

ΣΧΕΔΙΟ ΝΟΜΟΥ
ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΜΕ ΤΙΤΛΟ:

**«Κύρωση της Συμφωνίας μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της
Κυβέρνησης της Ιταλικής Δημοκρατίας σχετικά με την αμοιβαία προστασία των
διαβαθμισμένων πληροφοριών»**

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ	
Άρθρο πρώτο	Κύρωση της Συμφωνίας μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της Κυβέρνησης της Ιταλικής Δημοκρατίας σχετικά με την αμοιβαία προστασία των διαβαθμισμένων πληροφοριών
Άρθρο 1	Σκοπός
Άρθρο 2	Ορισμοί
Άρθρο 3	Αρμόδιες Αρχές Ασφαλείας
Άρθρο 4	Επίπεδα Διαβάθμισης Ασφαλείας
Άρθρο 5	Αρχές για την Προστασία των Διαβαθμισμένων Πληροφοριών
Άρθρο 6	Πρόσβαση σε Διαβαθμισμένες Πληροφορίες και Εξουσιοδοτήσεις Ασφαλείας Προσωπικού
Άρθρο 7	Προστασία των Διαβαθμισμένων Πληροφοριών στα Συστήματα Επικοινωνίας και Πληροφοριών
Άρθρο 8	Διαβίβαση Διαβαθμισμένων Πληροφοριών
Άρθρο 9	Αναπαραγωγή, Μετάφραση και Καταστροφή Διαβαθμισμένων Πληροφοριών
Άρθρο 10	Διαβαθμισμένες Συμβάσεις και Εξουσιοδοτήσεις Ασφαλείας Εγκαταστάσεων
Άρθρο 11	Επισκέψεις
Άρθρο 12	Παραβίαση της Ασφάλειας
Άρθρο 13	Εφαρμοστέο Δίκαιο
Άρθρο 14	Δαπάνες
Άρθρο 15	Επίλυση Διαφορών
Άρθρο 16	Τελικές Διατάξεις
Άρθρο δεύτερο	Έναρξη ισχύος

Άρθρο πρώτο
Κύρωση της Συμφωνίας μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της
Κυβέρνησης της Ιταλικής Δημοκρατίας σχετικά με την αμοιβαία προστασία των
διαβαθμισμένων πληροφοριών

Κυρώνεται και έχει την ισχύ που ορίζει η παρ. 1 του άρθρου 28 του Συντάγματος, η Συμφωνία μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της Κυβέρνησης της Ιταλικής Δημοκρατίας σχετικά με την αμοιβαία προστασία των διαβαθμισμένων πληροφοριών, που υπεγράφη στην Αθήνα, την 23η Σεπτεμβρίου 2022, το πρωτότυπο κείμενο της οποίας, στην ελληνική και την αγγλική γλώσσα, έχει ως εξής:

ΣΥΜΦΩΝΙΑ

ΜΕΤΑΞΥ

**ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ
ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ**

ΚΑΙ

**ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ
ΙΤΑΛΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ**

ΣΧΕΤΙΚΑ

**ΜΕ ΤΗΝ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ
ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ
ΠΛΗΡΟΦΟΡΙΩΝ**

Η Κυβέρνηση Της Ελληνικής Δημοκρατίας

και

Η Κυβέρνηση της Ιταλικής Δημοκρατίας

Εφεξής «τα Μέρη»,

ΕΠΙΘΥΜΩΝΤΑΣ να διασφαλίσουν την προστασία των Διαβαθμισμένων Πληροφοριών που ανταλλάσσονται μεταξύ των Μερών, σύμφωνα με τις εθνικές τους νομοθετικές και κανονιστικές διατάξεις και σύμφωνα με τα αντίστοιχα εθνικά συμφέροντα και την ασφάλειά τους, καθώς και τις διεθνείς δεσμεύσεις τους,

ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ την ανάγκη θέσπισης κοινών κανονισμών ασφαλείας για την προστασία των Διαβαθμισμένων Πληροφοριών, μεταξύ άλλων σε σχέση με τις δυνατότητες εφαρμογής τεχνικών συμφωνιών και ανάπτυξης συμβατικών δραστηριοτήτων μεταξύ των Μερών,

Συμφώνησαν ως προς τα εξής:

Άρθρο 1 Σκοπός

Σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις τους και λαμβάνοντας υπόψη τα εθνικά συμφέροντα και την ασφάλεια, καθώς και τις βιομηχανικές δραστηριότητες, τα Μέρη λαμβάνουν όλα τα κατάλληλα μέτρα για να εξασφαλίσουν την προστασία των Διαβαθμισμένων Πληροφοριών που διαβιβάζονται ή δημιουργούνται στο πλαίσιο της παρούσας συμφωνίας.

Άρθρο 2 Ορισμοί

Για τους σκοπούς της παρούσας Συμφωνίας, ισχύουν οι ακόλουθοι ορισμοί:

α) **Διαβαθμισμένες Πληροφορίες:** Κάθε πληροφορία, ανεξάρτητα από τη μορφή της, η οποία διαβιβάζεται/μεταδίδεται μεταξύ των Μερών ή παράγεται/δημιουργείται από αυτά σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις ενός εκ των Μερών, και η οποία, για λόγους εθνικής ασφαλείας, απαιτεί προστασία από μη εξουσιοδοτημένη αποκάλυψη ή άλλου είδους διακινδύνευση, και χαρακτηρίζεται ως τέτοια και επισημαίνεται κατάλληλα.

β) **Αρμόδια Αρχή Ασφαλείας:** Η αρχή η οποία, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις των Μερών, είναι υπεύθυνη για την προστασία των Διαβαθμισμένων Πληροφοριών και για την εφαρμογή της παρούσας συμφωνίας, όπως ορίζεται στο άρθρο 3 παράγραφος 1 της παρούσας συμφωνίας.

γ) **Μέρος Προέλευσης:** Το Συμβαλλόμενο Μέρος, συμπεριλαμβανομένων όλων των προσώπων, νομικών οντοτήτων ή άλλων μορφών οργανισμών που υπάγονται στη δικαιοδοσία του, το οποίο δημιουργεί ή μεταδίδει Διαβαθμισμένες Πληροφορίες.

δ) **Μέρος Παραλαβής:** Το Συμβαλλόμενο Μέρος, συμπεριλαμβανομένων όλων των προσώπων, νομικών οντοτήτων ή άλλων μορφών οργανισμών που υπάγονται στη δικαιοδοσία του, το οποίο λαμβάνει Διαβαθμισμένες Πληροφορίες, από το συμβαλλόμενο Μέρος Προέλευσης.

ε) **Ανάγκη Γνώσης:** Αρχή βάσει της οποίας η πρόσβαση σε Διαβαθμισμένες Πληροφορίες μπορεί να χορηγείται/παρέχεται σε ένα άτομο μόνο σε σχέση με τα επίσημα καθήκοντα ή τις δράσεις του.

στ) **Εξουσιοδότηση Ασφαλείας Προσωπικού:** Έγγραφο που εκδίδεται σύμφωνα με την εθνική νομοθεσία ενός από τα Συμβαλλόμενα Μέρη και το οποίο δηλώνει ότι ένα άτομο είναι εξουσιοδοτημένο να έχει πρόσβαση και να χειρίζεται Διαβαθμισμένες Πληροφορίες, έως το επίπεδο διαβάθμισης ασφαλείας που ορίζεται στο εν λόγω έγγραφο.

ζ) **Εξουσιοδότηση Ασφαλείας Εγκαταστάσεων:** Έγγραφο που εκδίδεται σύμφωνα με την εθνική νομοθεσία ενός από τα Συμβαλλόμενα Μέρη και το οποίο δηλώνει ότι ένας Ανάδοχος είναι σε θέση να προστατεύσει τις Διαβαθμισμένες Πληροφορίες.

η) **Ανάδοχος:** Φυσικό πρόσωπο, νομική οντότητα ή άλλη μορφή οργάνωσης σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις ενός από τα Συμβαλλόμενα Μέρη, εξουσιοδοτημένο να συνάπτει και να εκτελεί Διαβαθμισμένη Σύμβαση.

θ) **Διαβαθμισμένη Σύμβαση:** Σύμβαση της οποίας η εκτέλεση περιλαμβάνει πρόσβαση σε Διαβαθμισμένες Πληροφορίες.

ι) **Τρίτο Μέρος:** Κράτος, συμπεριλαμβανομένων όλων των φυσικών προσώπων, νομικών οντοτήτων ή άλλων μορφών οργανισμών ή διεθνούς οργανισμού που δεν είναι Συμβαλλόμενο Μέρος της παρούσας Συμφωνίας.

ια) **Επίσκεψη:** Πρόσβαση σε δημόσιους ή ιδιωτικούς φορείς, για τους σκοπούς της παρούσας Συμφωνίας, η οποία περιλαμβάνει την πρόσβαση σε Διαβαθμισμένες Πληροφορίες και το χειρισμό τους.

ιβ) **Παραβίαση Ασφάλειας:** Πράξη ή παράλειψη αντίθετη προς τις διατάξεις της παρούσας Συμφωνίας ή/και προς τις εθνικές νομοθετικές και κανονιστικές διατάξεις των Μερών, η οποία μπορεί να οδηγήσει σε άνευ αδείας αποκάλυψη, απώλεια, υπεξαίρεση ή οποιαδήποτε άλλη μορφή διαρροής Διαβαθμισμένων Πληροφοριών.

Άρθρο 3

Αρμόδιες Αρχές Ασφαλείας

(1) Οι Αρμόδιες Αρχές Ασφαλείας που ορίζονται από τα Συμβαλλόμενα Μέρη ως αρμόδιες για τη γενική εφαρμογή και τους σχετικούς ελέγχους όλων των πτυχών της παρούσας Συμφωνίας είναι:

Στην Ελληνική Δημοκρατία

Εθνική Αρχή Ασφαλείας (ΕΑΑ)

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)

Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)

Στην Ιταλική Δημοκρατία:

Προεδρία του Συμβουλίου των Υπουργών
Τμήμα Πληροφοριών Ασφαλείας
Κεντρικό Γραφείο Ασφαλείας/Απορρήτου

(2) Οι Αρμόδιες Αρχές Ασφαλείας ενημερώνουν η μια την άλλη για κάθε άλλη Αρμόδια Αρχή Ασφαλείας που είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας.

(3) Τα Συμβαλλόμενα Μέρη ενημερώνουν το ένα το άλλο διά της διπλωματικής οδού για κάθε μεταγενέστερη αλλαγή των Αρμόδιων Αρχών Ασφαλείας.

(4) Προκειμένου να επιτευχθούν και να διατηρηθούν συγκρίσιμα πρότυπα ασφάλειας, οι αντίστοιχες Αρμόδιες Αρχές Ασφαλείας παρέχουν αμοιβαία, κατόπιν αιτήματος, πληροφορίες σχετικά με τις διαδικασίες και τις πρακτικές των προτύπων ασφαλείας για την προστασία των Διαβαθμισμένων Πληροφοριών που χρησιμοποιεί το αντίστοιχο Συμβαλλόμενο Μέρος. Εκπρόσωποι των Αρμόδιων Αρχών Ασφαλείας μπορούν να επισκέπτονται οι μεν τους δε προκειμένου να συζητήσουν τις διαδικασίες για την προστασία των Διαβαθμισμένων Πληροφοριών, υπό την προϋπόθεση ότι έχει προηγηθεί κατάλληλη ενημέρωση.

(5) Οι αρμόδιες Αρχές Ασφαλείας διασφαλίζουν την αυστηρή και δεσμευτική τήρηση της παρούσας Συμφωνίας από κάθε δημόσιο ή ιδιωτικό φορέα στα Συμβαλλόμενα Μέρη που υπάγεται στη δικαιοδοσία τους, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις τους.

Άρθρο 4
Επίπεδα Διαβάθμισης Ασφαλείας

(1) Οι Διαβαθμισμένες Πληροφορίες που δημιουργούνται, ανταλλάσσονται/διακινούνται και κοινολογούνται/αποκαλύπτονται στο πλαίσιο της παρούσας Συμφωνίας επισημαίνονται με το κατάλληλο επίπεδο διαβάθμισης ασφαλείας σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις των Μερών.

(2) Τα επίπεδα διαβάθμισης ασφαλείας και τα ισοδύναμά τους για τα Μέρη είναι:

Ελληνική Δημοκρατία	Ιταλική Δημοκρατία	Αγγλική Μετάφραση
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	SEGRETISSIMO	TOP SECRET
ΑΠΟΡΡΗΤΟ	SEGRETO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	RISERVATISSIMO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RISERVATO	RESTRICTED

(3) Το επίπεδο διαβάθμισης ασφαλείας μπορεί να τροποποιηθεί ή να καταργηθεί μόνο από το συμβαλλόμενο Μέρος Προέλευσης. Το Συμβαλλόμενο Μέρος Παραλαβής ενημερώνεται αμέσως και εγγράφως για κάθε αλλαγή ή αφαίρεση του επιπέδου διαβάθμισης ασφαλείας των προηγουμένως παραληφθεισών Διαβαθμισμένων Πληροφοριών.

Άρθρο 5
Αρχές για την Προστασία των Διαβαθμισμένων Πληροφοριών

(1) Το Συμβαλλόμενο Μέρος Παραλαβής παρέχει, σύμφωνα με την εθνική του νομοθεσία, το επίπεδο προστασίας ασφαλείας για τις ληφθείσες Διαβαθμισμένες Πληροφορίες, που παρέχεται στις δικές του Διαβαθμισμένες Πληροφορίες ή ισοδύναμο επίπεδο διαβάθμισης σύμφωνα με τις διατάξεις του Άρθρου 4 παράγραφος 2.

(2) Η Αρμόδια Αρχή Ασφαλείας του Συμβαλλόμενου Μέρους Προέλευσης:

α) εξασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες φέρουν κατάλληλη σήμανση διαβάθμισης ασφαλείας σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις του,

β) ενημερώνει το Συμβαλλόμενο Μέρος Παραλαβής για τυχόν όρους αποκάλυψης/δημοσιοποίησης ή περιορισμούς όσον αφορά τη χρήση των παρεχόμενων Διαβαθμισμένων Πληροφοριών, καθώς και για τυχόν επακόλουθες αλλαγές στη διαβάθμιση ασφαλείας.

(3) Η Αρμόδια Αρχή Ασφαλείας του Μέρους Παραλαβής:

α) εξασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες φέρουν ισοδύναμη σήμανση διαβάθμισης ασφαλείας σύμφωνα με το Άρθρο 4 παράγραφος 2,

β) εξασφαλίζει ότι το επίπεδο διαβάθμισης ασφαλείας δεν μεταβάλλεται, εκτός εάν εγκριθεί εγγράφως από το συμβαλλόμενο Μέρος Προέλευσης,

γ) χρησιμοποιεί Διαβαθμισμένες Πληροφορίες μόνο για τον σκοπό για τον οποίο έχουν δημοσιοποιηθεί και με τους περιορισμούς που αναφέρει το συμβαλλόμενο Μέρος Προέλευσης,

δ) δεν κοινοποιεί/αποκαλύπτει/δημοσιοποιεί Διαβαθμισμένες Πληροφορίες σε Τρίτο Μέρος χωρίς την προηγούμενη γραπτή συγκατάθεση του Μέρους Προέλευσης.

Άρθρο 6
**Πρόσβαση σε Διαβαθμισμένες Πληροφορίες
και Εξουσιοδοτήσεις Ασφαλείας Προσωπικού**

(1) Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται σε άτομα που έχουν Ανάγκη Γνώσης και έχουν λάβει σχετική άδεια σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις κάθε Συμβαλλόμενου Μέρους.

(2) Κατόπιν αιτήματος, οι Αρμόδιες Αρχές Ασφαλείας συνεργάζονται και παρέχουν αμοιβαία συνδρομή κατά τη διάρκεια των διαδικασιών ελέγχου που απαιτούνται για την έκδοση των Εξουσιοδοτήσεων Ασφαλείας Προσωπικού.

(3) Εντός του πεδίου εφαρμογής της παρούσας συμφωνίας, κάθε Συμβαλλόμενο Μέρος αναγνωρίζει τις Εξουσιοδοτήσεις Ασφαλείας Προσωπικού που εκδίδονται σύμφωνα με την εθνική νομοθεσία του άλλου μέρους. Οι Εξουσιοδοτήσεις Ασφαλείας Προσωπικού ισοδυναμούν με τα επίπεδα διαβάθμισης που ορίζονται στην παράγραφο 2 του Άρθρου 4.

(4) Οι Αρμόδιες Αρχές Ασφαλείας ενημερώνουν αμέσως η μια την άλλη για τυχόν αλλαγές όσον αφορά τις αμοιβαίως αναγνωρισμένες Εξουσιοδοτήσεις Ασφαλείας Προσωπικού.

Άρθρο 7

Προστασία των Διαβαθμισμένων Πληροφοριών στα Συστήματα Επικοινωνίας και Πληροφοριών

(1) Κάθε Μέρος διασφαλίζει ότι εφαρμόζονται τα κατάλληλα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών που υποβάλλονται σε επεξεργασία, αποθηκεύονται και διαβιβάζονται μέσω συστημάτων επικοινωνίας και πληροφοριών. Τα μέτρα αυτά διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και, κατά περίπτωση, τη μη άρνηση αναγνώρισης και γνησιότητας των Διαβαθμισμένων Πληροφοριών, καθώς και το κατάλληλο επίπεδο λογοδοσίας και ιχνηλασιμότητας των δράσεων σε σχέση με τις εν λόγω Διαβαθμισμένες Πληροφορίες.

(2) Για τον σκοπό αυτό, τα Συμβαλλόμενα Μέρη διασφαλίζουν ότι οι Διαβαθμισμένες Πληροφορίες που ανταλλάσσονται, αποθηκεύονται, χειρίζονται και διαφυλάσσονται σύμφωνα με τους αντίστοιχους εθνικούς κανόνες και κανονισμούς τους.

(3) Αμφότερα τα Μέρη αναγνωρίζουν αμοιβαία κάθε επίσημη πράξη έγκρισης που αναφέρεται σε εξοπλισμό και μηχανισμούς που σχετίζονται με συστήματα επικοινωνίας και πληροφοριών που εκδίδονται από την Αρμόδια Αρχή Ασφαλείας .

(4) Όταν απαιτείται, ο ενημερωμένος κατάλογος του εγκεκριμένου εξοπλισμού και μηχανισμών ανταλλάσσεται μεταξύ των Αρμόδιων Αρχών Ασφαλείας .

Άρθρο 8

Διαβίβαση Διαβαθμισμένων Πληροφοριών

(1) Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται/μεταδίδονται μεταξύ των Μερών μέσω της διπλωματικής οδού ή μέσω άλλων διαύλων ασφαλείας που έχουν εγκριθεί αμοιβαία από τις Αρμόδιες Αρχές Ασφαλείας τους σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις.

(2) Οι πληροφορίες που έχουν ταξινομηθεί ως ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / **SEGRETISSIMO** / **TOP SECRET** αποστέλλονται μόνο μέσω διπλωματικών και στρατιωτικών διαύλων σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις κάθε Συμβαλλόμενου Μέρους.

(3) Οι πληροφορίες που έχουν ταξινομηθεί ως ΑΠΟΡΡΗΤΟ / **SEGRETO** / **SECRET**, ή **ΕΜΠΙΣΤΕΥΤΙΚΟ** / **RISERVATISSIMO** / **CONFIDENTIAL** ή **ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ** / **RISERVATO** / **RESTRICTED** διαβιβάζονται/μεταδίδονται μέσω κυβερνητικών διαύλων σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις ή μέσω άλλων ασφαλών διαύλων που έχουν εγκριθεί αμοιβαία από τις Αρμόδιες Αρχές Ασφαλείας αμφοτέρων των Μερών.

(4) Σε περίπτωση διαβίβασης/μετάδοσης μεγάλου φορτίου που περιέχει Διαβαθμισμένες Πληροφορίες, οι διαδικασίες μεταφοράς συμφωνούνται από κοινού και αξιολογούνται κατά περίπτωση από τις Αρμόδιες Αρχές Ασφαλείας των Μερών.

Άρθρο 9
Αναπαραγωγή, Μετάφραση και Καταστροφή
Διαβαθμισμένων Πληροφοριών

(1) Όλες οι αναπαραγωγές και μεταφράσεις φέρουν κατάλληλες σημάνσεις διαβάθμισης ασφαλείας και προστατεύονται ως πρωτότυπες Διαβαθμισμένες Πληροφορίες. Οι μεταφράσεις και ο αριθμός των αναπαραγωγών περιορίζονται στο ελάχιστο που απαιτείται για επίσημους σκοπούς.

(2) Όλες οι μεταφράσεις επισημαίνονται με το ίδιο επίπεδο διαβάθμισης με τις πρωτότυπες πληροφορίες και περιέχουν κατάλληλη σημείωση στη γλώσσα της μετάφρασης, αναφέροντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες του Μέρους Προέλευσης.

(3) Οι πληροφορίες που έχουν ταξινομηθεί ως ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / SEGRETISSIMO / TOP SECRET τόσο σε πρωτότυπη μορφή όσο και σε μετάφραση, αναπαράγονται μόνο κατόπιν προηγούμενης γραπτής άδειας του Μέρους Προέλευσης.

(4) Οι πληροφορίες που έχουν ταξινομηθεί ως ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / SEGRETISSIMO / TOP SECRET δεν καταστρέφονται. Επιστρέφονται στο συμβαλλόμενο Μέρος Προέλευσης αφού το Συμβαλλόμενο Μέρος Παραλαβής δεν τις κρίνει πλέον αναγκαίες.

(5) Οι πληροφορίες που έχουν διαβαθμιστεί ως ΑΠΟΡΡΗΤΟ / SEGRETO / SECRET ή με χαμηλότερη διαβάθμιση ασφαλείας, καταστρέφονται σύμφωνα με τις σχετικές εθνικές νομοθετικές και κανονιστικές διατάξεις του Μέρους Παραλαβής, αφού δεν θεωρούνται πλέον αναγκαίες από αυτό. Το Μέρος Παραλαβής ενημερώνει το Συμβαλλόμενο Μέρος Προέλευσης για την εν λόγω καταστροφή.

(6) Οι Διαβαθμισμένες Πληροφορίες καταστρέφονται κατά τρόπο που εμποδίζει τη μερική ή ολική ανακατασκευή τους.

(7) Εάν μια κατάσταση κρίσης καθιστά αδύνατη την προστασία ή την επιστροφή Διαβαθμισμένων Πληροφοριών που ανταλλάσσονται, διαβιβάζονται ή δημιουργούνται δυνάμει της παρούσας συμφωνίας, οι Διαβαθμισμένες Πληροφορίες καταστρέφονται αμέσως. Το Μέρος Παραλαβής ενημερώνει την Αρμόδια Αρχή Ασφαλείας του Συμβαλλόμενου Μέρους Προέλευσης σχετικά με την εν λόγω καταστροφή το συντομότερο δυνατόν.

Άρθρο 10
Διαβαθμισμένες Συμβάσεις και Εξουσιοδοτήσεις Ασφαλείας Εγκαταστάσεων

(1) Πριν από την παροχή πληροφοριών που έχουν ταξινομηθεί ως ΕΜΠΙΣΤΕΥΤΙΚΟ / RISERVATISSIMO / CONFIDENTIAL και άνω, οι οποίες σχετίζονται με Διαβαθμισμένη Σύμβαση με Αναδόχους ή μελλοντικούς Αναδόχους, τα Μέρη Παραλαβής διασφαλίζουν ότι:

α) οι εν λόγω Ανάδοχοι ή οι δυνητικοί Ανάδοχοι και οι εγκαταστάσεις τους έχουν τη δυνατότητα να προστατεύουν επαρκώς τις Διαβαθμισμένες Πληροφορίες,

d) **Receiving Party:** The Party, including all individuals, legal entities or other forms of organizations under its jurisdiction which receives Classified Information, from the Originating Party.

e) **Need-to-know:** A principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties or tasks.

f) **Personnel Security Clearance:** A document issued in accordance with the national legislation of one of the Parties stating that an individual is authorized to access and handle Classified Information, up to the level defined in that document.

g) **Facility Security Clearance:** A document issued in accordance with the national legislation of one of the Parties stating that a Contractor is capable to protect Classified Information.

h) **Contractor:** An individual, a legal entity or other form of organization under the national laws and regulations of one of the Parties, authorized to conclude and perform a Classified Contract.

i) **Classified Contract:** A contract, the performance of which involves access to Classified Information.

j) **Third Party:** A State, including all individuals, legal entities or other forms of organisations or an international organisation that is not a Party to this Agreement.

k) **Visit:** Access to public or private entities, for the purpose of this Agreement, which includes access to and handling of Classified Information.

l) **Security Breach:** An act or omission contrary to the provisions of this Agreement and/or to the national laws and regulations of the Parties, which may result in unauthorised disclosure, loss, misappropriation or any other form of compromise of Classified Information.

Article 3 Competent Security Authorities

(1) The Competent Security Authorities designated by the Parties as responsible for the general implementation and the relevant controls of all aspects of this Agreement are:

In the Hellenic Republic:

NATIONAL SECURITY AUTHORITY (NSA)
Hellenic National Defense General Staff (HNDGS)
Joint Military Intelligence Division (JMID)

In the Italian Republic:

Presidency of the Council of Ministers
Security Intelligence Department
Central Secrecy Office

(2) The Competent Security Authorities shall notify each other of any other Competent Security Authorities responsible for the implementation of this Agreement.

(3) The Parties shall inform each other through diplomatic channels of any subsequent changes of the Competent Security Authorities.

(4) In order to achieve and maintain comparable standards of security, the respective Competent Security Authorities shall, on request, provide each other information about the security standards procedures and practices for the protection of Classified Information employed by the respective Party. Representatives of the Competent Security Authorities may visit each other in order to discuss the procedures for the protection of Classified Information, provided that prior adequate notice is given.

(5) The Competent Security Authorities shall ensure a strict and binding observance of this Agreement by any public or private entity under its jurisdiction of the Parties in accordance with their national laws and regulations.

Article 4 Security Classification Levels

(1) Classified Information generated, exchanged and released under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws and regulations of the Parties.

(2) The security classification levels and their equivalents for the Parties are:

Hellenic Republic	Italian Republic	English Translation
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	SEGRETISSIMO	TOP SECRET
ΑΠΟΡΡΗΤΟ	SEGRETO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	RISERVATISSIMO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RISERVATO	RESTRICTED

(3) The security classification level may be changed or removed only by the Originating Party. The Receiving Party shall be immediately notified in writing of every change or removal of security classification level of previously received Classified Information.

Article 5 Principles for the Protection of Classified Information

(1) The Receiving Party shall, in accordance with its national legislation, afford a level of security protection to received Classified Information as it is afforded to its own Classified Information or equivalent classification level pursuant to the provisions of Article 4, paragraph 2.

(2) The Competent Security Authority of the Originating Party shall:

a) ensure that the Classified Information is marked with an appropriate security classification marking in accordance with its national laws and regulations;

b) inform the Receiving Party of any conditions of release or restrictions on the use of the provided Classified Information, and of any subsequent changes in the security classification.

(3) The Competent Security Authority of the Receiving Party shall:

a) ensure that the Classified Information is marked with an equivalent security classification marking in accordance with paragraph 2 of Article 4;

b) ensure that the security classification level is not changed unless authorized in writing by the Originating Party;

c) use Classified Information only for the purpose for which it has been released and with the limitations stated by the Originating Party;

d) not release Classified Information to a Third Party without the prior written consent of the Originating Party.

Article 6
Access to Classified Information
and Personnel Security Clearances

(1) Access to Classified Information shall be limited to individuals who have a Need-to-Know and have been authorized thereto in accordance with the national laws and regulations of each Party.

(2) On request, the Competent Security Authorities shall cooperate and provide each other assistance during the vetting procedures required for the release of Personnel Security Clearances.

(3) Within the scope of this Agreement, each Party shall recognise the Personnel Security Clearances issued in accordance with the national legislation of the other Party. The Personnel Security Clearances shall be equivalent to the classification levels laid down in paragraph 2 of Article 4.

(4) The Competent Security Authorities shall promptly inform each other of any changes regarding mutually recognised Personnel Security Clearances.

Article 7
Protection of Classified Information
in Communication and Information Systems

(1) Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored and transmitted through communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that Classified Information.

(2) To this end, the Parties shall ensure that Classified Information exchanged will be stored, handled and safeguarded in accordance with their respective national rules and regulations.

(3) Both Parties shall mutually recognise each formal act of approval referring to equipment and mechanisms related to communication and information systems issued by the relevant Competent Security Authority.

(4) When necessary, the updated list of approved equipment and mechanisms shall be exchanged between the Competent Security Authorities.

Article 8 Transmission of Classified Information

(1) Classified Information shall be transmitted between the Parties through diplomatic channels or through other security channels mutually approved by their Competent Security Authorities in accordance with the national laws and regulations.

(2) Information Classified as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / SEGRETISSIMO / TOP SECRET shall be sent only through diplomatic and military channels in accordance with national laws and regulations of each Party.

(3) Information Classified as ΑΠΟΡΡΗΤΟ / SEGRETO / SECRET, or ΕΜΠΙΣΤΕΥΤΙΚΟ/ RISERVATISSIMO / CONFIDENTIAL or ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RISERVATO/ RESTRICTED shall be transmitted through Government to Government channels in accordance with national laws and regulations, or through other secured channels mutually approved by the Competent Security Authorities of both Parties.

(4) In case of transmission of a large consignment containing Classified Information, procedures for transport shall be jointly agreed and evaluated on a case-by-case basis by the Competent Security Authorities of the Parties.

Article 9 Reproduction, Translation and Destruction of Classified Information

(1) All reproductions and translations shall bear appropriate security classification markings and shall be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum required for official purposes.

(2) All translations shall be marked with the same classification level as the original information and shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.

(3) Information Classified as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / SEGRETISSIMO / TOP SECRET both in original form and translation, shall be reproduced only upon prior written permission of the Originating Party.

(4) Information Classified as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / SEGRETISSIMO / TOP SECRET shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Party.

(5) Information classified as ΑΠΟΡΡΗΤΟ / SEGRETO / SECRET or below shall be destroyed in accordance with relevant national laws and regulations of the Receiving Party after it is no longer considered necessary by it. The Receiving Party shall inform the Originating Party of such destruction.

(6) Classified Information shall be destroyed in a way that prevents its partial or total reconstruction.

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

Article 10

Classified Contracts and Facility Security Clearances

(1) Before providing Information Classified as ΕΜΠΙΣΤΕΥΤΙΚΟ / RISERVATISSIMO / CONFIDENTIAL and above which is related to a Classified Contract to Contractors or prospective Contractors, the Receiving Parties shall ensure that:

a) such Contractors or prospective Contractors and their facilities have the capability to protect Classified Information adequately;

b) Contractors or respective sub-Contractors and their facilities hold an appropriate Facility Security Clearance at the adequate level before the execution of the contract;

c) individuals who perform functions requiring access to Classified Information hold an appropriate Personnel Security Clearance;

d) individuals having access to the Classified Information are informed of their responsibilities and obligations to protect the Information in accordance with the relevant laws and regulations of the Receiving Party.

(2) Each Competent Security Authority may request assessment visits to be carried out by the Competent Security Authority of the other Party at private or public facilities handling Classified Information exchanged pursuant to this Agreement, in order to ensure that best practices are employed and security standards are observed, in accordance with national laws and regulations as well as the present Agreement. Such visits are mutually agreed by the Parties in advance.

(3) A Classified Contract shall contain provisions related to the security requirements, classification of each aspect or element of the Classified Contract, and a specific reference to this Agreement. A copy of such document shall be submitted to the Competent Security Authorities of the Parties.

(4) The Parties shall mutually recognise their Facility Security Clearances.

(5) The Competent Security Authorities shall promptly inform each other about any changes regarding mutually recognised Facility Security Clearances.

Article 11 **Visits**

(1) Individuals arriving on a visit to the territory of the State of the other Party for the purposes of this Agreement shall be allowed access to Classified Information to the necessary extent, only after receiving a prior written permission issued by the hosting Party.

(2) The permission referred to in Paragraph 1 shall be granted exclusively to the persons authorized to access to Classified Information pursuant to the national legislation of the Party delegating such persons.

(3) A request for visit shall be submitted to relevant Competent Security Authority of the hosting Party at least 30 days prior to the commencement of the visit.

(4) The request for visit shall include the following data, that shall be used for the purpose of the visit only:

a) the visitor's name and surname date and place of birth, nationality, passport or ID number;

b) the visitor's position with the specifications of the employer which the visitor represents;

c) a specification of the project in which the visitor participates in;

d) if required, confirmation of the visitor's Personnel Security Clearance, its validity and level;

e) the name, address, phone/fax number, e-mail and point of contact of the facility to be visited;

f) the purpose of the visit including the highest security classification level of Classified Information to be involved;

g) the date and duration of the visit. In case of recurring visits, the total period covered by the visit shall be stated;

h) the date and signature and the official seal of the sending Competent Security Authority.

(5) In urgent cases, the Competent Security Authorities can agree on a shorter period for the submission of the request for Visit;

(6) The Competent Security Authorities may agree on the list of visitors entitled to recurring visits. The list shall be valid for a period not exceeding 12 months. Requests for recurring visits shall be submitted in accordance with the paragraph 2 of this Article. Once the list has been approved, Visits may be arranged directly between the facilities involved.

(7) Each Party shall guarantee the protection of Personal Data of the visitors according to its respective national legislation.

Article 12 Breach of Security

(1) In case a Security Breach results in unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such, the Competent Security Authority of the Receiving Party shall inform in writing, once it is aware of such Security Breach, the Competent Security Authority of the Originating Party and initiate appropriate investigations.

(2) The Competent Party shall undertake all measures, in accordance with its national laws and regulations, so as to limit the consequences of the Security Breach referred to in paragraph 1 of this Article and to prevent further Security Breaches. On request, the other Party shall provide appropriate assistance. The Originating Party shall be informed of the outcome of the proceedings and the measures undertaken due to the Security Breach.

(3) When the Security Breach occurs in a Third Party, the Competent Security Authority of the sending Party shall take the actions referred to in paragraph 2 of this Article without undue delay.

(4) The Competent Security Authorities shall inform each other without undue delay of exceptional security risks that may endanger the Classified Information released by the Parties.

Article 13 Applicable Law

This Agreement shall be implemented in accordance with national laws and regulations of the Parties, as well as applicable international law and the obligations arising from Greece's and Italy's membership of the European Union.

Article 14 Expenses

Each Party shall bear its own costs regarding the implementation of this Agreement without exceeding its ordinary budget availability.

Article 15 Settlement of Disputes

Any dispute regarding the interpretation and/or application of this Agreement shall be settled by direct consultations and negotiations between the Parties. Pending settlement procedures, the Parties shall continue to comply with the provisions set forth in this Agreement.

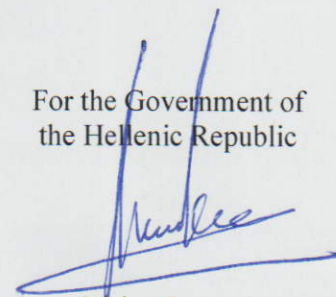
Article 16
Final Provisions

- (1) This Agreement shall enter into force on the first day of the second month from the date of the receipt of the last of the two written notifications by which the Parties have informed each other, through diplomatic channels, that the internal legal requirements necessary for its entry into force have been fulfilled.
- (2) This Agreement may be amended by the mutual written consent of the Parties. Amendments shall enter into force in accordance with the terms set out in paragraph 1 of this Article.
- (3) This Agreement is concluded for an indefinite period of time. Either Party may terminate the Agreement giving the other Party notice in writing through diplomatic channels. In such a case, the Agreement shall cease to be in force six months from the date of receipt by the other Party of the termination notice.
- (4) In case of termination of this Agreement, all Classified Information, transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and upon request returned, to the Providing Party.
- (5) The Competent Security Authorities may conclude implementing arrangements for the implementation of this Agreement.

In witness whereof the undersigned, being duly authorised to this effect, have signed this Agreement.

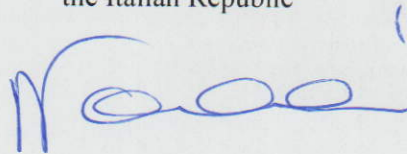
Done at Athens on 23 September 2022 in two originals, each in the Greek, Italian and English languages, all texts being equally authentic. In case of any divergence of interpretation the text in English shall prevail.

For the Government of
the Hellenic Republic



Major General
Konstantinos Kolokotronis

For the Government of
the Italian Republic



H.E. Patrizia Falcinelli

Άρθρο δεύτερο

Έναρξη ισχύος

Η ισχύς του παρόντος νόμου αρχίζει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως και της Συμφωνίας που κυρώνεται, από την πλήρωση των προϋποθέσεων του άρθρου 16 αυτής.

Αθήνα, 17 Απριλίου 2026

**ΕΘΝΙΚΗΣ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ
ΟΙΚΟΝΟΜΙΚΩΝ**

**ΟΙ ΥΠΟΥΡΓΟΙ
ΕΞΩΤΕΡΙΚΩΝ**

ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

ΚΥΡΙΑΚΟΣ ΠΙΕΡΡΑΚΑΚΗΣ

ΓΕΩΡΓΙΟΣ ΓΕΡΑΠΕΤΡΙΤΗΣ

ΝΙΚΟΛΑΟΣ – ΓΕΩΡΓΙΟΣ
ΔΕΝΔΙΑΣ

ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΠΟΛΙΤΗ

ΑΝΑΠΤΥΞΗΣ

ΔΙΚΑΙΟΣΥΝΗΣ

ΜΙΧΑΗΛ ΧΡΥΣΟΧΟΪΔΗΣ

ΠΑΝΑΓΙΩΤΗΣ ΘΕΟΔΩΡΙΚΑΚΟΣ

ΓΕΩΡΓΙΟΣ ΦΛΩΡΙΔΗΣ