22.10.2026 17:46:07
ΨΗΦΙΑΚΑ
ΥΠΟΓΕΓΡΑΜΜΕΝΟ
ΑΠΟ
VARVARA ZACHARAKI

ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

21 Οκτωβρίου 2026 | ΤΕΥΧΟΣ ΠΡΩΤΟ | Αρ. Φύλλου **171**

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 5345

Κύρωση της Συμφωνίας μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της Κυβέρνησης του Μεγάλου Δουκάτου του Λουξεμβούργου για την ανταλλαγή και την αμοιβαία προστασία διαβαθμισμένων πληροφοριών.

Ο ΠΡΟΕΔΡΟΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

Εκδίδομε τον ακόλουθο νόμο που ψήφισε η Βουλή:

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Άρθρο πρώτο Κύρωση Συμφωνίας
Άρθρο 1 Στόχος και πεδίο εφαρμογής
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 στη χρήση διαβαθμισμένων πληροφοριών
Άρθρο 8 Διαβίβαση διαβαθμισμένων πληροφοριών
Άρθρο 9 Αναπαραγωγή, μετάφραση και καταστροφή 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 διαφορών
Άρθρο 16 Τελικές διατάξεις
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 του Μεγάλου Δουκάτου του Λουξεμβούργου για την ανταλλαγή και την αμοιβαία προστασία διαβαθμισμένων πληροφοριών, που υπογράφηκε στην Αθήνα στις 24 Οκτωβρίου 2024, το πρωτότυπο κείμενο της οποίας, στην ελληνική και την αγγλική γλώσσα, έχει ως εξής:

ΣΥΜΦΩΝΙΑ

ΜΕΤΑΞΥ

ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΚΑΙ

ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΟΥ ΜΕΓΑΛΟΥ ΔΟΥΚΑΤΟΥ ΤΟΥ ΛΟΥΞΕΜΒΟΥΡΓΟΥ

ΓΙΑ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΚΑΙ ΤΗΝ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η Κυβέρνηση της Ελληνικής Δημοκρατίας

και

η Κυβέρνηση του Μεγάλου Δουκάτου του Λουξεμβούργου

Στο εξής αναφερόμενες συλλογικά ως "Μέρη" και ατομικά ως "Μέρος",

Επιθυμώντας να διασφαλίσουν την προστασία των Διαβαθμισμένων Πληροφοριών που παράγονται ή ανταλλάσσονται κατά τη διάρκεια της συνεργασίας μεταξύ των Μερών ή μεταξύ δημόσιων και ιδιωτικών φορέων που υπάγονται στη δικαιοδοσία τους,

Σεβόμενες τα εθνικά συμφέροντα και την ασφάλεια των Μερών,

Αναγνωρίζοντας τις τυποποιημένες διαδικασίες Βιομηχανικής Ασφάλειας που θεσπίστηκαν από την Πολυεθνική Ομάδα Εργασίας Βιομηχανικής Ασφάλειας (MISWG),

Συμφώνησαν τα ακόλουθα (εφεξής η "Συμφωνία"):

ΑΡΘΡΟ 1
ΣΤΟΧΟΣ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

1.1 Τα Μέρη και οι δημόσιοι και ιδιωτικοί φορείς που υπάγονται στη δικαιοδοσία τους λαμβάνουν, σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών, όλα τα κατάλληλα μέτρα για να διασφαλίσουν την προστασία των Διαβαθμισμένων Πληροφοριών που παράγονται ή ανταλλάσσονται στο πλαίσιο της παρούσας Συμφωνίας.

1.2 Η παρούσα Συμφωνία εφαρμόζεται σε όλες τις δραστηριότητες, συμβάσεις ή συμφωνίες που αφορούν Διαβαθμισμένες Πληροφορίες και οι οποίες θα καταρτιστούν ή θα διεξαχθούν μεταξύ των Μερών μετά την έναρξη ισχύος της παρούσας Συμφωνίας.

1.3 Οι διατάξεις της παρούσας Συμφωνίας εφαρμόζονται επίσης στις Διαβαθμισμένες Πληροφορίες που έχουν ήδη παραχθεί ή ανταλλαγεί κατά τη διαδικασία συνεργασίας μεταξύ των Μερών πριν από την έναρξη ισχύος της παρούσας Συμφωνίας.

ΑΡΘΡΟ 2
ΟΡΙΣΜΟΙ

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

Διαβαθμισμένη Πληροφορία: κάθε πληροφορία, ανεξαρτήτως μορφής, η οποία παράγεται ή ανταλλάσσεται μεταξύ των Μερών ή μεταξύ δημόσιων και ιδιωτικών φορέων που υπάγονται στη δικαιοδοσία τους, σύμφωνα με τους εθνικούς νόμους και κανονισμούς ενός εκ των Μερών, και η οποία, για λόγους εθνικής ασφάλειας, απαιτεί προστασία από μη εξουσιοδοτημένη αποκάλυψη, απώλεια, καταστροφή ή υπεξαίρεση ή οποιοδήποτε άλλο είδος παραβίασης και χαρακτηρίζεται ως τέτοια και επισημαίνεται κατάλληλα,

Μέρος Προέλευσης: το Μέρος, συμπεριλαμβανομένων όλων των δημόσιων ή ιδιωτικών φορέων που υπάγονται στη δικαιοδοσία του, το οποίο κοινοποιεί Διαβαθμισμένες Πληροφορίες στο Μέρος Αποδέκτη,

Μέρος Αποδέκτης: το Μέρος, συμπεριλαμβανομένων όλων των δημόσιων ή ιδιωτικών οντοτήτων που υπάγονται στη δικαιοδοσία του, το οποίο λαμβάνει Διαβαθμισμένες Πληροφορίες από το Μέρος Προέλευσης,

Ανάγκη για Γνώση: μια αρχή βάσει της οποίας η πρόσβαση σε Διαβαθμισμένες Πληροφορίες μπορεί να χορηγηθεί σε ένα άτομο μόνο σε σχέση με τα επίσημα καθήκοντα ή εργασίες του,

Διαβάθμιση Ασφαλείας Προσωπικού: καθορισμός, μετά από διαδικασία ελέγχου ασφαλείας, σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών, βάσει του οποίου ένα άτομο επιτρέπεται να έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες και να χειρίζεται Διαβαθμισμένες Πληροφορίες μέχρι το επίπεδο που ορίζεται στην διαβάθμιση,

Διαβάθμιση Ασφαλείας Εγκατάστασης: απόφαση, μετά από διαδικασία ελέγχου ασφαλείας, η οποία πιστοποιεί ότι ένας ανάδοχος που είναι νομικό πρόσωπο πληροί τις προϋποθέσεις για να χειρίζεται Διαβαθμισμένες Πληροφορίες συγκεκριμένου επιπέδου διαβάθμισης ασφαλείας σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών,

Ανάδοχος: φυσικό ή νομικό πρόσωπο που έχει τη δικαιοπρακτική ικανότητα να συνάπτει Διαβαθμισμένες Συμβάσεις,

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

Παραβίαση της Ασφάλειας: πράξη ή παράλειψη, αντίθετη προς τους αντίστοιχους νόμους και κανονισμούς των Μερών, η οποία οδηγεί ή μπορεί να οδηγήσει σε αποκάλυψη, απώλεια, καταστροφή, υπεξαίρεση ή οποιοδήποτε άλλο είδος παραβίασης των Διαβαθμισμένων Πληροφοριών,

Τρίτο Μέρος: κάθε Κράτος, συμπεριλαμβανομένου κάθε δημόσιου ή ιδιωτικού φορέα υπό τη δικαιοδοσία του, ή κάθε διεθνούς οργανισμού που δεν είναι συμβαλλόμενο Μέρος της παρούσας Συμφωνίας.

ΑΡΘΡΟ 3
ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

3.1 Οι Εθνικές Αρχές Ασφαλείας που έχουν οριστεί σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών ως υπεύθυνες για τη γενική εφαρμογή της παρούσας Συμφωνίας και για τη διασφάλιση της προστασίας των Διαβαθμισμένων Πληροφοριών που παράγονται ή ανταλλάσσονται σύμφωνα με την παρούσα Συμφωνία είναι:

Για την Ελληνική Δημοκρατία:
Εθνική Αρχή Ασφαλείας (ΕΑΑ), Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ), Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ),

Για το Μεγάλο Δουκάτο του Λουξεμβούργου:
Ministère d'Etat, Service de renseignement de l'Etat, Autorité nationale de sécurité. (Υπουργείο Εξωτερικών, Κρατική Υπηρεσία Πληροφοριών, Εθνική Αρχή Ασφαλείας).

3.2 Οι Εθνικές Αρχές Ασφαλείας κοινοποιούν εγγράφως η μία στην άλλη κάθε άλλη αρμόδια αρχή ασφαλείας που είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας.

3.3 Τα Μέρη κοινοποιούν αμοιβαία, μέσω της διπλωματικής οδού, κάθε μεταγενέστερη αλλαγή στις αντίστοιχες Εθνικές Αρχές Ασφαλείας τους, καθώς και κάθε τροποποίηση στους αντίστοιχους νόμους και κανονισμούς τους σχετικά με τις Διαβαθμισμένες Πληροφορίες.

ΑΡΘΡΟ 4
ΕΠΙΠΕΔΑ ΔΙΑΒΑΘΜΙΣΗΣ ΑΣΦΑΛΕΙΑΣ

4.1. Κάθε Διαβαθμισμένη Πληροφορία που δημοσιοποιείται στο πλαίσιο της παρούσας Συμφωνίας φέρει την κατάλληλη διαβάθμιση ασφαλείας σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών.

4.2. Τα Μέρη αναλαμβάνουν την υποχρέωση να προστατεύουν τις Διαβαθμισμένες Πληροφορίες που ανταλλάσσονται μεταξύ τους και συμφωνούν ότι τα ακόλουθα επίπεδα διαβάθμισης ασφαλείας είναι ισοδύναμα:

ΓΙΑ ΤΗΝ ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ	ΓΙΑ ΤΟ ΜΕΓΑΛΟ ΔΟΥΚΑΤΟ ΤΟΥ ΛΟΥΞΕΜΒΟΥΡΓΟΥ	ΣΤΗΝ ΑΓΓΛΙΚΗ ΓΛΩΣΣΑ*
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TRES SECRET LUX	TOP SECRET
ΑΠΟΡΡΗΤΟ	SECRET LUX	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIEL LUX	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTREINT LUX	RESTRICTED

* Χρησιμοποιείται μόνο για λόγους κατανόησης, όχι για επίσημη χρήση.

ΑΡΘΡΟ 5
ΠΡΟΣΒΑΣΗ ΣΕ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

5.1 Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται σε άτομα που έχουν Ανάγκη για Γνώση, τα οποία έχουν ενημερωθεί σχετικά με το χειρισμό και την προστασία των Διαβαθμισμένων Πληροφοριών και τα οποία είναι δεόντως εξουσιοδοτημένα προς τούτο σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών.

5.2 Τα Μέρη αναγνωρίζουν αμοιβαία τις Διαβαθμίσεις Ασφαλείας Προσωπικού και τις Διαβαθμίσεις Ασφαλείας Εγκαταστάσεων που χορηγούνται σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς τους. Το άρθρο 4 παράγραφος 2 της παρούσας Συμφωνίας εφαρμόζεται αναλόγως.

ΑΡΘΡΟ 6
ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

6.1 Σύμφωνα με τους εθνικούς τους νόμους και κανονισμούς, τα Μέρη λαμβάνουν όλα τα κατάλληλα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών που παράγονται ή ανταλλάσσονται στο πλαίσιο της παρούσας Συμφωνίας. Τα Μέρη παρέχουν στις Διαβαθμισμένες Πληροφορίες στο πλαίσιο της παρούσας Συμφωνίας την ίδια προστασία με τις δικές τους Διαβαθμισμένες Πληροφορίες με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας.

6.2 Το Μέρος Προέλευσης:

α) διασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες επισημαίνονται με το κατάλληλο επίπεδο διαβάθμισης ασφαλείας σύμφωνα με τους εθνικούς νόμους και κανονισμούς της, και

β) ενημερώνει το Μέρος Αποδέκτη για οποιουσδήποτε όρους αποδέσμευσης ή περιορισμούς στη χρήση των Διαβαθμισμένων Πληροφοριών και ενημερώνει εγγράφως για τυχόν μεταγενέστερες αλλαγές στο επίπεδο διαβάθμισης ασφαλείας.

6.3. Το Μέρος Αποδέκτης:

α) σύμφωνα με τους εθνικούς της νόμους και κανονισμούς, διασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες επισημαίνονται με ισοδύναμο επίπεδο διαβάθμισης ασφαλείας σύμφωνα με το άρθρο 4 παράγραφος 2 της παρούσας Συμφωνίας, και

β) διασφαλίζει ότι το επίπεδο διαβάθμισης ασφαλείας δεν αλλάζει χωρίς την προηγούμενη γραπτή συγκατάθεση του Μέρους Προέλευσης.

6.4 Κάθε Μέρος διασφαλίζει ότι λαμβάνονται τα κατάλληλα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών που υποβάλλονται σε επεξεργασία, αποθηκεύονται ή διαβιβάζονται σε συστήματα επικοινωνίας και πληροφοριών. Τα μέτρα αυτά διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και, κατά περίπτωση, τη μη αμφισβήτηση και τη γνησιότητα των Διαβαθμισμένων Πληροφοριών, καθώς και κατάλληλο επίπεδο λογοδοσίας και ιχνηλασιμότητας των ενεργειών σε σχέση με τις εν λόγω πληροφορίες.

ΑΡΘΡΟ 7
ΠΕΡΙΟΡΙΣΜΟΣ ΣΤΗ ΧΡΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

7.1 Το Μέρος Αποδέκτης χρησιμοποιεί τις Διαβαθμισμένες Πληροφορίες αποκλειστικά για τον σκοπό για τον οποίο έχουν δοθεί και εντός των περιορισμών που έχει δηλώσει το Μέρος Προέλευσης.

7.2 Το Μέρος Αποδέκτης δεν θα κοινοποιεί Διαβαθμισμένες Πληροφορίες σε τρίτο Μέρος χωρίς την προηγούμενη γραπτή συγκατάθεση του Μέρους Προέλευσης.

ΑΡΘΡΟ 8
ΔΙΑΒΙΒΑΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

8.1 Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται μεταξύ των Μερών μέσω της διπλωματικής οδού ή μέσω άλλων ασφαλών διαύλων που συμφωνούνται αμοιβαία εκ των προτέρων από τις Εθνικές Αρχές Ασφαλείας τους σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών.

8.2 Οι πληροφορίες με διαβάθμιση ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIEL LUX και άνω καταχωρίζονται.

8.3 Η ηλεκτρονική διαβίβαση Διαβαθμισμένων Πληροφοριών πραγματοποιείται μέσω πιστοποιημένων κρυπτογραφικών μέσων που συμφωνούνται από τις Εθνικές Αρχές Ασφαλείας.

8.4 Οι Διαβαθμισμένες Πληροφορίες με την ένδειξη ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/RESTREINT LUX μπορούν επίσης να μεταφερθούν μέσω ταχυδρομείου ή άλλης υπηρεσίας παράδοσης σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών.

ΑΡΘΡΟ 9
ΑΝΑΠΑΡΑΓΩΓΗ, ΜΕΤΑΦΡΑΣΗ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

9.1 Όλες οι αναπαραγωγές και μεταφράσεις φέρουν τα κατάλληλα επίπεδα διαβάθμισης ασφαλείας και προστατεύονται με τον ίδιο τρόπο όπως οι αρχικές Διαβαθμισμένες Πληροφορίες. Οι μεταφράσεις και ο αριθμός των αναπαραγωγών περιορίζονται στο ελάχιστο ποσό που απαιτείται για επίσημους σκοπούς.

9.2 Σε όλες τις μεταφράσεις αναγράφεται το επίπεδο διαβάθμισης ασφαλείας των αρχικών Διαβαθμισμένων Πληροφοριών και περιλαμβάνονται κατάλληλες σημειώσεις στη γλώσσα της μετάφρασης, οι οποίες υποδεικνύουν ότι περιέχουν Διαβαθμισμένες Πληροφορίες του Μέρους Προέλευσης.

9.3 Οι Διαβαθμισμένες Πληροφορίες με την ένδειξη ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TRES SECRET LUX, τόσο το πρωτότυπο όσο και η μετάφραση, αναπαράγονται ή μεταφράζονται μόνο κατόπιν προηγούμενης γραπτής συγκατάθεσης του Μέρους Προέλευσης.

9.4 Οι Διαβαθμισμένες Πληροφορίες με την ένδειξη ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TRES SECRET LUX δεν καταστρέφονται. Όταν δεν απαιτούνται πλέον, επιστρέφονται στο Μέρος Προέλευσης.

9.5 Οι Διαβαθμισμένες Πληροφορίες που χαρακτηρίζονται ως ΑΠΟΡΡΗΤΟ/SECRET LUX ή κατώτερες καταστρέφονται όταν δεν κρίνονται πλέον απαραίτητες από το Μέρος Αποδέκτη, στο βαθμό που εμποδίζεται η αναδημιουργία τους εν όλω ή εν μέρει, σύμφωνα με τους εθνικούς νόμους και κανονισμούς του.

9.6 Εάν μια κατάσταση κρίσης καθιστά αδύνατη την προστασία ή την επιστροφή των Διαβαθμισμένων Πληροφοριών που παράγονται ή ανταλλάσσονται στο πλαίσιο της παρούσας Συμφωνίας, οι Διαβαθμισμένες Πληροφορίες καταστρέφονται αμέσως. Το Μέρος Αποδέκτης ενημερώνει την Εθνική Αρχή Ασφαλείας του Μέρους Προέλευσης για την καταστροφή τους το συντομότερο δυνατό.

ΑΡΘΡΟ 10
ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΒΑΣΕΙΣ

10.1 Αναπόσπαστο Μέρος κάθε Διαβαθμισμένης Σύμβασης ή υπεργολαβίας αποτελεί παράρτημα ασφαλείας, με το οποίο η αναθέτουσα αρχή που υπάγεται στη δικαιοδοσία του Μέρους Προέλευσης καθορίζει ποιες Διαβαθμισμένες Πληροφορίες πρόκειται να παραδοθούν στον Ανάδοχο που υπάγεται στη δικαιοδοσία του Μέρους Αποδέκτη, ποιο επίπεδο διαβάθμισης ασφαλείας έχει αποδοθεί στις πληροφορίες αυτές και τις υποχρεώσεις του Αναδόχου για την προστασία των Διαβαθμισμένων Πληροφοριών. Αντίγραφο του παραρτήματος ασφαλείας αποστέλλεται στην Εθνική Αρχή Ασφαλείας του Μέρους Αποδέκτη.

10.2 Η Εθνική Αρχή Ασφαλείας του Μέρους Αποδέκτη διασφαλίζει ότι οι Διαβαθμισμένες Πληροφορίες που σχετίζονται με μια Διαβαθμισμένη Σύμβαση κοινοποιούνται σε Εργολάβους, υπεργολάβους ή υποψήφιους εργολάβους αφού:

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

β) οι εγκαταστάσεις διαθέτουν την κατάλληλη Διαβάθμιση Ασφαλείας Εγκατάστασης και

γ) τα πρόσωπα που εκτελούν καθήκοντα που απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες διαθέτουν την κατάλληλη Διαβάθμιση Ασφαλείας Προσωπικού.

10.3. Το Μέρος Αποδέκτης θα διασφαλίζει ότι όλα τα πρόσωπα που έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες ενημερώνονται για τις ευθύνες και την υποχρέωσή τους να προστατεύουν τις Διαβαθμισμένες Πληροφορίες σύμφωνα με τους εθνικούς του νόμους και κανονισμούς.

10.4. Η Εθνική Αρχή Ασφαλείας του αρχικού συμβαλλόμενου Μέρους μπορεί να ζητήσει τη διενέργεια επιθεώρησης ασφαλείας σχετικά με την προστασία των Διαβαθμισμένων Πληροφοριών σε μια εγκατάσταση για να διασφαλιστεί η συνεχής συμμόρφωση με τα πρότυπα ασφαλείας σύμφωνα με τους νόμους και τους κανονισμούς της.

ΑΡΘΡΟ 11
ΕΠΙΣΚΕΨΕΙΣ

11.1. Οι επισκέψεις που απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες υπόκεινται στην προηγούμενη έγκριση της Εθνικής Αρχής Ασφαλείας του Μέρους υποδοχής.

11.2 Η αίτηση επίσκεψης υποβάλλεται στην αρμόδια Εθνική Αρχή Ασφαλείας τουλάχιστον τρεις (3) εβδομάδες πριν από την έναρξη της επίσκεψης. Η αίτηση επίσκεψης περιλαμβάνει για κάθε επισκέπτη/συμμετέχοντα τις ακόλουθες πληροφορίες, οι οποίες χρησιμοποιούνται μόνο για τους σκοπούς της επίσκεψης:

α) όνομα και επώνυμο του επισκέπτη, ημερομηνία και τόπος γέννησης, εθνικότητα (-ες) και αριθμός δελτίου ταυτότητας/διαβατηρίου,

β) θέση του επισκέπτη και όνομα του οργανισμού που εκπροσωπεί,

γ) προδιαγραφές του έργου στο οποίο συμμετέχει ο επισκέπτης,

δ) την εγκυρότητα και το επίπεδο διαβάθμισης της Διαβάθμισης Ασφαλείας Προσωπικού του επισκέπτη, εάν απαιτείται,

ε) όνομα, διεύθυνση, αριθμός τηλεφώνου, διεύθυνση ηλεκτρονικού ταχυδρομείου και σημείο επαφής της εγκατάστασης που πρόκειται να επισκεφθεί,

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

ζ) αναφέρεται η ημερομηνία και η διάρκεια της επίσκεψης, και σε περίπτωση επαναλαμβανόμενων επισκέψεων, η συνολική περίοδος που καλύπτουν οι επισκέψεις,

η) ημερομηνία και υπογραφή της αποστέλλουσας Εθνικής Αρχής Ασφαλείας,

θ) άλλα πρόσθετα δεδομένα, τα οποία συμφωνούνται από τις Εθνικές Αρχές Ασφαλείας.

11.3. Σε επείγουσες περιπτώσεις, οι Εθνικές Αρχές Ασφαλείας μπορούν να συμφωνήσουν σε συντομότερη προθεσμία για την υποβολή αίτησης επίσκεψης.

11.4. Οι Εθνικές Αρχές Ασφάλειας μπορούν να συμφωνήσουν σχετικά με έναν κατάλογο επισκεπτών που δικαιούνται επαναλαμβανόμενες επισκέψεις. Ο κατάλογος ισχύει για αρχική περίοδο που δεν υπερβαίνει τους δώδεκα (12) μήνες και μπορεί να παραταθεί για περαιτέρω περίοδο που δεν υπερβαίνει τους δώδεκα (12) μήνες. Η αίτηση για επαναλαμβανόμενες επισκέψεις υποβάλλεται σύμφωνα με τη διαδικασία που προβλέπεται στη δεύτερη παράγραφο του παρόντος άρθρου. Μετά την έγκριση του καταλόγου, οι επισκέψεις μπορούν να κανονιστούν απευθείας μεταξύ των εμπλεκόμενων εγκαταστάσεων.

11.5 Κάθε Μέρος εγγυάται την προστασία των προσωπικών δεδομένων των επισκεπτών σύμφωνα με τους εθνικούς του νόμους και κανονισμούς.

11.6 Οποιαδήποτε Διαβαθμισμένη Πληροφορία στην οποία είχε πρόσβαση ένας επισκέπτης κατά τη διάρκεια της επίσκεψής του, θεωρείται ως Διαβαθμισμένη Πληροφορία στο πλαίσιο της παρούσας Συμφωνίας.

ΑΡΘΡΟ 12
ΣΥΝΕΡΓΑΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

12.1 Για την επίτευξη και τη διατήρηση συγκρίσιμων προτύπων ασφαλείας, οι Εθνικές Αρχές Ασφαλείας, κατόπιν αιτήματος, παρέχουν αμοιβαίως πληροφορίες σχετικά με τα εθνικά πρότυπα ασφαλείας τους, τις διαδικασίες και τις πρακτικές τους για την προστασία των Διαβαθμισμένων Πληροφοριών.

12.2 Κατόπιν αιτήματος, η Εθνική Αρχή Ασφαλείας ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας του Μέρους Προέλευσης εξουσιοδοτείται να επισκεφθεί το άλλο Μέρος προκειμένου να εξακριβώσει με την Εθνική Αρχή Ασφαλείας ή οποιαδήποτε αρμόδια αρχή ασφαλείας του Μέρους Αποδέκτη, εάν οι Διαβαθμισμένες Πληροφορίες που ανταλλάσσονται σύμφωνα με την παρούσα Συμφωνία προστατεύονται σύμφωνα με την παρούσα Συμφωνία.

12.3. Οι αρμόδιες αρχές ασφαλείας αλληλοενημερώνονται για έκτακτους κινδύνους ασφαλείας που ενδέχεται να θέσουν σε κίνδυνο κοινοποιημένες Διαβαθμισμένες Πληροφορίες ή συστήματα προστασίας Διαβαθμισμένων Πληροφοριών.

12.4 Κατόπιν αιτήματος και σύμφωνα με τους αντίστοιχους νόμους και κανονισμούς των Μερών, οι Εθνικές Αρχές Ασφαλείας συνδράμουν η μία την άλλη στη διεξαγωγή διαδικασίας ελέγχου ασφαλείας. Ανταλλάσσουν πληροφορίες σχετικά με πιθανά ζητήματα ασφαλείας που έχουν σημασία για τη διαδικασία ελέγχου ασφαλείας.

12.5 Μετά από αίτημα της Εθνικής Αρχής Ασφαλείας του Μέρους Προέλευσης, η Εθνική Αρχή Ασφαλείας του Μέρους Αποδέκτη εκδίδει γραπτή επιβεβαίωση ότι ένα φυσικό πρόσωπο έχει λάβει Διαβάθμιση Ασφαλείας Προσωπικού ή μια νομική οντότητα έχει λάβει Διαβάθμιση Ασφαλείας Εγκατάστασης.

12.6 Οι Εθνικές Αρχές Ασφαλείας αλληλοενημερώνονται αμέσως για τυχόν αλλαγές στις Διαβαθμίσεις Ασφαλείας Προσωπικού και στις Διαβαθμίσεις Ασφαλείας Εγκαταστάσεων.

ΑΡΘΡΟ 13
ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

13.1. Σε περίπτωση Παραβίασης της Ασφάλειας που οδηγεί σε μη εξουσιοδοτημένη αποκάλυψη, υπεξαίρεση ή απώλεια Διαβαθμισμένων Πληροφοριών ή υποψίας τέτοιας παραβίασης, η Εθνική Αρχή Ασφάλειας του Μέρους Αποδέκτη ενημερώνει αμέσως εγγράφως την Εθνική Αρχή Ασφάλειας του Μέρους Προέλευσης και μεριμνά για την έναρξη κατάλληλης έρευνας.

13.2 Οι αρμόδιες αρχές του Μέρους Αποδέκτη λαμβάνουν όλα τα κατάλληλα μέτρα βάσει των εθνικών τους νόμων και κανονισμών για να περιορίσουν τις συνέπειες της παράβασης που αναφέρεται στην πρώτη παράγραφο του παρόντος άρθρου και να αποτρέψουν τυχόν περαιτέρω παραβάσεις. Κατόπιν αιτήματος, το Μέρος Προέλευσης παρέχει την κατάλληλη συνδρομή, ενημερώνεται για το αποτέλεσμα της έρευνας και τα διορθωτικά μέτρα που λαμβάνονται λόγω της παραβίασης.

13.3 Όταν έχει σημειωθεί Παραβίαση της Ασφάλειας σε τρίτο Μέρος, η Εθνική Αρχή Ασφάλειας του τρίτου Μέρους καλείται από την Εθνική Αρχή Ασφάλειας του Μέρους Αποδέκτη να λάβει χωρίς καθυστέρηση τα μέτρα που αναφέρονται στο δεύτερο εδάφιο του παρόντος άρθρου.

ΑΡΘΡΟ 14
ΕΞΟΔΑ

Κάθε συμβαλλόμενο Μέρος αναλαμβάνει τα δικά του έξοδα που προκύπτουν από την εφαρμογή της παρούσας Συμφωνίας.

ΑΡΘΡΟ 15
ΕΠΙΛΥΣΗ ΔΙΑΦΟΡΩΝ

Κάθε διαφορά σχετικά με την ερμηνεία ή την εφαρμογή της παρούσας Συμφωνίας επιλύεται με διαβουλεύσεις ή/και διαπραγματεύσεις μεταξύ των Μερών και δεν παραπέμπεται σε εθνικό ή διεθνές δικαστήριο ή σε τρίτο Μέρος για διευθέτηση.

ΑΡΘΡΟ 16
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

16.1. 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 της διπλωματικής οδού, ότι πληρούνται οι εσωτερικές νομικές προϋποθέσεις για την έναρξη ισχύος της.

16.2. Η παρούσα Συμφωνία μπορεί να τροποποιηθεί με την αμοιβαία, γραπτή συναίνεση των Μερών. Οι τροποποιήσεις αυτές τίθενται σε ισχύ σύμφωνα με τη διαδικασία που προβλέπεται στην πρώτη παράγραφο του παρόντος άρθρου.

16.3 Η παρούσα Συμφωνία συνάπτεται για αόριστο χρονικό διάστημα. Κάθε Μέρος μπορεί να καταγγείλει την παρούσα Συμφωνία με γραπτή ειδοποίηση καταγγελίας προς το άλλο Μέρος μέσω της διπλωματικής οδού. Στην περίπτωση αυτή, η παρούσα Συμφωνία θα τερματιστεί έξι (6) μήνες μετά την ημερομηνία παραλαβής της ειδοποίησης καταγγελίας από το άλλο Μέρος.

16.4. Σε περίπτωση καταγγελίας της παρούσας Συμφωνίας, κάθε Διαβαθμισμένη Πληροφορία που ανταλλάσσεται ή παράγεται στο πλαίσιο της παρούσας Συμφωνίας εξακολουθεί να προστατεύεται σύμφωνα με τις διατάξεις της παρούσας και, κατόπιν αιτήματος, επιστρέφεται στο αρχικό συμβαλλόμενο Μέρος.

16.5 Όπου είναι αναγκαίο, οι Εθνικές Αρχές Ασφαλείας ή άλλες αρμόδιες αρχές ασφαλείας των Μερών μπορούν να διαβουλεύονται μεταξύ τους για λεπτομερείς τεχνικές πτυχές που αφορούν την εφαρμογή της παρούσας Συμφωνίας και μπορούν να συνάπτουν, κατά περίπτωση, κατάλληλες νομικές πράξεις ή ειδικά πρωτόκολλα ασφαλείας για τη συμπλήρωση της παρούσας Συμφωνίας.

Σε πίστωση των ανωτέρω, οι υπογεγραμμένοι, δεόντως εξουσιοδοτημένοι προς τούτο, υπέγραψαν την παρούσα Συμφωνία.

Έγινε στην Αθήνα, την 24 Οκτωβρίου 2024, σε δύο πρωτότυπα, το καθένα στην Ελληνική, Γαλλική και Αγγλική γλώσσα και κάθε κείμενο είναι εξίσου αυθεντικό. Σε περίπτωση διαφορετικής ερμηνείας, υπερισχύει το αγγλικό κείμενο.

Για την Κυβέρνηση της Ελληνικής Δημοκρατίας

Υποστράτηγος
Γρηγόριος Π. Μπουντλιάκης
Διευθυντής Ε΄ Κλάδου
Γενικού Επιτελείου Εθνικής Άμυνας

Για την Κυβέρνηση του Μεγάλου Δουκάτου του Λουξεμβούργου

Ελισάβετ Καρντόσο
Πρέσβης του Μεγάλου Δουκάτου του Λουξεμβούργου στην Ελλάδα

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE HELLENIC REPUBLIC

AND

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG

ON EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Hellenic Republic

and

the Government of the Grand Duchy of Luxembourg

Hereinafter collectively referred to as the "Parties" and individually as the "Party",

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

In respect of the national interests and security of the Parties,

Acknowledging the standardized Industrial Security procedures established by the Multinational Industrial Security Working Group (MISWG),

Have agreed as follows (hereafter the "Agreement"):

ARTICLE 1
OBJECTIVE AND SCOPE

1.1 The Parties and public and private entities under their jurisdiction shall, in accordance with the Parties' respective laws and regulations, take all appropriate measures to ensure the protection of Classified Information which is generated or exchanged under this Agreement.

1.2 This Agreement shall apply to any activities, contracts or agreements involving Classified Information that will be conducted or concluded between the Parties following the entering into force of this Agreement.

1.3 The provisions of this Agreement shall also apply to Classified Information already generated or exchanged in the process of cooperation between the Parties before the entering into force of 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 generated or exchanged between the Parties or between public and private entities under their jurisdiction, under the national laws and regulations of either Party, and which, in the interests of national security, requires protection against unauthorised disclosure, loss, destruction, or misappropriation or any other kind of 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 vetting process, in accordance with the Parties' respective 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 vetting process, certifying that a contractor which is a legal entity fulfills the conditions to handle Classified Information of a specified security classification level in accordance with the Parties' respective laws and regulations;

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

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

Breach of Security: an act or an omission, contrary to the Parties' respective laws and regulations, which results, or may result in disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;

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

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

3.1 The National Security Authorities designated in accordance with the Parties' respective laws and regulations by them as responsible for the general implementation of this Agreement and for the assurance of protection of Classified Information generated or exchanged according to this Agreement are:

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

For the Grand Duchy of Luxembourg:
Ministère d'Etat, Service de renseignement de l'Etat, Autorité nationale de sécurité.

3.2 The National Security Authorities shall notify each other in writing of any other competent security authorities responsible for the implementation of this Agreement.

3.3 The Parties shall notify each other, through diplomatic channels, of any subsequent changes to their respective National Security Authorities as well as of any change in their respective laws and regulations related to Classified Information.

ARTICLE 4
SECURITY CLASSIFICATION LEVELS

4.1 Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the Parties' respective laws and regulations.

4.2 The Parties undertake to protect Classified Information exchanged between them and agree that the following security classification levels shall be equivalent:

FOR THE HELLENIC REPUBLIC	FOR THE GRAND DUCHY OF LUXEMBOURG	IN THE ENGLISH LANGUAGE*
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TRES SECRET LUX	TOP SECRET
ΑΠΟΡΡΗΤΟ	SECRET LUX	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIEL LUX	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTREINT LUX	RESTRICTED

* Used only for understanding purposes, not for official use.

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

5.1 Access to Classified Information shall be limited to individuals on a Need-to-Know basis, who have been briefed on handling and protecting Classified Information, and who are duly authorised thereto in accordance with the Parties' respective laws and regulations.

5.2 The Parties shall mutually recognise their Personnel Security Clearances and Facility Security Clearances granted in accordance with their respective laws and regulations. Article 4, paragraph 2 of this Agreement, shall apply accordingly.

ARTICLE 6
PROTECTION OF CLASSIFIED INFORMATION

6.1 In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information, which is generated or exchanged under this Agreement. 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.

6.2 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 inform in writing of any subsequent changes in security classification level.

6.3 The Recipient Party shall:

a) in accordance with its national laws and regulations, ensure that Classified Information is marked with an equivalent level of security classification in accordance with Article 4, paragraph 2 of this Agreement, and

b) ensure that the security classification level is not changed without the prior written consent of the Originating Party.

6.4 Each Party shall ensure that appropriate measures are taken to protect Classified Information which is 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

7.1 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.

7.2 The Recipient Party shall not release Classified Information to a Third Party without the prior written consent of the Originating Party.

ARTICLE 8
TRANSFER OF CLASSIFIED INFORMATION

8.1 Classified Information shall be transferred between the Parties through diplomatic channels or through other secure channels mutually agreed upon in advance by their National Security Authorities in accordance with the Parties' respective laws and regulations.

8.2 Information classified ΕΜΠΙΣΤΕΥΤΙΚΟ/CONFIDENTIEL LUX and above shall be registered.

8.3 Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed upon by the National Security Authorities.

8.4 Classified Information marked as ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/RESTREINT LUX may also be transferred by post or another delivery service in accordance with the Parties' respective laws and regulations.

ARTICLE 9
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

9.1 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.

9.2 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.

9.3 Classified Information marked as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TRES SECRET LUX, both the original and translation, shall be reproduced or translated only upon prior written consent of the Originating Party.

9.4 Classified Information marked as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TRES SECRET LUX shall not be destroyed. When no longer required, it shall be returned to the Originating Party.

9.5 Classified Information marked as ΑΠΟΡΡΗΤΟ/SECRET LUX or below shall be destroyed when it is no longer considered necessary by the Recipient Party, insofar as to prevent its reconstruction in whole or in part, in accordance with its national laws and regulations.

9.6 If a crisis situation makes it impossible to protect or return Classified Information generated or exchanged 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

10.1 A security annex shall be an integral part of each Classified Contract, or subcontract, by which the contracting authority under the jurisdiction of the Originating Party shall specify which Classified Information is to be released to the Contractor under the jurisdiction of the Recipient Party, which security classification level has been assigned to that information and the Contractor's obligations to protect the Classified Information. A copy of the security annex shall be sent to the National Security Authority of the Recipient Party.

10.2 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.

10.3 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 its national laws and regulations.

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

ARTICLE 11
VISITS

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

11.2 A request for visit shall be submitted to the competent National Security Authority at least three (3) weeks prior to the commencement of the visit. The request for visit shall include for each visitor/participant, the following information, which shall be used only for the purpose of the visit:

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

b) position of the visitor and name of the organization represented;

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 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, and 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;

i) other additional data, agreed upon by the National Security Authorities.

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

11.4 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 twelve (12) months and may be extended for a further period not exceeding twelve (12) months. The request for recurring visits shall be submitted in accordance with the procedure set forth in the second paragraph of this article. Once a list has been approved, visits may be arranged directly between the facilities involved.

11.5 Each Party shall guarantee the protection of personal data of visitors in accordance with its national laws and regulations.

11.6 Any Classified Information to which a visitor had access to, during his visit, shall be considered as Classified Information under this Agreement.

ARTICLE 12
COOPERATION ON THE PROTECTION OF CLASSIFIED INFORMATION

12.1 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.

12.2 Upon request, the National Security Authority or any other competent security authority of the Originating Party shall be authorized to visit the other Party in order to ascertain with the National Security Authority or any competent security authority of the Recipient Party, whether the Classified Information exchanged pursuant to this Agreement is protected in accordance with this Agreement.

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

12.4 Upon request, and in accordance with the Parties' respective laws and regulations, the National Security Authorities shall assist each other in carrying out a security vetting process. They shall exchange information on possible security concerns that are of importance in the security vetting process.

12.5 Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Recipient Party shall issue a written confirmation that an individual has been issued a Personnel Security Clearance or a legal entity has been issued a Facility Security Clearance.

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

ARTICLE 13
BREACH OF SECURITY

13.1 In the event of a Breach of Security 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 notify the National Security Authority of the Originating Party thereof in writing and ensure the initiation of an appropriate investigation.

13.2 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 any further breaches. Upon request, the Originating Party shall provide appropriate assistance; it shall be informed of the outcome of the investigation and the corrective measures taken due to the breach.

13.3 When a Breach of Security has occurred in a Third Party, the National Security Authority of the Third Party shall be requested by the National Security Authority of the Recipient Party to take without delay the measures referred to in the second paragraph of this article.

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 implementation of this Agreement shall be settled by consultation and/or negotiation between the Parties and shall not be referred to any national or international tribunal or to any third party for settlement.

ARTICLE 16
FINAL PROVISIONS

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

16.2 This Agreement may be amended by the mutual, written consent of the Parties. Such amendments shall enter into force in accordance with the procedure set forth in the first paragraph of this article.

16.3 This Agreement shall be concluded for an indefinite period. Either Party may terminate this Agreement by giving a written notice of termination to the other Party through diplomatic channels. In such case, this Agreement will be terminated six (6) months after the date of the receipt of the termination notice by the other Party.

16.4 In the event of termination of this Agreement, any Classified Information exchanged or generated under this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

16.5 Where necessary, the National Security Authorities or any other competent security authorities of the Parties may consult each other on detailed technical aspects relating to the application of this Agreement and may conclude, on a case-by-case basis, appropriate legal instruments or specific security protocols in order to complement this Agreement.

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

Done at Athens, on this 24th day of October 2024, in two originals, each in the Greek, French and English languages and 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
Grigorios P. Bountliakis

Director of the E’ Branch of the Hellenic National Defence General Staff

For the Government of the Grand Duchy of Luxembourg

Elisabeth Cardoso

Ambassador of the Grand Duchy of Luxembourg in Greece

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.

Παραγγέλλομε τη δημοσίευση του παρόντος στην Εφημερίδα της Κυβερνήσεως και την εκτέλεσή του ως νόμου του Κράτους.

Αθήνα, 21 Οκτωβρίου 2026

Ο Πρόεδρος της Δημοκρατίας
ΚΩΝΣΤΑΝΤΙΝΟΣ ΑΝ. ΤΑΣΟΥΛΑΣ

Οι Υπουργοί

Εθνικής Οικονομίας και Οικονομικών	Εξωτερικών	Εθνικής Άμυνας
ΚΥΡΙΑΚΟΣ ΠΙΕΡΡΑΚΑΚΗΣ	**ΓΕΩΡΓΙΟΣ ΓΕΡΑΠΕΤΡΙΤΗΣ**	**ΝΙΚΟΛΑΟΣ - ΓΕΩΡΓΙΟΣ Σ. ΔΕΝΔΙΑΣ**

Θεωρήθηκε και τέθηκε η Μεγάλη Σφραγίδα του Κράτους.

Αθήνα, 21 Οκτωβρίου 2026

Ο επί της Δικαιοσύνης Υπουργός
ΓΕΩΡΓΙΟΣ ΦΛΩΡΙΔΗΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ
Καποδιστρίου 34, 104 32 Αθήνα
Τηλ. Κέντρο 210 5279000
Αποστολή εγγράφων προς δημοσίευση στο ΦΕΚ
στην ηλεκτρονική διεύθυνση **https://eservices.et.gr**
0100171211026004