VRLO ΤΑΙΝΟ shall be translated or reproduced only upon prior written consent of the Providing Party.
3. All copies of Classified Information shall be marked and protected as the original Classified Information.
4. Such reproduced Classified Information shall be protected in the same way as the original Classified Information.
5. The number of copies of Classified Information shall be limited to that required for official purposes.
6. The translation shall be marked with the original Security Classification Level and shall bear an appropriate annotation in the language of the translation indicating that it contains Classified Information received from the Providing Party.

#### Article 8

##### Destruction of Classified Information

1. Classified Information shall be destroyed in a way that prevents its partial or total reconstruction.
2. Classified Information marked up to SECRET / ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ shall be destroyed in accordance with the national legislation of the Parties.
3. Classified Information marked as TOP SECRET / ΑΚΡΟΣ ΑΠΟΡΡΗΤΟ / VRLO ΤΑΙΝΟ shall not be destroyed. It shall be returned to the Providing Party.
4. The report on the destruction of Classified Information made in the English language shall be delivered to the National Security Authority or any other Competent Security Authority of the Providing Party.

5. In a crisis situation in which it is impossible to protect or return Classified Information exchanged or generated under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall inform the National Security Authority or any other Competent Security Authority of the Providing Party about this destruction as soon as possible.

#### Article 9 Classified Contracts.

1. Classified Contracts shall be agreed and implemented in accordance with the national legislation of each Party.
2. The National Security Authority of a Party shall provide to the National Security Authority of the other Party prior written confirmation that a contractor or a sub-contractor, wishing to undertake a classified contract marked as CONFIDENTIAL / ΕΜΠΙΣΤΕΥΤΙΚΟ / POVJERLJIVO or/and SECRET / ΑΠΟΡΡΗΤΟ / ΤΑΙΝΟ with such other Party, holds or is in the process of obtaining a Facility Security Clearance of the appropriate Security Classification Level.
3. A security annex by which the Providing Party shall specify which Classified Information is to be released to the Receiving Party, which Security Classification Level has been assigned to that information and the Contractor's obligations to protect the Classified Information, shall be an integral part of each Classified Contract or sub-contract.
4. Each Classified Contract concluded in accordance with this Agreement shall include:
  - a) A commitment of the Contractor or sub-contractor to ensure that its premises have the necessary conditions for handling and storing Classified Information of a given Security Classification Level;
  - b) A commitment of the Contractor or sub-contractor to ensure that the persons who perform duties requiring access to Classified Information are duly authorised in accordance with their national legislation to have access to Classified Information of the equivalent Security Classification Level and have been regularly security briefed;
  - c) A commitment to communicate any change in the Security Classification Level of Classified Information in accordance with their national legislation.

- d) A list of Classified Information and a list of areas in which Classified Information can be handled and stored;
- e) The procedure for the transmission of Classified Information;
- f) A commitment of the Contractor or sub-contractor to notify their relevant National Security Authority of any actual or suspected Breach of Security, in accordance with their national legislation;
- g) A commitment of the Contractor or sub-contractor to forward a copy of the Classified Contract to the National Security Authorities of both Parties;
- h) A commitment of the subcontractor to fulfil the same security obligations as the Contractor.

5. As soon as pre-contractual negotiations begin between potential Contractors, the National Security Authority of the Providing Party shall inform the National Security Authority of the other Party of the Security Classification Level given to the Classified Information related to those pre-contractual negotiations.

6. A copy of each Classified Contract shall be forwarded to the National Security Authority of the Party where the work is to be performed, to allow adequate security supervision and control.

#### Article 10 Visits

1. Visits related to Classified Contracts and involving access to Classified Information shall be subject to prior written authorisation given by the National Security Authority of the host Party.

2. The National Security Authority of the host Party shall receive a request for visit at least ten days in advance.

3. In urgent cases, the request for visit can be submitted in shorter time.

4. The request for visit shall include:

- a) Visitor's name and surname, place and date of birth, citizenship, passport 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 and the facility to be visited;
- d) Confirmation of the visitor's Personnel Security Clearance, its validity and level;
- e) Object and purpose of the visit and the highest Security Classification Level of Classified Information to be involved;
- 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) Date, signature and the official seal of the relevant National Security Authority.

5. Once the visit has been approved, the National 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 the visit approval shall not exceed one year.

7. The National Security Authorities of the Parties may draw up lists of individuals authorised to make recurring visits. These lists shall be 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 actual or suspected Breach of Security, the National Security Authority of the Receiving Party shall, as soon as possible, inform the National Security Authority of the Providing Party and, in accordance with its national legislation, initiate appropriate inquiries in order to determine the circumstances of the Breach of Security. The results of the investigations and final report on the causes and degree of damage shall be forwarded to the National Security Authority of the Providing Party.

2. If a Breach of Security occurs in a third country, the National Security Authority of the Party that released the information to the third country shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 of this Article are initiated.

3. The Providing Party shall, upon request, co-operate in the inquiry in accordance with Paragraph 1 of this Article.

#### Article 12 Expenses

Each Party shall bear its own expenses incurred by the implementation 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 internal legal requirements necessary for its entry into force have been fulfilled.

2. This Agreement may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with Paragraph 1 of this Article.

3. Each Party may at any time terminate this Agreement by giving the other Party a written notification, through diplomatic channels. In that case the termination shall become effective six (6) months from the date on which the other Party has received the termination notification.

4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and returned to the Providing Party.

5. The Party in the state of which this Agreement is concluded shall commence the procedure concerning the registration of this Agreement to the Secretariat of the United Nations, in accordance with Article 102 of the Charter of the United Nations, immediately following its entry into force. The other

Party shall be informed of the registration, and the UN registration number, as soon as the registration has been confirmed by the Secretariat of the United Nations.

Done at Zagreb on 4 October 2011 in two originals, each in the Croatian, Greek 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 GOVERNMENT OF  
THE REPUBLIC OF CROATIA

