

ΣΧΕΔΙΟ ΝΟΜΟΥ
ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΜΕ ΤΙΤΛΟ

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

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ	
Άρθρο πρώτο	Κύρωση Συμφωνίας
Άρθρο 1	Σκοπός
Άρθρο 2	Ορισμοί
Άρθρο 3	Αρμόδιες αρχές ασφαλείας
Άρθρο 4	Επίπεδα διαβάθμισης ασφαλείας
Άρθρο 5	Πρόσβαση σε διαβαθμισμένες πληροφορίες
Άρθρο 6	Προστασία των διαβαθμισμένων πληροφοριών
Άρθρο 7	Περιορισμός για τη χρήση των διαβαθμισμένων πληροφοριών
Άρθρο 8	Διαβίβαση των διαβαθμισμένων πληροφοριών
Άρθρο 9	Αναπαραγωγή, μετάφραση και καταστροφή των διαβαθμισμένων πληροφοριών
Άρθρο 10	Διαβαθμισμένες συμβάσεις
Άρθρο 11	Επισκέψεις
Άρθρο 12	Συνεργασία για την προστασία των διαβαθμισμένων πληροφοριών
Άρθρο 13	Παραβίαση της ασφάλειας
Άρθρο 14	Έξοδα
Άρθρο 15	Επίλυση των διαφορών
Άρθρο 16	Τελικές ρήτρες
Άρθρο δεύτερο	Έναρξη ισχύος

Άρθρο πρώτο
Κύρωση Συμφωνίας

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 Δημοκρατίας της Σλοβενίας σχετικά με την αμοιβαία προστασία των ανταλλασσόμενων διαβαθμισμένων πληροφοριών, που υπεγράφη, στην Αθήνα την 4η Οκτωβρίου 2021, το πρωτότυπο κείμενο της οποίας, στην ελληνική και την αγγλική γλώσσα, έχει ως εξής:

ΣΥΜΦΩΝΙΑ

μεταξύ

**ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ
ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ**

και

**ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ
ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΣΛΟΒΕΝΙΑΣ**

**ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ
ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ
ΤΩΝ ΑΝΤΑΛΛΑΣΣΟΜΕΝΩΝ
ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ
ΠΛΗΡΟΦΟΡΙΩΝ**

Η Κυβέρνηση της Ελληνικής Δημοκρατίας

και

η Κυβέρνηση της Δημοκρατίας της Σλοβενίας

εφεξής «τα Μέρη»,

Επιθυμώντας να διασφαλίσουν την προστασία των Διαβαθμισμένων Πληροφοριών που ανταλλάσσονται μεταξύ των Μερών ή μεταξύ δημόσιων και ιδιωτικών φορέων που υπάγονται στη δικαιοδοσία τους,

Όσον αφορά τα εθνικά συμφέροντα και την ασφάλεια των Συμβαλλομένων Κρατών,

Συμφώνησαν τα εξής:

ΑΡΘΡΟ 1

ΣΚΟΠΟΣ

Τα Μέρη, σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς τους, λαμβάνουν όλα τα κατάλληλα μέτρα για να διασφαλίσουν την προστασία των Διαβαθμισμένων Πληροφοριών που μεταδίδονται ή δημιουργούνται βάσει της παρούσας Συμφωνίας.

ΑΡΘΡΟ 2

ΟΡΙΣΜΟΙ

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

Διαβαθμισμένες Πληροφορίες: οποιεσδήποτε πληροφορίες, ανεξάρτητα από τη μορφή τους, που μεταδίδονται ή δημιουργούνται μεταξύ των Μερών σύμφωνα με τους εθνικούς νόμους και κανονισμούς οποιουδήποτε Μέρους και οι οποίες, προς το συμφέρον της εθνικής ασφάλειας, απαιτούν προστασία από μη εξουσιοδοτημένη αποκάλυψη ή άλλη διακινδύνευση, και χαρακτηρίζονται ως τέτοιες και επισημαίνονται κατάλληλα,

Μέρος Προέλευσης: το Μέρος, συμπεριλαμβανομένων τυχόν δημόσιων ή ιδιωτικών φορέων που υπάγονται στη δικαιοδοσία του, το οποίο διαβιβάζει Διαβαθμισμένες Πληροφορίες στο Μέρος Παραλαβής,

Μέρος Παραλαβής: το Μέρος, συμπεριλαμβανομένων τυχόν δημόσιων ή ιδιωτικών φορέων που υπάγονται στη δικαιοδοσία του, το οποίο λαμβάνει Διαβαθμισμένες Πληροφορίες από το Μέρος Προέλευσης,

Ανάγκη Γνώσης: σημαίνει μια αρχή βάσει της οποίας η πρόσβαση σε Διαβαθμισμένες Πληροφορίες μπορεί να παρέχεται σε ένα άτομο μόνο σε σχέση με τα επίσημα καθήκοντα ή τις δράσεις του,

Έλεγχος Ασφάλειας Προσωπικού: προσδιορισμός, μετά από διαδικασία διαβάθμισης ασφάλειας σύμφωνα με τους εθνικούς νόμους και κανονισμούς, βάσει του οποίου ένα άτομο δικαιούται να έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες έως ένα συγκεκριμένο επίπεδο διαβάθμισης ασφαλείας,

Έλεγχος Ασφάλειας Εγκαταστάσεων: προσδιορισμός μετά από διαδικασία διαβάθμισης ασφάλειας που πιστοποιεί ότι ένας ανάδοχος που είναι νομική οντότητα πληροί τις προϋποθέσεις για τον χειρισμό των Διαβαθμισμένων Πληροφοριών σύμφωνα με τους εθνικούς νόμους και κανονισμούς του αντίστοιχου Μέρους,

Ανάδοχος: άτομο ή νομική οντότητα που διαθέτει τη νομική ικανότητα να συνάπτει συμβάσεις,

Διαβαθμισμένη Σύμβαση: μια σύμβαση ή μια υπεργολαβία, συμπεριλαμβανομένων των προσυμβατικών διαπραγματεύσεων, η οποία περιέχει Διαβαθμισμένες Πληροφορίες ή περιλαμβάνει πρόσβαση σε αυτές τις πληροφορίες,

Τρίτο Μέρος: οποιοδήποτε κράτος, συμπεριλαμβανομένου οποιουδήποτε δημόσιου ή ιδιωτικού φορέα που υπάγεται στη δικαιοδοσία του, ή διεθνής οργανισμός που δεν είναι συμβαλλόμενο Μέρος της παρούσας Συμφωνίας.

ΑΡΘΡΟ 3

ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

(1) Οι Εθνικές Αρχές Ασφαλείας που ορίζονται από τα Μέρη ως υπεύθυνες για τη γενική εφαρμογή της παρούσας Συμφωνίας είναι:

Στην Ελληνική Δημοκρατία:

Εθνική Αρχή Ασφαλείας (ΕΑΑ), Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ), Κοινή Διοίκηση Στρατιωτικών Πληροφοριών (ΚΔΣΠ),

Στη Δημοκρατία της Σλοβενίας:

Το Γραφείο της Κυβέρνησης της Δημοκρατίας της Σλοβενίας για την Προστασία των Διαβαθμισμένων Πληροφοριών (ΕΑΑ).

(2) Οι Εθνικές Αρχές Ασφαλείας κοινοποιούν η μία στην άλλη οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας.

(3) Τα Μέρη κοινοποιούν αμοιβαία, μέσω διπλωματικών οδών, τυχόν μεταγενέστερες αλλαγές στις αντίστοιχες Εθνικές Αρχές Ασφαλείας.

ΑΡΘΡΟ 4

ΕΠΙΠΕΔΑ ΔΙΑΒΑΘΜΙΣΗΣ ΑΣΦΑΛΕΙΑΣ

(1) Κάθε Διαβαθμισμένη Πληροφορία που διακινείται βάσει της παρούσας Συμφωνίας επισημαίνεται με το κατάλληλο επίπεδο διαβάθμισης ασφαλείας σύμφωνα με τους εθνικούς νόμους και κανονισμούς των Μερών.

- (2) Τα ακόλουθα επίπεδα διαβάθμισης ασφαλείας ισοδυναμούν με:

ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ	ΣΤΗ ΔΗΜΟΚΡΑΤΙΑ ΤΗΣ ΣΛΟΒΕΝΙΑΣ	ΣΤΗΝ ΑΓΓΛΙΚΗ ΓΛΩΣΣΑ
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STROGO ΤΑJΝΟ	TOP SECRET
ΑΠΟΡΡΗΤΟ	ΤΑJΝΟ	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ΖΑΥΡΝΟ	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	INTERNO	RESTRICTED

ΑΡΘΡΟ 5 ΠΡΟΣΒΑΣΗ ΣΕ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

- (1) Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται σε εκείνα τα άτομα για τα οποία υφίσταται Ανάγκη Γνώσης, τα οποία ενημερώθηκαν σχετικά με το χειρισμό και την προστασία των Διαβαθμισμένων Πληροφοριών, και τα οποία έχουν λάβει την δέουσα εξουσιοδότηση σύμφωνα με τους εθνικούς νόμους και κανονισμούς.
- (2) Τα Μέρη αναγνωρίζουν αμοιβαία τον Έλεγχο Ασφάλειας Προσωπικού και τον Έλεγχο Ασφάλειας Εγκαταστάσεων. Το δεύτερο εδάφιο του άρθρου 4 εφαρμόζεται αναλόγως.

ΑΡΘΡΟ 6 ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

- (1) Τα Μέρη παρέχουν στις Διαβαθμισμένες Πληροφορίες βάσει της παρούσας Συμφωνίας το ίδιο επίπεδο προστασίας ασφαλείας που παρέχουν στις Διαβαθμισμένες Πληροφορίες τους ισοδύναμης διαβάθμισης.
- (2) Η αρμόδια αρχή ασφαλείας του Μέρους Προέλευσης:
- α) διασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες επισημαίνονται με κατάλληλο επίπεδο διαβάθμισης ασφαλείας σύμφωνα με τους εθνικούς νόμους και κανονισμούς τους, και
 - β) ενημερώνει το Μέρος Παραλαβής για τυχόν όρους αποχαρακτηρισμού ή περιορισμούς σχετικά με τη χρήση των Διαβαθμισμένων Πληροφοριών και για τυχόν επακόλουθες αλλαγές στο επίπεδο διαβάθμισης ασφαλείας
- (3) Η αρμόδια αρχή ασφαλείας του Μέρους Παραλαβής:
- α) διασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες επισημαίνονται με ισοδύναμο επίπεδο διαβάθμισης ασφαλείας σύμφωνα με το δεύτερο εδάφιο του άρθρου 4, και
 - β) διασφαλίζει ότι το επίπεδο διαβάθμισης ασφαλείας δεν θα αλλάξει χωρίς προηγούμενη γραπτή άδεια από το Μέρος Προέλευσης.

(4) Κάθε Μέρος διασφαλίζει ότι λαμβάνονται τα κατάλληλα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών που υποβάλλονται σε επεξεργασία, αποθηκεύονται ή μεταδίδονται με συστήματα επικοινωνίας και πληροφοριών. Τα μέτρα αυτά διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και, κατά περίπτωση, τη μη απόρριψη και την αυθεντικότητα των Διαβαθμισμένων Πληροφοριών, καθώς και το κατάλληλο επίπεδο λογοδοσίας και ιχνηλασιμότητας των ενεργειών σε σχέση με αυτές τις πληροφορίες.

ΑΡΘΡΟ 7

ΠΕΡΙΟΡΙΣΜΟΣ ΓΙΑ ΤΗ ΧΡΗΣΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

(1) Το Μέρος Παραλαβής θα χρησιμοποιεί Διαβαθμισμένες Πληροφορίες αποκλειστικά για το σκοπό για τον οποίο έχουν διαβιβαστεί και εντός των περιορισμών που δηλώνονται από το Μέρος Προέλευσης.

(2) Το Μέρος Παραλαβής δεν θα κοινοποιεί-αποκαλύπτει Διαβαθμισμένες Πληροφορίες σε Τρίτο Μέρος χωρίς προηγούμενη γραπτή συγκατάθεση- έγκριση από το Μέρος Προέλευσης.

ΑΡΘΡΟ 8

ΔΙΑΒΙΒΑΣΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

(1) Διαβαθμισμένες Πληροφορίες διαβιβάζονται μεταξύ των Μερών μέσω διπλωματικών οδών ή μέσω άλλων ασφαλών διαύλων που έχουν εγκριθεί αμοιβαία από τις Εθνικές Αρχές Ασφαλείας σύμφωνα με τους εθνικούς νόμους και κανονισμούς.

(2) Διαβαθμισμένες Πληροφορίες σε επίπεδο ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ μπορούν επίσης να διαβιβάζονται ταχυδρομικώς ή με άλλη υπηρεσία παράδοσης σύμφωνα με τους εθνικούς νόμους και κανονισμούς.

ΑΡΘΡΟ 9

ΑΝΑΠΑΡΑΓΩΓΗ, ΜΕΤΑΦΡΑΣΗ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

(1) Όλες οι αναπαραγωγές και οι μεταφράσεις πρέπει να φέρουν τα κατάλληλα επίπεδα διαβάθμισης ασφαλείας και να προστατεύονται με τον ίδιο τρόπο όπως οι αρχικές διαβαθμισμένες πληροφορίες. Οι μεταφράσεις και ο αριθμός των αναπαραγωγών περιορίζονται στην ελάχιστη ποσότητα που απαιτείται για επίσημη χρήση.

(2) Όλες οι μεταφράσεις θα σημαίνονται με το επίπεδο διαβάθμισης ασφαλείας των αρχικών Διαβαθμισμένων Πληροφοριών και θα περιέχουν κατάλληλο σχολιασμό στη γλώσσα της μετάφρασης που θα υποδεικνύει ότι περιέχουν Διαβαθμισμένες Πληροφορίες του Μέρους Προέλευσης.

(3) Οι Διαβαθμισμένες Πληροφορίες που σημειώνονται με το επίπεδο ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ, τόσο το πρωτότυπο όσο και η μετάφραση, θα αναπαράγονται μόνο μετά από γραπτή άδεια του Μέρους Προέλευσης.

(4) Οι Διαβαθμισμένες Πληροφορίες που σημειώνονται με το επίπεδο ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ δεν καταστρέφονται. Όταν δεν χρειάζονται – απαιτούνται πλέον, θα επιστρέφονται στο Μέρος Προέλευσης.

(5) Διαβαθμισμένες Πληροφορίες σε επίπεδο ΑΠΟΡΡΗΤΟ ή κατώτερο καταστρέφονται όταν δεν θεωρούνται πλέον απαραίτητες από το Μέρος Παραλαβής, σύμφωνα με τους εθνικούς νόμους και κανονισμούς.

(6) Εάν μια κατάσταση κρίσης καθιστά αδύνατη την προστασία ή την επιστροφή των Διαβαθμισμένων Πληροφοριών που διαβιβάζονται ή δημιουργούνται βάσει της παρούσας Συμφωνίας, οι Διαβαθμισμένες Πληροφορίες καταστρέφονται αμέσως. Το Μέρος Παραλαβής κοινοποιεί στην Εθνική Αρχή Ασφαλείας του Μέρους Προέλευσης την καταστροφή του το συντομότερο δυνατό.

ΑΡΘΡΟ 10

ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΒΑΣΕΙΣ

(1) Η Εθνική Αρχή Ασφαλείας του Μέρους Παραλαβής διασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες που σχετίζονται με Διαβαθμισμένη Σύμβαση κοινοποιούνται σε Ανάδοχους, υπεργολάβους ή μελλοντικούς εργολάβους αφού:

α) έχει διασφαλιστεί ότι ο Ανάδοχος, ο υπεργολάβος ή ο μελλοντικός ανάδοχος και οι εγκαταστάσεις του είναι σε θέση να παρέχουν την κατάλληλη προστασία για τις Διαβαθμισμένες Πληροφορίες,

β) οι εγκαταστάσεις έχουν λάβει την κατάλληλη Διαβάθμιση Ασφάλειας Εγκαταστάσεων και

γ) τα άτομα που εκτελούν λειτουργίες που απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες έχουν λάβει την κατάλληλη Διαβάθμιση Ασφάλειας Προσωπικού.

(2) Το Μέρος Παραλαβής διασφαλίζει ότι όλα τα άτομα που έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες ενημερώνονται για τις ευθύνες και την υποχρέωσή τους να προστατεύουν τις Διαβαθμισμένες Πληροφορίες σύμφωνα με τους εθνικούς νόμους και κανονισμούς.

(3) Η Εθνική Αρχή Ασφαλείας του Μέρους Προέλευσης μπορεί να ζητήσει να διενεργηθεί επιθεώρηση ασφαλείας σχετικά με την προστασία των Διαβαθμισμένων Πληροφοριών σε εγκατάσταση για να διασφαλιστεί η συνεχής συμμόρφωση με τα πρότυπα ασφαλείας σύμφωνα με τους εθνικούς νόμους και κανονισμούς.

(4) Μια Διαβαθμισμένη Σύμβαση περιλαμβάνει διατάξεις σχετικά με τις απαιτήσεις ασφαλείας και το επίπεδο διαβάθμισης ασφαλείας κάθε πτυχής ή στοιχείου της Διαβαθμισμένης Σύμβασης. Αντίγραφο αυτού του εγγράφου υποβάλλεται στις Εθνικές Αρχές Ασφαλείας των Μερών.

ΑΡΘΡΟ 11

ΕΠΙΣΚΕΨΕΙΣ

(1) Οι επισκέψεις που απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες υπόκεινται στην προηγούμενη έγκριση της Εθνικής Αρχής Ασφαλείας του Μέρους Υποδοχής.

(2) Ένα αίτημα για επίσκεψη υποβάλλεται στην αρμόδια Εθνική Αρχή Ασφαλείας τουλάχιστον 30 ημέρες πριν από την έναρξη της επίσκεψης. Η αίτηση επίσκεψης περιλαμβάνει τις ακόλουθες πληροφορίες, οι οποίες χρησιμοποιούνται μόνο για τους σκοπούς της επίσκεψης:

α) όνομα και επώνυμο του επισκέπτη, ημερομηνία και τόπος γέννησης, εθνικότητα και ταυτότητα/διαβατήριο,

β) τη θέση του επισκέπτη, με λεπτομερείς πληροφορίες του εργοδότη που αντιπροσωπεύει ο επισκέπτης,

γ) λεπτομέρειες του έργου στο οποίο συμμετέχει ο επισκέπτης,

δ) την εγκυρότητα και το επίπεδο διαβάθμισης Ασφάλειας Προσωπικού του επισκέπτη, εάν απαιτείται,

ε) όνομα, διεύθυνση, αριθμός τηλεφώνου/φαξ, διεύθυνση ηλεκτρονικού ταχυδρομείου και πρόσωπο επικοινωνίας της εγκατάστασης που πρόκειται να επισκεφθεί,

στ) τον σκοπό της επίσκεψης, συμπεριλαμβανομένου του υψηλότερου επιπέδου διαβάθμισης ασφαλείας των Διαβαθμισμένων Πληροφοριών που πρόκειται να εμπλακούν,

ζ) την ημερομηνία και τη διάρκεια της επίσκεψης. Σε περίπτωση επαναλαμβανόμενων επισκέψεων, θα λαμβάνεται υπόψη η συνολική περίοδος που καλύπτεται από τις επισκέψεις,

η) ημερομηνία και υπογραφή της αποστέλλουσας Εθνικής Αρχής Ασφαλείας.

(3) Σε επείγουσες περιπτώσεις, οι Εθνικές Αρχές Ασφαλείας μπορούν να συμφωνήσουν σε μικρότερο χρονικό διάστημα για την υποβολή αιτήματος επίσκεψης.

(4) Οι Εθνικές Αρχές Ασφαλείας μπορούν να συμφωνήσουν σε έναν κατάλογο επισκεπτών που δικαιούνται επαναλαμβανόμενες επισκέψεις. Ο κατάλογος ισχύει για μια αρχική περίοδο που δεν υπερβαίνει τους 12 μήνες και μπορεί να παραταθεί για μια περαιτέρω περίοδο που δεν υπερβαίνει τους 12 μήνες. Η αίτηση για επαναλαμβανόμενες επισκέψεις υποβάλλεται σύμφωνα με τη δεύτερη παράγραφο του παρόντος Άρθρου. Μόλις εγκριθεί ένας κατάλογος, οι επισκέψεις μπορούν να κανονιστούν απευθείας μεταξύ των σχετικών εγκαταστάσεων.

(5) Κάθε Μέρος εγγυάται την προστασία των προσωπικών δεδομένων των επισκεπτών σύμφωνα με τους εθνικούς νόμους και κανονισμούς.

(6) Τυχόν Διαβαθμισμένες Πληροφορίες που αποκτώνται από έναν επισκέπτη θεωρούνται Διαβαθμισμένες Πληροφορίες βάσει της παρούσας Συμφωνίας.

ΑΡΘΡΟ 12
ΣΥΝΕΡΓΑΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ
ΠΛΗΡΟΦΟΡΙΩΝ

- (1) Προκειμένου να επιτευχθούν και να διατηρηθούν συγκρίσιμα πρότυπα ασφάλειας, οι Εθνικές Αρχές Ασφαλείας παρέχουν, κατόπιν αιτήματος, αμοιβαία πληροφόρηση σχετικά με τα εθνικά πρότυπα ασφάλειας, τις διαδικασίες και τις πρακτικές τους για την προστασία των Διαβαθμισμένων Πληροφοριών. Για το σκοπό αυτό, οι Εθνικές Αρχές Ασφαλείας μπορούν να επισκέπτονται η μία την άλλη.
- (2) Οι αρμόδιες αρχές ασφαλείας αλληλοενημερώνονται για εξαιρετικούς κινδύνους ασφαλείας που ενδέχεται να θέσουν σε κίνδυνο τις Διαβαθμισμένες Πληροφορίες ή τα συστήματα προστασίας Διαβαθμισμένων Πληροφοριών.
- (3) Κατόπιν αιτήματος, οι Εθνικές Αρχές Ασφαλείας αλληλοβοηθούνται κατά τη διεξαγωγή διαδικασίας διαβάθμισης ασφαλείας. Ανταλλάσσουν πληροφορίες σχετικά με πιθανές ανησυχίες ασφαλείας που είναι σημαντικές στη διαδικασία διαβάθμισης ασφαλείας.
- (4) Οι Εθνικές Αρχές Ασφαλείας ενημερώνουν αμέσως η μία την άλλη για τυχόν αλλαγές στην Διαβάθμιση Ασφάλειας Προσωπικού και Εγκαταστάσεων.

ΑΡΘΡΟ 13
ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

- (1) Σε περίπτωση παραβίασης ασφάλειας με αποτέλεσμα μη εξουσιοδοτημένη αποκάλυψη, κατάχρηση ή απώλεια Διαβαθμισμένων Πληροφοριών ή υποψία για τέτοια παράβαση, η Εθνική Αρχή Ασφαλείας του Μέρους Παραλαβής ενημερώνει σχετικά αμέσως γραπτώς την Εθνική Αρχή Ασφαλείας του Μέρους Προέλευσης.
- (2) Οι αρμόδιες αρχές του Μέρους Παραλαβής λαμβάνουν όλα τα κατάλληλα μέτρα σύμφωνα με τους εθνικούς νόμους και κανονισμούς του για να περιορίσουν τις συνέπειες της παραβίασης που αναφέρονται στην πρώτη παράγραφο του παρόντος άρθρου και να αποτρέψουν περαιτέρω παραβιάσεις. Κατόπιν αιτήματος, το άλλο Μέρος παρέχει την κατάλληλη βοήθεια, ενημερώνεται για το αποτέλεσμα της διαδικασίας και τα μέτρα που ελήφθησαν λόγω της παράβασης.
- (3) Όταν έχει σημειωθεί παραβίαση της ασφάλειας σε Τρίτο Μέρος, η Εθνική Αρχή Ασφαλείας του αποστέλλοντος Μέρους λαμβάνει αμέσως τα μέτρα που αναφέρονται στο δεύτερο εδάφιο του παρόντος Άρθρου χωρίς καθυστέρηση.

ΑΡΘΡΟ 14
ΕΞΟΔΑ

Κάθε Συμβαλλόμενο Μέρος καλύπτει τα δικά του έξοδα που πραγματοποιούνται κατά την εφαρμογή της παρούσας Συμφωνίας.

ΑΡΘΡΟ 15
ΕΠΙΛΥΣΗ ΤΩΝ ΔΙΑΦΟΡΩΝ

Οποιαδήποτε διαφορά σχετικά με την ερμηνεία ή την εφαρμογή της παρούσας Συμφωνίας επιλύεται με διαβούλευση και διαπραγμάτευση μεταξύ των Μερών και δεν παραπέμπεται σε κανένα εθνικό ή διεθνές δικαστήριο ή Τρίτο Μέρος για διευθέτηση.

ΑΡΘΡΟ 16
ΤΕΛΙΚΕΣ ΡΗΤΡΕΣ

- (1) Η παρούσα Συμφωνία αρχίζει να ισχύει την πρώτη ημέρα του δεύτερου μήνα μετά την παραλαβή της τελευταίας κοινοποίησης με την οποία τα Μέρη ενημερώνουν το ένα το άλλο, μέσω διπλωματικών οδών, ότι έχουν ολοκληρωθεί οι εσωτερικές νομικές απαιτήσεις για την έναρξη ισχύος της.
- (2) Η παρούσα Συμφωνία μπορεί να τροποποιηθεί με αμοιβαία γραπτή συγκατάθεση των Μερών. Οι τροποποιήσεις αυτές τίθενται σε ισχύ σύμφωνα με την πρώτη παράγραφο του παρόντος άρθρου.
- (3) Η παρούσα Συμφωνία συνάπτεται για αόριστο χρονικό διάστημα. Κάθε Μέρος μπορεί να καταγγείλει την παρούσα συμφωνία με γραπτή ειδοποίηση που παρέχεται στο άλλο Μέρος μέσω διπλωματικών οδών. Σε μια τέτοια περίπτωση, η ισχύς της παρούσας Συμφωνίας λήγει έξι μήνες μετά την ημέρα κατά την οποία το άλλο Μέρος έλαβε ειδοποίηση καταγγελίας.
- (4) Σε περίπτωση καταγγελίας της παρούσας Συμφωνίας, τυχόν Διαβαθμισμένες Πληροφορίες που ανταλλάσσονται σύμφωνα με την παρούσα Συμφωνία θα εξακολουθήσουν να προστατεύονται σύμφωνα με τις διατάξεις που ορίζονται στο παρόν και, κατόπιν αιτήματος, επιστρέφονται στο Μέρος Προέλευσης.
- (5) Μπορούν να συναφθούν πρόσθετες ρυθμίσεις για την εφαρμογή της παρούσας Συμφωνίας.

Σε απόδειξη των ανωτέρω, οι υπογράφωντες, δεόντως εξουσιοδοτημένοι προς τούτο, υπέγραψαν την παρούσα Συμφωνία.

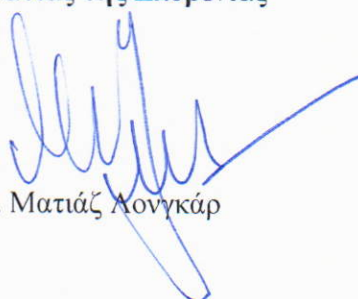
Συνήφθη στην Αθήνα την 04 Οκτωβρίου 2021 σε δύο πρωτότυπα στην Ελληνική, Σλοβενική και Αγγλική γλώσσα και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση απόκλισης της ερμηνείας, υπερισχύει το Αγγλικό κείμενο.

**Για την Κυβέρνηση της
Ελληνικής Δημοκρατίας**



Υποστράτηγος Δημήτριος Χούπης

**Για την Κυβέρνηση της
Δημοκρατίας της Σλοβενίας**



A.E. Ματιάς Λονγκάρ

AGREEMENT

between

**THE GOVERNMENT OF
THE HELLENIC REPUBLIC**

and

**THE GOVERNMENT OF
THE REPUBLIC OF SLOVENIA**

**ON MUTUAL PROTECTION
OF EXCHANGED CLASSIFIED
INFORMATION**

The Government of the Hellenic Republic

and

the Government of the Republic of Slovenia

Hereinafter referred to as the "Parties",

Wishing to ensure the protection of Classified Information exchanged between the Parties or between public and private entities under their jurisdiction,

In respect of the national interests and security of the Contracting States,

Have agreed as follows:

ARTICLE 1 OBJECTIVE

The Parties shall, in accordance with their respective laws and regulations, take all appropriate measures to ensure the protection of Classified Information which is transmitted or generated under this Agreement.

ARTICLE 2 DEFINITIONS

For the purposes of this Agreement, the following definitions shall apply:

Classified Information: any information, regardless of its form, which is transmitted or generated between the Parties under the national laws and regulations of either Party, and which, in the interests of national security, requires protection against unauthorised disclosure or other compromise, and is designated as such and marked appropriately;

Originating Party: the Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party;

Recipient Party: the Party, including any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party;

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;

Personnel Security Clearance: a determination, following a security clearance process in accordance with national laws and regulations, on the basis of which an individual is authorised to access to and handle Classified Information up to the level defined in the clearance;

Facility Security Clearance: a determination following a security clearance process certifying that a contractor which is a legal entity fulfils the conditions to handle Classified Information in accordance with the national laws and regulations of the respective Party;

Contractor: an individual or legal entity possessing the legal capacity to conclude contracts;

Classified Contract: a contract or a subcontract, including pre-contractual negotiations, which contains Classified Information or involves access to such information;

Third Party: any state, including any public or private entity under its jurisdiction, or an international organisation that is not a Party to this Agreement.

ARTICLE 3 COMPETENT SECURITY AUTHORITIES

(1) The National Security Authorities designated by the Parties as responsible for the general implementation of this Agreement are:

In the Hellenic Republic:

National Security Authority (NSA), Hellenic National Defence General Staff (HNDGS), Joint Military Intelligence Division (JMID),

In the Republic of Slovenia:

The Office of the Government of the Republic of Slovenia for the Protection of Classified Information (NSA).

(2) The National Security Authorities shall notify each other of any other competent security authorities responsible for the implementation of this Agreement.

(3) The Parties shall notify each other, through diplomatic channels, of any subsequent changes to their respective National Security Authorities.

ARTICLE 4 SECURITY CLASSIFICATION LEVELS

(1) Any Classified Information 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 following security classification levels shall be equivalent:

IN THE HELLENIC REPUBLIC	IN THE REPUBLIC OF SLOVENIA	IN THE ENGLISH LANGUAGE
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STROGO TAJNO	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ZAUPNO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	INTERNO	RESTRICTED

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

- (1) Access to Classified Information shall be limited to individuals who have a Need-to-Know, who have been briefed on handling and protecting Classified Information, and who are duly authorised thereto in accordance with national laws and regulations.
- (2) The Parties shall mutually recognise their Personnel Security Clearances and Facility Security Clearances. The second paragraph of Article 4 shall apply accordingly.

ARTICLE 6
PROTECTION OF CLASSIFIED INFORMATION

- (1) The Parties shall afford to Classified Information under this Agreement the same protection as to their own Classified Information with the corresponding security classification level.
- (2) The competent security authority of the Originating Party shall:
 - a) ensure that Classified Information is marked with an appropriate security classification level in accordance with its national laws and regulations, and
 - b) inform the Recipient Party of any conditions of release or limitations on the use of Classified Information, and of any subsequent changes in security classification level.
- (3) The competent security authority of the Recipient Party shall:
 - a) ensure that Classified Information is marked with an equivalent level of security classification in accordance with the second paragraph of Article 4, and
 - b) ensure that the security classification level is not changed without a prior written authorization by the Originating Party.
- (4) Each Party shall ensure that appropriate measures are taken to protect Classified Information processed, stored or transmitted in 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 information.

ARTICLE 7
RESTRICTION ON THE USE OF CLASSIFIED INFORMATION

- (1) The Recipient Party shall use Classified Information solely for the purpose for which it has been released and within the limitations stated by the Originating Party.
- (2) The Recipient Party shall not release Classified Information to a Third Party without a prior written consent from the Originating Party.

ARTICLE 8 TRANSMISSION OF CLASSIFIED INFORMATION

- (1) Classified Information shall be transmitted between the Parties through diplomatic channels or through other secure channels mutually approved by their National Security Authorities in accordance with national laws and regulations.
- (2) Classified Information at the RESTRICTED level may also be transmitted by post or another delivery service in accordance with national laws and regulations.

ARTICLE 9 REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

- (1) All reproductions and translations shall bear appropriate security classification levels and shall be protected in the same way as the original Classified Information. Translations and the number of reproductions shall be limited to the minimum amount required for official purposes.
- (2) All translations shall be marked with the security classification level of the original Classified Information, and shall contain suitable annotation in the language of translation indicating that they contain Classified Information of the Originating Party.
- (3) Classified Information marked with the TOP SECRET level, both the original and translation, shall be reproduced only upon the written permission of the Originating Party.
- (4) Classified Information marked with the TOP SECRET level shall not be destroyed. When no longer required, it shall be returned to the Originating Party.
- (5) Classified Information at the SECRET level or below shall be destroyed when it is no longer considered necessary by the Recipient Party, in accordance with national laws and regulations.
- (6) If a crisis situation makes it impossible to protect or return Classified Information transmitted or generated under this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall notify the National Security Authority of the Originating Party of its destruction as soon as possible.

ARTICLE 10 CLASSIFIED CONTRACTS

- (1) The National Security Authority of the Recipient Party shall ensure that Classified Information related to a Classified Contract is released to Contractors, subcontractors or prospective contractors after:
 - a) it has been ensured that the Contractor, subcontractor or prospective contractor and its facilities are able to provide suitable protection for the Classified Information;
 - b) the facilities have an appropriate Facility Security Clearance and

c) persons who perform functions which require access to Classified Information have appropriate Personnel Security Clearance.

(2) The Recipient Party shall ensure that all persons having access to Classified Information are informed of their responsibilities and obligation to protect the Classified Information in accordance with national laws and regulations.

(3) The National Security Authority of the Originating Party may request that a security inspection regarding the protection of Classified Information be undertaken at a facility to ensure continuing compliance with security standards in accordance with national laws and regulations.

(4) A Classified Contract shall contain provisions on the security requirements and on the security classification level of each aspect or element of the Classified Contract. A copy of such document shall be submitted to the National Security Authorities of the Parties.

ARTICLE 11 VISITS

(1) Visits requiring access to Classified Information shall be subject to the prior authorisation of the National Security Authority of the host Party.

(2) A request for visit shall be submitted to the competent National Security Authority at least 30 days prior to the commencement of the visit. The request for visit shall include the following information, which shall be used only for the purpose of the visit:

a) first and last name of the visitor, date and place of birth, nationality and identity card/passport number;

b) position of the visitor, with a specification of the employer that the visitor represents;

c) a specification of the project in which the visitor is a participant;

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

e) name, address, phone/fax number, e-mail address 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 the case of recurring visits, the total period covered by the visits shall be stated;

h) date and signature of the sending National Security Authority.

(3) In urgent cases, the National Security Authorities may agree on a shorter period for the submission of a request for visit.

(4) The National Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding 12 months and may be extended for a further period not exceeding 12 months. The request for recurring visits shall be submitted in accordance with the second paragraph of this Article. Once a list has been approved, visits may be arranged directly between the facilities involved.

(5) Each Party shall guarantee the protection of personal data of visitors in accordance with national laws and regulations.

(6) Any Classified Information acquired by a visitor shall be considered as Classified Information under this Agreement.

ARTICLE 12

CO-OPERATION ON THE PROTECTION OF CLASSIFIED INFORMATION

(1) In order to achieve and maintain comparable standards of security, the National Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. For this purpose, the National Security Authorities may visit each other.

(2) The competent security authorities shall inform each other of exceptional security risks that may endanger released Classified Information or Classified Information protection systems.

(3) On request, the National Security Authorities shall assist each other in carrying out a security clearance process. They shall exchange information on possible security concerns that are of importance in the security clearance process.

(4) The National Security Authorities shall promptly inform each other about any changes in Personnel and Facility Security Clearances.

ARTICLE 13

BREACH OF SECURITY

(1) In the event of a security breach resulting in the unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a breach, the National Security Authority of the Recipient Party shall immediately inform the National Security Authority of the Originating Party thereof in writing.

(2) The competent authorities of the Recipient Party shall take all appropriate measures under its national laws and regulations to limit the consequences of the breach referred to in the first paragraph of this Article and to prevent further breaches. On request, the other Party shall provide appropriate assistance; it shall be informed of the outcome of the proceedings and measures taken due to the breach.

(3) When a breach of security has occurred in a Third Party, the National Security Authority of the sending Party shall take the measures referred to in the second paragraph of this Article without delay.

ARTICLE 14 EXPENSES

Each Contracting Party shall bear its own costs incurred in the course of implementing this Agreement.

ARTICLE 15 RESOLUTION OF DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultation and negotiation between the Parties and shall not be referred to any national or international tribunal or Third Party for settlement.

ARTICLE 16 FINAL PROVISIONS

(1) This Agreement shall enter into force on the first day of the second month following the receipt of the last notification with which the Parties inform each other, through diplomatic channels, that the internal legal requirements for its entry into force have been fulfilled.

(2) This Agreement may be amended by the mutual, written consent of the Parties. Such amendments shall enter into force in accordance with the first paragraph of this Article.

(3) This Agreement shall be concluded for an indefinite period. Either Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels. In such a case, the validity of this Agreement shall expire six months after the day on which the other Party received notice of termination.

(4) In the event of termination of this Agreement, any Classified Information exchanged in accordance with this Agreement shall continue to be protected in accordance with the provisions set forth herein and, on request, returned to the Originating Party.

(5) Additional arrangements may be concluded for the implementation of this Agreement.

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

Done at Athens on.....04 October 2021.....in two
originals in the Greek, Slovenian and English languages, each text being equally authentic.
In case of divergence of interpretation, the English text shall prevail.

**For the Government of the
Hellenic Republic**



Major General Dimitrios Choupis

**For the Government of the
Republic of Slovenia**



H.E. Matjaž Longar

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 της παρ. 1 του άρθρου 16 αυτής.

Αθήνα, 16 Οκτωβρίου 2026

**ΕΘΝΙΚΗΣ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ
ΟΙΚΟΝΟΜΙΚΩΝ**

KYRIAKOS
PIERRAKAKIS
16.10.2026 18:17

ΚΥΡΙΑΚΟΣ ΠΙΕΡΡΑΚΑΚΗΣ

**ΟΙ ΥΠΟΥΡΓΟΙ
ΕΞΩΤΕΡΙΚΩΝ**

GEORGIOS
GERAPETRITIS
16.10.2026 16:58

ΓΕΩΡΓΙΟΣ ΓΕΡΑΠΕΤΡΙΤΗΣ

ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

NIKOLAS DENDIAS
16.10.2026 19:35

ΝΙΚΟΛΑΟΣ – ΓΕΩΡΓΙΟΣ ΔΕΝΔΙΑΣ