

No. 58056*

**Cyprus
and
Portugal**

Agreement between the Portuguese Republic and the Republic of Cyprus on the exchange and mutual protection of classified information. Nicosia, 8 October 2022

Entry into force: *1 January 2024, in accordance with article 16*

Authentic texts: *English, Greek and Portuguese*

Registration with the Secretariat of the United Nations: *Cyprus, 31 January 2024*

**No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

**Chypre
et
Portugal**

Accord entre la République portugaise et la République de Chypre relatif à l'échange et la protection mutuelle des informations classifiées. Nicosie, 8 octobre 2022

Entrée en vigueur : *1^{er} janvier 2024, conformément à l'article 16*

Textes authentiques : *anglais, grec et portugais*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Chypre,
31 janvier 2024*

**Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.*

[TEXT IN ENGLISH – TEXTE EN ANGLAIS]

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

**The Republic of Cyprus
and the
Portuguese Republic,**

hereinafter referred to as "the Parties",

Recognizing the need to set rules on protection of Classified Information mutually exchanged in the interest of national security within the scope of any form and area of co-operation, as well as, any Classified Information generated in the process of such co-operation;

Intending to ensure the mutual protection of Classified Information, which has been classified by one Party and transferred to the other Party in the course of co-operation between the Parties;

Desiring to create a set of rules on the mutual protection of Classified Information exchanged between the Parties;

Considering the mutual interest in the protection of Classified Information, in accordance with the legislation of the Parties;

Have agreed as follows:

Article 1

Objective

The objective of this Agreement is to ensure the protection of Classified Information that is generated or mutually exchanged between the Parties.

Article 2
Definitions

For the purposes of this Agreement:

- a) **"Classified Information"** means any information, regardless of its form or nature, which requires protection against unauthorised access or manipulation and for which a security classification level has been assigned, in accordance with the national legislation of the Parties;
- b) **"National Security Authority (NSA)"** means the state authority of each Party, which in accordance with its national legislation is responsible for the general implementation and supervision of this Agreement;
- c) **"Breach of Security"** means an act which is contrary or an omission to this Agreement or to the national legislation of the Parties, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;
- d) **"Classified Contract"** means an agreement between two or more Contractors or sub-contractors, which contains or involves access to, or the creation of Classified Information;
- e) **"Competent Security Authority"** means any competent authority of the Parties other than the NSA's that according to its national legislation, is responsible for the implementation of this Agreement;
- f) **"Contractor"** means a natural person, or a legal entity possessing the legal capacity to conclude or undertake Classified Contracts;
- g) **"Facility Security Clearance"** means the positive decision by the National Security Authority confirming that a natural person or the legal entity has the physical and organisational capability to handle and store Classified Information in accordance with the respective national legislation of both Parties;
- h) **"Need-to-know"** means the principle whereby access to specific Classified Information is granted exclusively in the scope of a given official position and for the performance of a specific task;
- i) **"Providing Party"** means the Party that creates or provides classified information to the Receiving Party;

- j) "Personnel Security Clearance" means the positive decision by the National Security Authority confirming, in accordance with the respective national legislation of the Parties, that a natural person is authorized to have access to and handle Classified Information up to a specific classification level;
- k) "Receiving Party" means the Party to which Classified Information is transmitted.
- l) "Third Party" means any State, organisation, legal or natural person, which is not a party to this Agreement.

Article 3

Security Classification Levels

The Parties agree that the following security classification levels and markings are equivalent and correspond to the security classification levels specified in their respective national legislation:

For the Republic of Cyprus	For the Portuguese Republic	Equivalent in English
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	MUITO SECRETO	TOP SECRET
ΑΠΟΡΡΗΤΟ	SECRETO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENCIAL	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESERVADO	RESTRICTED

Article 4

Security Authorities

1. The National Security Authorities of the Parties are:

For the Republic of Cyprus:

National Security Authority

Ministry of Defence of the Republic of Cyprus

For the Portuguese Republic:

National Security Authority

Presidency of the Council of Ministers

2. The National Security Authorities shall inform each other, in writing, through diplomatic channels, of any changes regarding the designation of the National Security Authorities.

3. The National Security Authorities shall provide each other with their official contact details and shall inform each other of any subsequent changes.

4. Any changes regarding the National Security Authorities shall not constitute an amendment to this Agreement.

5. The National Security Authorities shall inform each other of their respective national legislation on Classified Information and of any significant amendments thereto and shall exchange information about the security standards, procedures and practices for the protection of Classified Information.

Article 5

Protection Measures and Access to Classified Information

1. In accordance with their national legislation, the Parties shall take all necessary measures for the protection of Classified Information that is created or exchanged under this Agreement.

2. The Parties shall afford to Classified Information created or provided under this Agreement the same level of protection as they would to their own Classified Information of the equivalent security classification level, as set forth in Article 3 of this Agreement.

3. The Providing Party shall inform in writing:

- a) The Receiving Party of any conditions of release or limitations on the use of the Classified Information;
- b) The Receiving Party about any change of the security classification level of the transmitted Classified Information.

4. Classified Information shall only be made accessible to natural persons or legal entities who are authorized in accordance with the respective national legislation to have access to Classified Information of the equivalent security classification level and on a Need to-know basis.

5. Within the scope of this Agreement, each Party shall recognise the Personnel Security Clearances and Facility Security Clearances issued by the other Party.

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

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

8. The Receiving Party shall:

a) Release Classified Information to any Third Party only upon receipt of the prior written consent of the Providing Party.

b) Mark the received Classified Information in accordance with Article 3 of this Agreement;

c) Use Classified Information solely for the purposes which it has been provided for.

9. Upon a request of the National Security Authority of the Providing Party, the National Security Authority of the Receiving Party shall issue a written confirmation that an individual has the right to access Classified Information.

10. The Competent Security Authorities of the Parties, within the spirit of good will for mutual co-operation, and understanding, may visit each other in order to discuss and exchange views, experiences, lessons learned and technical knowledge in the fields of physical security, electronic security, industrial security, vetting procedures and any other issues related to the security of Classified Information.

11. Access to Classified Information of both Parties, by natural persons from a Third Party shall only be authorized after a written consent of the National Security Authority of the Providing Party.

Article 6

Transmission of Classified Information

1. Classified Information shall be transmitted between the Parties, in accordance with the national legislation of the Providing Party, normally through the diplomatic channels, or as otherwise arranged between the Competent Security Authorities.

2. The Receiving Party shall confirm, in writing, the receipt of the Classified Information.

3. Classified Information marked as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET shall be transmitted through Government to Government channels in accordance with the national legislations of the Parties.
4. As a minimum-security requirement Classified Information marked as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET shall be carried by, and under the sole control of a Government courier holding a Personnel Security Clearance of the same level.
5. The Receiving Party shall confirm the receipt of Classified Information of level ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET in writing.
6. Classified Information marked as ΑΠΟΡΡΗΤΟ / SECRETO / SECRET or ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL shall be transmitted through Government to Government channels in accordance with the national legislation of the Parties, or through other secure channels mutually approved by the National Security Authorities of both Parties.
7. The Receiving Party shall confirm the receipt of ΑΠΟΡΡΗΤΟ / SECRETO / SECRET and ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL level of Classified Information in writing.
8. Classified Information marked as ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED shall be transmitted through secure channels in accordance with the national legislation of the Parties.
9. The procedures for the carriage of large consignments containing Classified Information shall be jointly agreed and evaluated, on a case-by case basis, by the National Security Authority of both Parties.
10. If Classified Information marked as ΑΠΟΡΡΗΤΟ / SECRETO / SECRET, ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL or ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED is to be transmitted electronically between the Parties, it shall not be sent in clear text.
11. Electronic transmission of the specific classification levels referred in the previous article shall be carried out through certified cryptographic means mutually approved by the National Security Authorities.

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

For the Republic of Cyprus:

The Central TOP SECRET Registry at the Ministry of Foreign Affairs.

For the Portuguese Republic:

The Central Registry at the National Security Authority.

13. Without prejudice to Paragraph 12 of this Article, whenever deemed necessary, by the Security Forces, the Military Forces or the Police, to exchange Classified information, this exchange shall be done in accordance with the national legislation of the Parties.

14. The main points of entry and exit for this category of Classified Information shall be agreed by the Security Forces, Military Forces, or the Police upon a prior written consent and approval of the National Security Authorities of the Parties.

Article 7

Reproduction and Translation of Classified Information

1. Translations and reproductions of Classified Information shall be made in accordance with the national legislation of the Receiving Party and the following procedures:

- a) The translations and the reproductions shall be marked and protected as the original Classified Information;
- b) The translations and the number of copies shall be limited to that required for official purposes;
- c) The translations shall bear an appropriate annotation in the language of the translation indicating that it contains Classified Information received from the Providing Party

2. Classified Information marked as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET or ΑΠΟΡΡΗΤΟ / SECRETO / SECRET shall be translated or reproduced only upon the prior written consent of the Providing Party.

Article 8

Destruction of Classified Information

1. Classified Information shall be destroyed in a way that prevents its partial or total reconstruction.
2. Classified Information marked up to ΑΠΟΡΡΗΤΟ / SECRETO / SECRET shall be destroyed in accordance with the national legislation of the Parties.
3. Classified Information marked as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / ΜΥΙΤΟ SECRETO / TOP SECRET shall not be destroyed and shall be returned to the National Security Authority of the Providing Party.
4. A report on destruction of Classified Information shall be made and its translation in English shall be delivered to the National Security Authority of the Providing Party.
5. In case of a crisis situation in which it is impossible to protect or return Classified Information it shall be destroyed immediately, and the Receiving Party shall inform the National Security Authority of the Providing Party about this destruction as soon as possible.

Article 9

Classified Contracts

1. The National Security Authority of a Party shall provide to the National Security Authority of the other Party prior written assurance that a Contractor or a sub contractor wishing to undertake a Classified Contract marked as ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL and ΑΠΟΡΡΗΤΟ / SECRETO / SECRET holds or is in the process of obtaining a Facility Security Clearance of the appropriate security classification level.
2. Each National Security Authority may request the other to carry out a security inspection in a facility located in their State's territory in order to ensure continuing compliance with security standards according to the respective national legislation.
3. Each Classified Contract in accordance with this Agreement shall include:
 - a) A commitment to comply with the provisions of the present Agreement;
 - b) A commitment of the Contractor or sub-contractor to ensure that their premises have necessary conditions for handling and storing Classified Information of a given security classification level;

- c) A commitment of the Contractor or sub contractor to ensure that persons who perform duties requiring access to Classified Information are duly authorised in accordance with their national legislation to have access to Classified Information of the equivalent security classification level and have been regularly security briefed;
- d) A list of Classified Information involved and a list of areas in which Classified Information will be handled and stored;
- e) The procedures for the transportation of Classified Information;
- f) Communication channels and means for electronic transmission.
- g) A commitment of the Contractor or sub-contractor to notify its National Security Authority of any actual or suspected Breach of Security;
- h) A commitment of the Contractor or sub-contractor to forward a copy of the Classified Contract to the National Security Authority of both Parties.

4. A Facility Security Clearance and a Personnel Security Clearance are not required for Classified Contracts that are limited to Classified Information marked as ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

5. Classified Contracts referred to in Paragraph 4 of this Article, shall contain an appropriate security requirement clause defining the minimum security requirement to be applied by the Contractor to Classified Information that is generated and / or provided as a result of the Contract.

6. The security clause referred to in Paragraph 5 of this Article, shall include a provision concerning the appointment, by the Contractor, of a person who has the overall responsibility of the protection of Classified Information marked as ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

7. A copy of the security requirement provision referred to in Paragraph 6 of this Article shall be provided to the National Security Authority, only upon request.

Article 10

Visits

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

2. The National Security Authority of the host Party shall receive a request for a visit at least 20 (twenty) days in advance.
3. In urgent cases, the request for a visit is submitted in shorter time.
4. The request for a visit shall include:
 - a) The visitor's name and surname, place and date of birth, citizenship, passport or identification document number;
 - b) The name of the legal person represented by the visitor and position of the visitor in the legal entity;
 - c) The name, address and contact information of the legal entity and the facility to be visited;
 - d) The confirmation of the visitor's Personnel Security Clearance, its validity and level;
 - e) The object and purpose of the visit and the highest Security Classification Level of Classified Information to be involved;
 - f) The expected date and duration of the requested visit and, in case of recurring visits, the total period covered by the visits shall be stated;
 - g) The date, signature and the official seal of the National Security Authority.
5. Once the visit has been approved, the National Security Authority of the host Party shall provide a copy of the request for visit to the security officer of the legal entity to be visited.
6. The validity of visit approval shall not exceed twelve (12) months.
7. The National Security Authority of the Party that receives the request for visit shall inform, in due time, the National Security Authority of the requesting Party about the decision.
8. The National Security Authorities of the Parties may draw up lists of individuals authorised to make recurring visits and shall be valid for an initial period of twelve (12) months and, upon agreement, may be extended for a further period of time not exceeding another twelve (12) months.
9. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited, in accordance with the terms and conditions agreed upon.

Article 11

Breach of Security

1. In case of actual or suspected Breach of Security, the National Security Authority of the Party where it has occurred shall inform, without delay and in writing, the National Security Authority of the Providing Party and initiate appropriate proceedings in accordance with national laws and regulations, in order to determine the circumstances of the Breach of Security, the extent of the damage and the measures adopted for its mitigation.
2. If a Breach of Security occurs in a Third Party, the National Security Authority of the Party who released the information to the Third Party shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 of this Article are initiated.
3. The Providing Party shall, upon request, cooperate in the investigation in accordance with paragraph 1 of this Article.
4. The Providing Party shall be informed of the results of the investigation and shall receive the final report on the causes and degree of damage.

Article 12

Expenses

Each Party shall bear its own expenses incurred in the implementation of this Agreement and its supervision.

Article 13

Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiations between the Parties, through diplomatic channels.

Article 14

Amendments

1. This agreement may be amended on the basis of mutual written approval of the Parties.
2. The amendments shall enter into force according to the terms specified in Article 16.

Article 15

Duration and termination

1. This Agreement shall remain in force for an undetermined period.
2. Each Party may, at any time, terminate this Agreement by written notification to the other Party through diplomatic channels.
3. The Agreement shall be terminated six (6) months following the date of the receipt of the aforementioned notification.
4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Providing Party exonerates the Receiving Party from this obligation.

Article 16

Entry into force

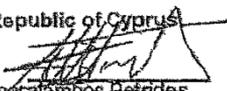
The present agreement shall enter into force on the first day of the second month after the date of the receipt of the last written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

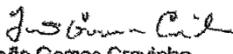
Article 17

Registration

Upon the entry into force of this Agreement, the Party in whose territory this Agreement is signed shall transmit it to the Secretariat of the United Nations for registration, in accordance with Article 102 of the Charter of the United Nations and shall notify the other Party of the completion of this procedure as well as of its registration number.

Done at Nicosia, on 08 October 2022, in two originals, each in the Greek, Portuguese and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the
Republic of Cyprus

Charalambos Petrides
Minister of Defence

For the
Portuguese Republic

João Gomes Cravinho
Minister of Foreign Affairs

[TEXT IN GREEK – TEXTE EN GREC]

ΠΙΝΑΚΑΣ
ΜΕΡΟΣ Ι
(Κείμενο στην ελληνική γλώσσα)
ΣΥΜΦΩΝΙΑ
ΜΕΤΑΞΥ
ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ
ΚΑΙ
ΤΗΣ ΠΟΡΤΟΓΑΛΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ
ΓΙΑ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΚΑΙ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤ
ΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η Κυπριακή Δημοκρατία
και η
Πορτογαλική Δημοκρατία,

εφεξής καλούμενες «τα Μέρη».

Αναγνωρίζοντας την ανάγκη για τον καθορισμό κανόνων σχετικά με την προστασία Διαβαθμισμένων Πληροφοριών, τις οποίες ανταλλάσσουν προς το συμφέρον της εθνικής ασφάλειας στο πλαίσιο οποιασδήποτε μορφής και τομέα συνεργασίας, καθώς και οποιωνδήποτε Διαβαθμισμένων Πληροφοριών που προκύπτουν από τη διαδικασία της εν λόγω συνεργασίας.

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία των Διαβαθμισμένων Πληροφοριών, οι οποίες διαβαθμίστηκαν από το ένα μέρος και διαβίβαστηκαν στα άλλα μέρη στο πλαίσιο συνεργασίας μεταξύ των Μερών.

Επιθυμώντας να θεσπίσουν κανόνες για την αμοιβαία προστασία των Διαβαθμισμένων Πληροφοριών, τις οποίες ανταλλάσσουν τα Μέρη μεταξύ τους.

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

Συμφώνησαν ως ακολούθως:

Άρθρο 1
Σκοπός

Σκοπός της παρούσας Συμφωνίας είναι η διασφάλιση της προστασίας Διαβαθμισμένων Πληροφοριών, τις οποίες παράγουν ή ανταλλάσσουν μεταξύ τους τα Μέρη.

Άρθρο 2 Ορισμοί

Για τους σκοπούς της παρούσας Συμφωνίας:

- α) «Διαβαθμισμένες Πληροφορίες» σημαίνει κάθε πληροφορία, ανεξαρτήτως τύπου ή φύσεως, η οποία χρήζει προστασίας από μη εξουσιοδοτημένη πρόσβαση ή χειρισμό και διαβαθμίστηκε με κάποιο επίπεδο διαβάθμισης ασφαλείας, σύμφωνα με την εθνική νομοθεσία των Μερών,
- β) «Εθνική Αρχή Ασφαλείας» σημαίνει την αρχή κάθε Μέρους, η οποία σύμφωνα με την εθνική νομοθεσία του είναι υπεύθυνη για τη γενική εφαρμογή και επιτοπεία της παρούσας Συμφωνίας,
- γ) «Παραβίαση Ασφαλείας» σημαίνει πράξη ή παράλειψη, η οποία αντιβαίνει στην παρούσα Συμφωνία ή στην εθνική νομοθεσία των Μερών και το αποτέλεσμα της οποίας ενδέχεται να οδηγήσει σε γνωστοποίηση, απώλεια, καταστροφή, παράνομη χρήση ή οποιαδήποτε άλλη διακροή Διαβαθμισμένων Πληροφοριών,
- δ) «Διαβαθμισμένη Σύμβαση» σημαίνει κάθε συμφωνία μεταξύ δύο ή περισσότερων εργολάβων ή υπεργολάβων και η οποία περιέχει ή περιλαμβάνει πρόσβαση σε Διαβαθμισμένες Πληροφορίες ή δημιουργία Διαβαθμισμένων Πληροφοριών,
- ε) «Αρμόδια Αρχή Ασφαλείας» σημαίνει οποιαδήποτε αρμόδια αρχή των Μερών πλην των Εθνικών Αρχών Ασφαλείας, η οποία, σύμφωνα με την εθνική νομοθεσία των Μερών, είναι υπεύθυνη για την εφαρμογή της παρούσας Συμφωνίας,
- στ) «Εργολάβος» σημαίνει το φυσικό ή νομικό πρόσωπο που έχει τη νομική ικανότητα σύναψης ή ανάληψης διαβαθμισμένων συμβάσεων,
- ζ) «Εξουσιοδότηση Ασφαλείας Φορέας» σημαίνει τη θετική απόφαση της Εθνικής Αρχής Ασφαλείας, η οποία επιβεβαιώνει ότι κάποιο φυσικό ή νομικό πρόσωπο έχει την τεχνική και οργανωτική ικανότητα να χειρίζεται και να αποθηκεύει Διαβαθμισμένες Πληροφορίες, σύμφωνα με την αντίστοιχη εθνική νομοθεσία και των δύο Μερών,
- η) «Ανάγκη για γνώση» σημαίνει την αρχή βάσει της οποίας παρέχεται πρόσβαση σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες αποκλειστικά στο πλαίσιο συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας,
- θ) «Μέρος Αποστολέας» σημαίνει το Μέρος, το οποίο δημιουργεί και παρέχει Διαβαθμισμένες Πληροφορίες στο Μέρος Παραλήπτη,

- ι) «Εξουσιοδότηση Ασφαλείας Προσωπικού» σημαίνει τη θετική απόφαση της Εθνικής Αρχής Ασφαλείας, η οποία επιβεβαιώνει, σύμφωνα με την αντίστοιχη εθνική νομοθεσία των Μερών, ότι κάποιο φυσικό πρόσωπο εξουσιοδοτείται να έχει πρόσβαση σε και να χειρίζεται Διαβαθμισμένες Πληροφορίες έως κάποιο συγκεκριμένο επίπεδο διαβάθμισης.
- ια) «Μέρος Παραλήπτης» σημαίνει το Μέρος, στο οποίο διαβιβάζονται Διαβαθμισμένες Πληροφορίες.
- ιβ) «Τρίτο Μέρος» σημαίνει οποιαδήποτε κράτος, οργανισμό, νομικό ή φυσικό πρόσωπο, το οποίο δεν είναι συμβαλλόμενο μέρος στην παρούσα Συμφωνία.

Άρθρο 3

Επίπεδα Διαβάθμισης Ασφαλείας

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

Για την Κυπριακή Δημοκρατία	Για την Πορτογαλική Δημοκρατία	Αντίστοιχη αγγλική ορολογία
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	MUITO SECRETO	TOP SECRET
ΑΠΟΡΡΗΤΟ	SECRETO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENCIAL	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESERVADO	RESTRICTED

Άρθρο 4

Αρχές Ασφαλείας

1. Οι Εθνικές Αρχές Ασφαλείας των Μερών είναι:

Για την Κυπριακή Δημοκρατία:

Εθνική Αρχή Ασφαλείας

Υπουργείο Άμυνας της Κυπριακής Δημοκρατίας

Για την Πορτογαλική Δημοκρατία:

Εθνική Αρχή Ασφαλείας

Προεδρία του Υπουργικού Συμβουλίου

2. Οι Εθνικές Αρχές Ασφαλείας αλληλοενημερώνονται γραπτώς, μέσω της διπλωματικής οδού, για τυχόν αλλαγές που αφορούν στις Εθνικές Αρχές Ασφαλείας.
3. Οι Εθνικές Αρχές Ασφαλείας ανταλλάσσουν τα επίσημα στοιχεία επικοινωνίας τους και αλληλοενημερώνονται για τυχόν μεταγενέστερες αλλαγές.
4. Τυχόν αλλαγές αναφορικά με τις Εθνικές Αρχές Ασφαλείας δεν αποτελούν τροποποίηση της παρούσας Συμφωνίας.
5. Οι Εθνικές Αρχές Ασφαλείας αλληλοενημερώνονται για την αντίστοιχη εθνική νομοθεσία περί Διαβαθμισμένων Πληροφοριών και για τυχόν σημαντικές τροποποιήσεις σε αυτή και ανταλλάσσουν πληροφορίες σχετικά με τα πρότυπα, τις διαδικασίες και πρακτικές που αφορούν στην προστασία Διαβαθμισμένων Πληροφοριών.

Άρθρο 5

Μέτρα Προστασίας και Πρόσβαση σε Διαβαθμισμένες Πληροφορίες

1. Σύμφωνα με την εθνική τους νομοθεσία, τα Μέρη λαμβάνουν όλα τα κατάλληλα μέτρα για την προστασία Διαβαθμισμένων Πληροφοριών, τις οποίες δημιουργούν ή ανταλλάσσουν βάσει της παρούσας Συμφωνίας.
2. Τα Μέρη θα παρέχουν στις Διαβαθμισμένες Πληροφορίες, οι οποίες παράγονται ή και παρέχονται βάσει της παρούσας Συμφωνίας, το ίδιο επίπεδο ασφαλείας, όπως προβλέπεται για τις εθνικές τους Διαβαθμισμένες Πληροφορίες του αντίστοιχου Επιπέδου Διαβάθμισης Ασφαλείας, σύμφωνα με το Άρθρο 3 της παρούσας Συμφωνίας.
3. Το Μέρος Αποστολέας ενημερώνει γραπτώς:
 - α) το Μέρος Παραλήπτη για τυχόν προϋποθέσεις κυκλοφορίας ή περιορισμούς στη χρήση των Διαβαθμισμένων Πληροφοριών,
 - β) το Μέρος Παραλήπτη για τυχόν αλλαγή στο Επίπεδο Διαβάθμισης Ασφαλείας των διαβιβασθέντων Διαβαθμισμένων Πληροφοριών.
4. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται μόνο σε φυσικά ή νομικά πρόσωπα που εξουσιοδοτούνται σύμφωνα με την αντίστοιχη εθνική νομοθεσία να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας και βάσει της αρχής της ανάγκης για γνώση.
5. Στο πλαίσιο της παρούσας Συμφωνίας, κάθε Μέρος αναγνωρίζει τις Εξουσιοδοτήσεις Ασφαλείας Προσωπικού και Εξουσιοδοτήσεις Ασφαλείας Φορέα, οι οποίες εκδίδονται από το άλλο Μέρος.

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

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

8. Το Μέρος Παραλήπτης:

- α) Υποβάλλει Διαβαθμισμένες Πληροφορίες σε τυχόν τρίτο μέρος μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα,
- β) Διαβαθμίζει την παραληφθείσα πληροφορία σύμφωνα με το Άρθρο 3 της παρούσας Συμφωνίας,
- γ) Χρησιμοποιεί Διαβαθμισμένες Πληροφορίες μόνο για τους σκοπούς για τους οποίους προβλέπονται.

9. Κατόπιν αιτήματος της Εθνικής Αρχής Ασφαλείας του Μέρους Αποστολέα, η Εθνική Αρχή Ασφαλείας του Μέρους Παραλήπτη εκδίδει γραπτή επιβεβαίωση ότι συγκεκριμένο άτομο έχει δικαίωμα πρόσβασης σε Διαβαθμισμένες Πληροφορίες.

10. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών, εντός του πνεύματος καλής θέλησης για αμοιβαία συνεργασία και κατανόηση, δύνανται να ανταλλάζουν επισκέψεις για να συζητούν και να ανταλλάζουν απόψεις, εμπειρίες, διδάγματα και τεχνική γνώση στους τομείς της φυσικής, ηλεκτρονικής και βιομηχανικής ασφάλειας, των διαδικασιών ελέγχου ασφαλείας και οποιαδήποτε άλλα θέματα σχετίζονται με την ασφάλεια Διαβαθμισμένων Πληροφοριών.

11. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες και των δύο Μερών από φυσικά πρόσωπα Τρίτου Μέρους επιτρέπεται μόνο κατόπιν γραπτής συγκατάθεσης της Εθνικής Αρχής Ασφαλείας του Μέρους Αποστολέα.

Άρθρο 6

Διαβίβευση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται μεταξύ των Μερών, σύμφωνα με την εθνική νομοθεσία του Μέρους Αποστολέα, κανονικά μέσω της διπλωματικής οδού, ή διαφορετικά σύμφωνα με τρόπο που συμφωνούν οι Αρμόδιες Αρχές Ασφαλείας μεταξύ τους.
2. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη Διαβαθμισμένων Πληροφοριών.
3. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / ΜΥΙΤΟ ΣΕΚΡΕΤΟ / TOP SECRET διαβιβάζονται μέσω κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών.
4. Ως ελάχιστο επίπεδο ασφαλείας, πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΩΣ ΑΠΟΡΡΗΤΟ / ΜΥΙΤΟ ΣΕΚΡΕΤΟ / TOP SECRET μεταφέρονται από και υπό τον αποκλειστικό έλεγχο κυβερνητικού μεταφορέα, ο οποίος κατέχει Εξουσιοδότηση Ασφαλείας Προσωπικού στο ίδιο επίπεδο.
5. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / ΜΥΙΤΟ ΣΕΚΡΕΤΟ / TOP SECRET.
6. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / ΣΕΚΡΕΤΟ / ΣΕΚΡΕΤ ή ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL διαβιβάζονται μέσω κυβερνητικής οδού σύμφωνα με την εθνική νομοθεσία των Μερών, ή μέσω άλλης ασφαλούς οδού, την οποία έχουν εγκρίνει αμοιβαία οι Εθνικές Αρχές Ασφαλείας και των δύο Μερών.
7. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / ΣΕΚΡΕΤΟ / ΣΕΚΡΕΤ και ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL.
8. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED διαβιβάζονται μέσω ασφαλούς οδού σύμφωνα με την εθνική νομοθεσία των Μερών.
9. Οι διαδικασίες για τη μεταφορά μεγάλων φορτίων που περιέχουν Διαβαθμισμένες Πληροφορίες αξιολογούνται και συμφωνούνται από κοινού από τις Εθνικές Αρχές Ασφαλείας, για κάθε περίπτωση ξεχωριστά.

10. Εάν πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET, ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL ή ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED πρόκειται να διαβιβαστούν ηλεκτρονικά μεταξύ των Μερών, δεν αποστέλλονται υπό μορφή απλού κειμένου.

11. Η ηλεκτρονική διαβίβαση τέτοιων συγκεκριμένων Επιπέδων Διαβάθμισης Ασφαλείας γίνεται μέσω πιστοποιημένων κρυπτογραφικών μέσων, τα οποία έχουν εγκριθεί αμοιβαία από τις Εθνικές Αρχές Ασφαλείας.

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

Για την Κυπριακή Δημοκρατία:

Η Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ του Υπουργείου Εξωτερικών.

Για την Πορτογαλική Δημοκρατία:

Το Κεντρικό Μητρώο της Εθνικής Αρχής Ασφαλείας.

13. Τηρουμένης της Παραγράφου 12 του παρόντος Άρθρου, όποτε η ανταλλαγή Διαβαθμισμένων Πληροφοριών κρίνεται αναγκαία από τις Δυνάμεις Ασφαλείας, το Στρατό ή την Αστυνομία, η ανταλλαγή αυτή θα γίνεται σύμφωνα με την εθνική νομοθεσία των Μερών.

14. Τα κύρια σημεία εισόδου και εξόδου για αυτή την κατηγορία Διαβαθμισμένων Πληροφοριών θα συμφωνούνται από τις Δυνάμεις Ασφαλείας, το Στρατό ή την Αστυνομία, κατόπιν γραπτής συγκατάθεσης και έγκρισης των Εθνικών Αρχών Ασφαλείας των Μερών.

Άρθρο 7

Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών

1. Οι μεταφράσεις και οι αναπαραγωγές Διαβαθμισμένων Πληροφοριών θα γίνονται σύμφωνα με την εθνική νομοθεσία του Μέρους Παραλήπτη και με τις ακόλουθες διαδικασίες:

- α) Οι μεταφράσεις και οι αναπαραγωγές διαβαθμίζονται και προστατεύονται όπως και οι πρωτότυπες Διαβαθμισμένες Πληροφορίες,
- β) Οι μεταφράσεις και ο αριθμός των αντιγράφων περιορίζονται στον αριθμό που απαιτείται για επίσημους σκοπούς,
- γ) Οι μεταφράσεις φέρουν κατάλληλη σημείωση στη γλώσσα μετάφρασης υποδεικνύοντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες που λήφθηκαν από το Μέρος Αποστολέα.

2. Πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET αναπαράγονται μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα.

Άρθρο 8

Καταστροφή Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες καταστρέφονται με τέτοιο τρόπο ώστε να αποφεύγεται η μερική ή ολική ανακατασκευή τους.
2. Οι πληροφορίες που έχουν διαβαθμιστεί έως το Επίπεδο Διαβάθμισης Ασφαλείας ΑΠΟΡΡΗΤΟ / SECRETO / SECRET καταστρέφονται σύμφωνα με την εθνική νομοθεσία των Μερών.
3. Οι πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / ΜΥΙΤΟ SECRETO / TOP SECRET δεν καταστρέφονται. Επιστρέφονται στην Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα.
4. Συντάσσεται έκθεση για την καταστροφή των Διαβαθμισμένων Πληροφοριών και η μετάφρασή της στην αγγλική γλώσσα παραδίδεται στην Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα.
5. Σε περίπτωση κατάστασης κρίσης κατά την οποία δεν είναι δυνατή η προστασία ή η επιστροφή Διαβαθμισμένων Πληροφοριών, αυτές καταστρέφονται αμέσως. Το Μέρος Παραλήπτης ενημερώνει την Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα σχετικά με την εν λόγω καταστροφή τα συντομότερο δυνατόν.

Άρθρο 9

Διαβαθμισμένες Συμβάσεις

1. Η Εθνική Αρχή Ασφαλείας του ενός Μέρους παρέχει, εκ των προτέρων, στην Εθνική Αρχή Ασφαλείας του άλλου Μέρους γραπτή επιβεβαίωση ότι, ο εργολάβος ή ο υπεργολάβος που επιθυμεί να συνάψει διαβαθμισμένη σύμβαση με Επίπεδο Διαβάθμισης Ασφαλείας ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL και ΑΠΟΡΡΗΤΟ / SECRETO / SECRET, διαθέτει ή έχει κινήσει διαδικασίες για την εξασφάλιση Εξουσιοδότηση Ασφαλείας Φορέα στο κατάλληλο Επίπεδο Διαβάθμισης Ασφαλείας.

2. Κάθε Εθνική Αρχή Ασφαλείας δύναται να ζητήσει από την άλλη να διεξάγει επιθεώρηση ασφαλείας στις εγκαταστάσεις που βρίσκονται στην επικράτεια του κράτους τους για να διασφαλίσει τη συνεχιζόμενη συμμόρφωση με τα πρότυπα ασφαλείας σύμφωνα με την αντίστοιχη εθνική νομοθεσία.

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

- α) Δέσμευση συμμόρφωσης με τις πρόνοιες της παρούσας Συμφωνίας.
- β) Δέσμευση του εργολάβου ή του υπεργολάβου με την οποία διασφαλίζεται ότι, τα υποστατικά του πληρούν τις απαραίτητες προϋποθέσεις για χειρισμό και αποθήκευση Διαβαθμισμένων Πληροφοριών ενός συγκεκριμένου Επιπέδου Διαβάθμισης Ασφαλείας,
- γ) Δέσμευση του εργολάβου ή του υπεργολάβου με την οποία διασφαλίζεται ότι, όλα τα άτομα που εκτελούν καθήκοντα τα οποία απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες είναι δεόντως εξουσιοδοτημένα, σύμφωνα με την εθνική τους νομοθεσία, να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες με το αντίστοιχο Επίπεδο Διαβάθμισης Ασφαλείας και ότι ενημερώνονται τακτικά σε θέματα ασφαλείας,
- δ) Κατάλογο των Διαβαθμισμένων Πληροφοριών και των χώρων χειρισμού και αποθήκευσης Διαβαθμισμένων Πληροφοριών,
- ε) Τη διαδικασία μεταφοράς Διαβαθμισμένων Πληροφοριών,
- στ) Οδούς επικοινωνίας και μέσα ηλεκτρονικής διαβίβασης,
- ζ) Δέσμευση του εργολάβου ή του υπεργολάβου να ενημερώνει τις αντίστοιχες Εθνικές Αρχές Ασφαλείας του για τυχόν πραγματική ή ενδεχόμενη Παραβίαση Ασφαλείας,
- η) Δέσμευση του εργολάβου ή του υπεργολάβου να προωθήσει αντίγραφο της Διαβαθμισμένης Σύμβασης στις Εθνικές Αρχές Ασφαλείας και των δύο Μερών.

4. Δεν απαιτείται Εξουσιοδότηση Ασφαλείας Φορέα ούτε και Εξουσιοδότηση Ασφαλείας Προσωπικού για Διαβαθμισμένες Συμβάσεις που περιορίζονται σε πληροφορίες με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

5. Οι Διαβαθμισμένες Συμβάσεις που αναφέρονται στην Παράγραφο 4 του παρόντος Άρθρου περιέχουν κατάλληλη ρήτρα απαίτησης ασφαλείας, η οποία ορίζει την ελάχιστη απαίτηση ασφαλείας που πρέπει να εφαρμοστεί από τον εργολάβο σε Διαβαθμισμένες Πληροφορίες που παράγονται ή και παρέχονται ως αποτέλεσμα της Σύμβασης.

6. Η ρήτρα ασφαλείας που αναφέρεται στην Παράγραφο 5 του παρόντος Άρθρου, περιέχει πρόνοια αναφορικά με τον διορισμό, από τον εργολάβο, προσώπου που έχει τη συνολική ευθύνη για την προστασία διαβαθμισμένων πληροφοριών με Επίπεδο Διαβάθμισης Ασφαλείας ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

7. Αντίγραφο της πρόνοιας απαίτησης ασφαλείας, η οποία αναφέρεται στην Παράγραφο 6 του παρόντος Άρθρου, παρέχεται στην Εθνική Αρχή Ασφαλείας, μόνο κατόπιν απαίτησης.

Άρθρο 10 Επισκέψεις

1. Οι επισκέψεις που αφορούν σε Διαβαθμισμένες Συμβάσεις και περιλαμβάνουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες υπόκεινται στην εκ των προτέρων γραπτή εξουσιοδότηση (έγκριση), την οποία παρέχει η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής.

2. Η Εθνική Αρχή Ασφαλείας του Μέρους υποδοχής θα πρέπει να λάβει αίτηση επίσκεψης τουλάχιστον 20 (είκοσι) ημέρες νωρίτερα.

3. Σε έκτακτες περιπτώσεις η αίτηση επίσκεψης μπορεί να διαβιβαστεί εντός συντομότερης προθεσμίας.

4. Η αίτηση επίσκεψης περιλαμβάνει:

- α) Το ονοματεπώνυμο του επισκέπτη, τον τόπο και την ημερομηνία γέννησης, την υπηκοότητα και τον αριθμό διαβατηρίου ή εγγράφου ταυτοποίησης,
- β) Την επωνυμία του νομικού προσώπου, το οποίο εκπροσωπεί ο επισκέπτης και τη θέση του επισκέπτη στο νομικό πρόσωπο,
- γ) Την επωνυμία, τη διεύθυνση και τα στοιχεία επικοινωνίας του νομικού προσώπου και των εγκαταστάσεων που πρόκειται να δεχθούν την επίσκεψη,
- δ) Επιβεβαίωση της Εξουσιοδότησης Ασφαλείας Προσωπικού του επισκέπτη, της εγκυρότητάς και του επιπέδου αυτής,

- ε) Τον σκοπό και τους λόγους της επίσκεψης, καθώς και το υψηλότερο Επίπεδο Διαβάθμισης Ασφαλείας των Διαβαθμισμένων Πληροφοριών στις οποίες αφορά η επίσκεψη,
- στ) Την αναμενόμενη ημερομηνία και διάρκεια της επίσκεψης. Σε περίπτωση επαναλαμβανόμενων επισκέψεων, αναφέρεται η συνολική διάρκεια των επισκέψεων,
- ζ) Την ημερομηνία, την υπογραφή και την επίσημη σφραγίδα της Εθνικής Αρχής Ασφαλείας.

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

6. Η ισχύς της έγκρισης επίσκεψης δεν υπερβαίνει τους δώδεκα (12) μήνες.

7. Η Εθνική Αρχή Ασφαλείας του Μέρους που λαμβάνει την αίτηση για επίσκεψη ενημερώνει, εν ευθέτω χρόνω, την Εθνική Αρχή Ασφαλείας του αιτούντος Μέρους σχεπικά με την απόφαση.

8. Οι Εθνικές Αρχές Ασφαλείας των Μερών δύνανται να καταρτίσουν καταλόγους με φυσικά πρόσωπα, τα οποία είναι εξουσιοδοτημένα να κάνουν επαναλαμβανόμενες επισκέψεις. Οι κατάλογοι αυτοί ισχύουν για αρχική περίοδο δώδεκα (12) μηνών και κατόπιν συμφωνίας η περίοδος δύνανται να παραταθεί για περίοδο που δεν υπερβαίνει τους δώδεκα (12) μήνες.

9. Οι όροι των αντίστοιχων επισκέψεων θα καθορίζονται απευθείας από τα αρμόδια άτομα του νομικού προσώπου που πρόκειται να δεχτεί την επίσκεψη, σύμφωνα με τους όρους και προϋποθέσεις που θα συμφωνηθούν.

Άρθρο 11

Παραβίαση Ασφαλείας

1. Σε περίπτωση πραγματικής ή εικαζόμενης Παραβίασης Ασφαλείας, η Εθνική Αρχή Ασφαλείας του Μέρους όπου συνέβη ενημερώνει γραππώς και χωρίς καθυστέρηση την Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα και κινεί τις κατάλληλες διαδικασίες σύμφωνα με την εθνική νομοθεσία και κανονισμούς, για τη διαπίστωση των περιστάσεων της Παραβίασης Ασφαλείας, της έκτασης της ζημιάς και των μέτρων που υιοθετήθηκαν για τον μετριασμό της.

2. Εάν η Παραβίαση Ασφαλείας επέλθει σε Τρίτο Μέρος, η Εθνική Αρχή Ασφαλείας του Μέρους, το οποίο κοινοποίησε τις πληροφορίες στο Τρίτο Μέρος λαμβάνει όλα τα απαραίτητα μέτρα για να διασφαλίσει ότι, οι δράσεις που περιγράφονται στην Παράγραφο 1 του παρόντος Άρθρου έχουν τεθεί σε εφαρμογή.

3. Το Μέρος Αποστολέας, κατόπιν αιτήματος, συνεργάζεται στην έρευνα σύμφωνα με την Παράγραφο 1 του παρόντος Άρθρου.

4. Το Μέρος Αποστολέας ενημερώνεται για τα αποτελέσματα της έρευνας και λαμβάνει την τελική έκθεση για τα αίτια και τον βαθμό της ζημιάς.

Άρθρο 12

Έξοδα

Κάθε Μέρος αναλαμβάνει τα δικά του έξοδα, τα οποία θα προκύψουν από την εφαρμογή και εποπτεία της παρούσας Συμφωνίας.

Άρθρο 13

Διευθέτηση Διαφορών

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

Άρθρο 14

Τροποποιήσεις

1. Η παρούσα Συμφωνία δύναται να τροποποιείται με την αμοιβαία γραπτή έγκριση των Μερών.
2. Οι τροποποιήσεις τίθενται σε ισχύ σύμφωνα με τους όρους που αναφέρονται στο Άρθρο 16.

Άρθρο 15

Διάρκεια και Τερματισμός

1. Η παρούσα Συμφωνία συνάπτεται για απεριόριστο χρονικό διάστημα.
2. Κάθε Μέρος δύναται, ανά πάσα στιγμή, να τερματίσει τη Συμφωνία δίδοντας στο άλλο Μέρος γραπτή ειδοποίησή μέσω της διπλωματικής οδού.

3. Η Συμφωνία τερματίζεται έξι (6) μήνες μετά την ημερομηνία παραλαβής της προαναφερθείσας ειδοποίησης.

4. Σε περίπτωση τερματισμού της παρούσας Συμφωνίας, τα Μέρη διασφαλίζουν ότι, όλες οι Διαβαθμισμένες Πληροφορίες θα συνεχίσουν να προστατεύονται έως ότου το Μέρος Αποστολέας απαλλάξει το Μέρος Παραλήπτη από την εν λόγω υποχρέωση.

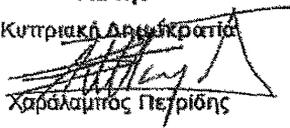
Άρθρο 16 Έναρξη ισχύος

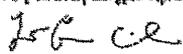
Η παρούσα Συμφωνία τίθεται σε ισχύ την πρώτη ημέρα του δεύτερου μήνα μετά την ημερομηνία λήψης της τελευταίας γραπτής ειδοποίησης με την οποία τα Μέρη ανακοινώνουν το ένα στο άλλο, μέσω της διπλωματικής οδού, ότι πληρούνται όλες οι αναγκαίες εθνικές νομικές προϋποθέσεις που απαιτούνται για την έναρξη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

Άρθρο 17 Καταχώρηση

Μετά την έναρξη ισχύος της παρούσας Συμφωνίας, το Μέρος στην επικράτεια του οποίου υπεγράφη η παρούσα Συμφωνία τη διαβιβάζει στη Γραμματεία των Ηνωμένων Εθνών προς καταχώρηση, σύμφωνα με το Άρθρο 102 της Χάρτας των Ηνωμένων Εθνών και ενημερώνει το άλλο Μέρος για την ολοκλήρωση της εν λόγω διαδικασίας, καθώς και για τον αριθμό καταχώρησής της.

Συντάχθηκε στην Λευκωσία, στις 08 Οκτωβρίου 2022, σε δύο πρωτότυπα, στην Ελληνική, Πορτογαλική και Αγγλική γλώσσα, και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση διαφωνίας στην ερμηνεία, το αγγλικό κείμενο υπερισχύει.

Για την
Κυπριακή Δημοκρατία

Χαράλαμπος Πετρίδης
Υπουργός Άμυνας

Για την
Πορτογαλική Δημοκρατία

João Gomes Cravinho
Υπουργός Εξωτερικών

[TEXT IN PORTUGUESE – TEXTE EN PORTUGAIS]

ΜΕΡΟΣ ΙΙ
(Κείμενο στην πορτογαλική γλώσσα)
ACORDO
ENTRE
A REPÚBLICA DE CHIPRE
E
A REPÚBLICA PORTUGUESA
SOBRE A TROCA E A PROTEÇÃO MÚTUA DE INFORMAÇÃO CLASSIFICADA

A República de Chipre
e a
República Portuguesa,

doravante designadas por "Partes",

Reconhecendo a necessidade de estabelecer normas para proteção da Informação Classificada mutuamente trocada no interesse da segurança nacional no âmbito de qualquer forma e área de cooperação, bem como, qualquer Informação Classificada gerada no processo dessa cooperação;

Pretendendo assegurar a proteção mútua da Informação Classificada, que tenha sido classificada por uma Parte e transferida para a outra Parte no âmbito da cooperação entre as Partes;

Desejando estabelecer um conjunto de regras sobre a proteção mútua da Informação Classificada trocada entre as Partes;

Considerando o mútuo interesse na proteção da Informação Classificada de acordo com o Direito nacional das Partes,

Acordam no seguinte:

Artigo 1.º

Objetivo

O objetivo do presente Acordo é garantir a proteção da Informação Classificada que é gerada ou mutuamente trocada entre as Partes.

Artigo 2.º

Definições

Para os efeitos do presente Acordo:

- a) **"Informação Classificada"** designa a informação, qualquer que seja a sua forma ou natureza, que necessita de proteção contra acesso não autorizado ou manipulação, à qual tenha sido atribuído um nível de classificação de segurança de acordo com o Direito nacional das Partes;
- b) **"Autoridade Nacional de Segurança (ANS)"** designa a autoridade estatal de cada Parte, a qual de acordo com o Direito nacional respetivo é responsável pela implementação e supervisão do presente Acordo;
- c) **"Quebra de Segurança"** designa uma ação contrária ou omissão ao presente Acordo ou ao respetivo Direito nacional das Partes, que possa levar à divulgação não autorizada, perda, destruição, apropriação indevida ou qualquer outro tipo de comprometimento da Informação Classificada;
- d) **"Contrato Classificado"** designa um acordo entre dois ou mais Cocontratantes ou subcontratados, que contém ou envolve acesso, ou criação de Informação Classificada;
- e) **"Autoridade de Segurança Competente"**, designa a autoridade competente das Partes, que não a ANS, que de acordo com o Direito respetivo das Partes é responsável pela implementação do presente Acordo;
- f) **"Cocontratante"** designa uma pessoa singular ou coletiva que tem capacidade jurídica para celebrar e empreender Contratos Classificados;
- g) **"Credenciação de Segurança Física"** designa a decisão positiva pela Autoridade Nacional de Segurança de que uma pessoa singular ou coletiva, tem a capacidade física e organizacional para manusear e armazenar Informação Classificada de acordo com o respetivo direito nacional de ambas as Partes;
- h) **"Necessidade de Conhecer"** designa o princípio segundo o qual o acesso a Informação Classificada é concedido exclusivamente no âmbito de um determinado cargo oficial e para o desempenho de uma tarefa específica;
- i) **"Parte Transmissora"** designa a Parte que cria ou disponibiliza a Informação Classificada à Parte Destinatária;

- j) "Credenciação de Segurança Pessoal" designa a decisão positiva da Autoridade Nacional de Segurança confirmando, de acordo com o Direito nacional respetivo das Partes, que uma pessoa singular está autorizada a aceder e manusear a Informação Classificada até um nível de classificação específico;
- k) "Parte Destinatária" designa a Parte à qual a Informação Classificada é transmitida;
- l) "Terceira Parte" designa qualquer Estado, organização, pessoa coletiva ou singular que não é Parte no presente Acordo.

Artigo 3.º

Níveis de Classificação de Segurança

As Partes acordam que os seguintes níveis e marcas de classificações de segurança são equivalentes e correspondem aos níveis de classificação de segurança previstos no Direito nacional respetivo:

Para a República de Chipre	Para a República Portuguesa	Equivalente em Inglês
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	MUITO SECRETO	TOP SECRET
ΑΠΟΡΡΗΤΟ	SECRETO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENCIAL	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESERVADO	RESTRICTED

Artigo 4.º

Autoridades de Segurança

1. As Autoridades Nacionais de Segurança das Partes são:

Pela República de Chipre:

Autoridade Nacional de Segurança

Ministério da Defesa da República de Chipre

Pela República Portuguesa:

Autoridade Nacional de Segurança

Presidência do Conselho de Ministros

2. As Autoridades Nacionais de Segurança informar-se-ão mutuamente, por escrito e por via diplomática, sobre qualquer alteração de designação das Autoridades Nacionais de Segurança.
3. As Autoridades Nacionais de Segurança fornecem uma à outra os seus contactos oficiais e informam-se de quaisquer alterações subsequentes.
4. Quaisquer alterações relativas às Autoridades Nacionais de Segurança não constituirão uma revisão deste Acordo.
5. As Autoridades Nacionais de Segurança informam-se mutuamente do respetivo Direito nacional sobre Informação Classificada e sobre quaisquer alterações significativas ao mesmo e devem trocar informações sobre as normas, procedimentos e práticas de segurança para a proteção da Informação Classificada.

Artigo 5.º

Medidas de Proteção e Acesso à Informação Classificada

1. Em conformidade com o Direito respetivo as Partes adotam as medidas necessárias à proteção da Informação Classificada criada ou trocada no âmbito do presente Acordo.
2. As Partes atribuem à Informação Classificada criada ou disponibilizada no âmbito do presente Acordo, o mesmo nível de proteção que atribuem à sua Informação Classificada com o equivalente nível de classificação de segurança como tal previsto no artigo 3º do presente Acordo.
3. A Parte Transmissora informa por escrito:
 - a) A Parte Destinatária de quaisquer condições de liberação ou limitações ao uso da Informação Classificada;
 - b) A Parte Destinatária de alterações ao nível de classificação da Informação Classificada transmitida.
4. A Informação Classificada só é acessível às pessoas singulares ou coletivas que de acordo com o Direito nacional respetivo estão autorizadas a aceder a Informação Classificada de equivalente nível de segurança e de acordo com a Necessidade de Conhecer.

5. No âmbito do presente Acordo, cada Parte reconhece a Credenciação de Segurança Pessoal e a Credenciação de Segurança Física atribuídas pela outra Parte.

6. As Autoridades Nacionais de Segurança de acordo com o Direito nacional respetivo assistem-se mutuamente, mediante solicitação, na realização dos procedimentos de verificação necessários para a aplicação do presente Acordo.

7. No âmbito do presente Acordo, as Autoridades de Segurança das Partes informam-se mutuamente e sem demora sobre qualquer alteração relacionada com as Credenciações de Segurança Física ou Pessoal, em particular sobre a sua revogação/caducidade ou abaixamento de nível.

8. A Parte Destinatária:

- a) Libera Informação Classificada para uma Terceira Parte somente após o recebimento do consentimento prévio por escrito da Parte Transmissora;
- b) Marca a Informação Classificada em conformidade com o Artigo 3º do presente Acordo;
- c) Usa a Informação Classificada apenas com o intuito para que a mesma foi fornecida.

9. Mediante solicitação da Autoridade Nacional de Segurança da Parte Transmissora, a Autoridade Nacional de Segurança da Parte Destinatária emite uma confirmação por escrito de que determinada pessoa tem o direito de aceder a Informação Classificada.

10. As Autoridades de Segurança Competentes das Partes, dentro do espírito de boa vontade de cooperação mútua e compreensão, podem visitar-se mutuamente para discutir e trocar pontos de vista, experiências, lições aprendidas e conhecimentos técnicos nas áreas de segurança física, segurança eletrónica, segurança industrial, procedimentos de verificação e quaisquer outras questões relacionadas com a segurança da Informação Classificada.

11. O acesso à Informação Classificada de ambas as Partes por pessoas singulares de uma Terceira Parte só é autorizado após consentimento por escrito da Autoridade Nacional de Segurança da Parte Transmissora.

Artigo 6.º

Transmissão da Informação Classificada

1. A Informação Classificada é transmitida entre as Partes, de acordo com o Direito nacional da Parte Transmissora, normalmente por via diplomática, ou por qualquer outro meio decidido entre as Autoridades de Segurança Competentes.
2. A Parte Destinatária confirmará, por escrito, a receção da Informação Classificada.
3. A Informação Classificada com o nível de ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET é transmitida pelos Governos através de canais do Governo de acordo com o Direito nacional das Partes.
4. Como requisito mínimo de segurança, Informação Classificada com o nível de ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET deve ser transportada por, e sob o controle exclusivo de um correio do Governo que possua uma Credenciação de Segurança Pessoal do mesmo nível.
5. A Parte Destinatária confirma por escrito a receção da Informação Classificada de nível ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET.
6. A Informação Classificada com o nível ΑΠΟΡΡΗΤΟ / SECRETO / SECRET ou ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL, é transmitida pelos Governos através de canais do Governo de acordo com o Direito nacional das Partes, ou através de outros canais seguros mutuamente aprovados pelas Autoridades Nacionais de Segurança de ambas as Partes.
7. A Parte Destinatária confirma por escrito a receção da Informação Classificada nível ΑΠΟΡΡΗΤΟ / SECRETO / SECRET ou ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL.
8. A Informação Classificada nível ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED, é transmitida através de canais seguros de acordo com o Direito nacional das partes.
9. Os procedimentos para o transporte de grandes remessas contendo Informação Classificada serão acordados e avaliados conjuntamente, caso a caso, pela Autoridade Nacional de Segurança de ambas as Partes.

10. Se a Informação Classificada nível ΑΠΟΡΡΗΤΟ / SECRETO / SECRET, ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL ou ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED, for transmitida eletronicamente entre as Partes, não é enviada em texto claro.

11. A transmissão eletrônica dos níveis específicos de classificação referidos no nº anterior deve ser efetuada através de meios criptográficos certificados mutuamente aprovados pelas Autoridades Nacionais de Segurança.

12. Os principais pontos de entrada e saída da Informação Classificada trocada nos termos do presente Acordo são:

Para a República de Chipre:

Central TOP SECRET Registry do Ministério dos Negócios Estrangeiros

Para a República Portuguesa:

O Registo Central do Gabinete Nacional de Segurança

13. Sem prejuízo do disposto no n.º 12 deste artigo, sempre que seja considerado necessário, pelas Forças de Segurança, Forças Militares ou pela Polícia, o intercâmbio de Informação Classificada, esse intercâmbio será efetuado de acordo com o respetivo Direito nacional das Partes.

14. Os principais pontos de entrada e saída para esta categoria de Informação Classificada será acordada pelas Forças de Segurança, Forças Militares ou pela Polícia, mediante prévio consentimento e aprovação por escrito pelas Autoridades Nacionais de Segurança das Partes.

Artigo 7.º

Reprodução e Tradução da Informação Classificada

1. As traduções e reproduções da Informação Classificada são efetuadas em conformidade com o Direito nacional da Parte Destinatária e com os seguintes procedimentos:

- a) As traduções e as reproduções são marcadas e protegidas da mesma forma que a Informação Classificada original;

- b) As traduções e o número de reproduções são limitados ao necessário para fins oficiais;
 - c) As traduções têm uma anotação apropriada na língua de tradução indicando que contém Informação Classificada recebida da Parte Transmissora.
2. A Informação Classificada marcada com nível ΑΠΟΡΡΗΤΟ / SECRETO / SECRET ou ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET só é traduzida ou reproduzida mediante prévia permissão por escrito da Parte Transmissora.

Artigo 8º

Destruição da Informação Classificada

1. A Informação Classificada é destruída de forma a prevenir a sua reconstrução total ou parcial.
2. A Informação Classificada marcada com nível até ΑΠΟΡΡΗΤΟ / SECRETO / SECRET é destruída de acordo com o Direito nacional das Partes.
3. A Informação Classificada com nível ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TOP SECRET não é destruída e será devolvida à Autoridade Nacional de Segurança da Parte Transmissora.
4. Deve ser elaborado um relatório da destruição da Informação Classificada sendo a sua tradução em inglês enviada à Autoridade Nacional de Segurança da Parte Transmissora.
5. Em caso de situação de crise na qual seja impossível proteger ou devolver Informação Classificada esta é imediatamente destruída sendo a Autoridade Nacional de Segurança da Parte Transmissora informada dessa destruição pela Parte Destinatária com a brevidade possível.

Artigo 9.º

Contratos Classificados

1. A Autoridade Nacional de Segurança duma Parte entregará à Autoridade Nacional de Segurança da outra Parte uma garantia escrita prévia de que o Cocontratante ou subcontratado que deseja empreender um Contrato Classificado de nível ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIAL e ΑΠΟΡΡΗΤΟ / SECRETO / SECRET, detém ou está em processo de obtenção de uma Credenciação de Segurança Física de nível de classificação de segurança apropriado.

2. A Autoridade Nacional de Segurança duma Parte pode solicitar à outra uma inspeção de segurança numa instalação situada no território da outra Parte por forma a assegurar o contínuo cumprimento dos padrões de segurança em conformidade com o respetivo Direito nacional.

3. Cada Contrato Classificado em conformidade com o presente Acordo tem de incluir:

- a) Um compromisso de cumprir as disposições do presente Acordo;
- b) Um compromisso do Cocontratante ou subcontratado de garantir que as suas instalações têm as condições necessárias para o manuseio e armazenamento de Informações Classificadas de um determinado nível de classificação de segurança;
- c) Um compromisso do Cocontratante ou subcontratado garantindo que as pessoas que desempenham funções que requerem acesso a Informação Classificada estão devidamente autorizadas de acordo com o respetivo Direito nacional para ter acesso a Informação Classificada do nível de classificação de segurança equivalente e tenham sido regulamentemente instruídas sobre segurança;
- d) Uma lista da Informação Classificada envolvida e uma lista das áreas onde vai ser manuseada e armazenada;
- e) Os procedimentos para o transporte da Informação Classificada;
- f) Os canais de comunicação e meios para transmissão eletrónica;
- g) Um compromisso do Cocontratante ou subcontratado de notificar a sua Autoridade Nacional de Segurança de qualquer Quebra de Segurança real ou suspeita;
- h) Um compromisso do Cocontratante ou subcontratado de encaminhar uma cópia do Contrato Classificado à Autoridade Nacional de Segurança de ambas as Partes.

4. A Credenciação de Segurança Física e a Credenciação de Segurança Pessoal não são necessárias para os Contratos Classificados cuja Informação Classificada seja limitada ao nível de classificação de ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

5. Os Contratos Classificados a que se refere o número 4 deste Artigo, contêm uma cláusula de exigência de segurança adequada definindo o requisito mínimo de segurança a ser aplicado pelo Cocontratante à Informação Classificada que é gerada e / ou fornecida como resultado do Contrato.

6. A cláusula de segurança a que se refere o número 5 deste Artigo inclui uma disposição relativa à nomeação, pelo Cocontratante, de uma pessoa que tem a responsabilidade geral pela proteção da Informação Classificada marcada com o nível ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTRICTED.

7. Uma cópia da cláusula de exigência de segurança a que se refere o número 6 deste Artigo deverá ser fornecida à Autoridade Nacional de Segurança, somente mediante solicitação.

Artigo 10.º

Visitas

1. As visitas relacionadas com Contratos Classificados e que envolvam acesso a Informação Classificada estão sujeitas a autorização prévia por escrito (aprovação) conferida pela Autoridade Nacional de Segurança da Parte visitada.

2. A Autoridade Nacional de Segurança da Parte visitada tem que receber o pedido de visita com pelo menos 20 (vinte) dias de antecedência.

3. Em casos urgentes, o pedido de visita é submetido num prazo mais curto.

4. O pedido de visita inclui:

- a) O nome e o apelido do visitante, o local e a data de nascimento, a nacionalidade, o número do passaporte ou do documento de identificação;
- b) O nome da pessoa coletiva que o visitante representa ou a que pertence e o cargo que detém;
- c) Nome, morada e informação de contacto da entidade e das instalações que irão ser visitadas;
- d) Confirmação da Credenciação de Segurança Pessoal do visitante, da sua validade e do seu nível;
- e) Objeto e propósito da visita e qual o mais elevado nível de Classificação de Segurança da Informação Classificada envolvido;

f) Data e duração previstas para a visita solicitada e, em caso de visitas recorrentes, o período total abrangido pelas mesmas deverá ser referido;

g) A data, a assinatura e o selo oficial da Autoridade Nacional de Segurança.

5. Assim que a visita for autorizada, a Autoridade Nacional de Segurança da Parte anfitriã providenciará uma cópia do pedido de visita ao encarregado de segurança da entidade a ser visitada.

6. A validade da autorização de visita não excederá os doze (12) meses.

7. A Autoridade Nacional de Segurança da Parte que recebe o pedido de visita informará, assim que possível, a Autoridade Nacional de Segurança da Parte requerente sobre a sua decisão.

8. As Autoridades Nacionais de Segurança das Partes podem acordar estabelecer listas de pessoas autorizadas a efetuar visitas recorrentes as quais serão válidas por um período de doze (12) meses, podendo mediante acordo ser alargadas por um novo período que não exceda mais doze (12) meses.

9. Os termos das respetivas visitas são acertados diretamente com os pontos de contacto adequados da entidade a visitar, nos termos e condições acordados.

Artigo 11.º

Quebra de Segurança

1. Em caso de Quebra de Segurança ou suspeita de tal, a Autoridade Nacional de Segurança da Parte onde ocorreu informa, sem demora e por escrito, a Autoridade Nacional de Segurança da Parte Transmissora e inicia os procedimentos apropriados de acordo com as leis e regulamentos nacionais, a fim de determinar as circunstâncias da Quebra de Segurança, a extensão dos danos e as medidas adotadas para sua mitigação.

2. Se uma Quebra de Segurança ocorrer numa Terceira Parte, a Autoridade Nacional de Segurança da Parte que divulgou a informação à Terceira Parte, toma todas as medidas necessárias para garantir que as ações prescritas no número 1 deste artigo são iniciadas.

3. A Parte Transmissora, mediante solicitação, coopera na investigação de acordo com o número 1 deste Artigo.

4. A Parte Transmissora é informada dos resultados da investigação e receberá o relatório final sobre as causas e o grau dos danos.

Artigo 12.º

Despesas

Cada Parte assume as despesas que para si advenham da aplicação do presente Acordo e respetiva supervisão.

Artigo 13.º

Solução de Controvérsias

Qualquer controvérsia sobre a interpretação ou aplicação do presente Acordo será solucionada através de negociação entre as Partes, por via diplomática.

Artigo 14.º

Revisão

1. O presente Acordo pode ser objeto de revisão com base no mútuo consentimento escrito das Partes.
2. As emendas entrarão em vigor nos termos previstos no artigo 16º.

Artigo 15.

Vigência e Denúncia

1. O presente Acordo permanecerá em vigor por um período de tempo indeterminado.
2. Qualquer das Partes poderá, a qualquer momento, denunciar o presente Acordo mediante notificação escrita à outra Parte por via diplomática.
3. O presente acordo cessa a sua vigência seis (6) meses após a data da receção da notificação acima mencionada.
4. Não obstante a denúncia do presente Acordo, as Partes asseguram que toda a Informação Classificada continuará a ser protegida até que a Parte Transmissora dispense a Parte Destinatária desta obrigação.

Artigo 16º

Entrada em vigor

O presente Acordo entrará em vigor no primeiro dia do segundo mês após a data de recebimento da última notificação escrita pela qual as Partes se notificaram, por via diplomática, de que os requisitos legais nacionais necessários para sua entrada em vigor foram cumpridos.

Artigo 17.º

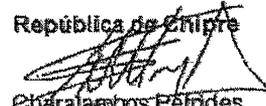
Registo

Após a entrada em vigor do presente Acordo, a Parte em cujo território o Acordo for assinado submetê-lo-á para registo junto do Secretariado das Nações Unidas, nos termos do Artigo 102º da Carta das Nações Unidas, e notificará a outra Parte da conclusão deste procedimento, indicando-lhe o respetivo número de registo.

Feito em Nicósia, aos 8 de outubro de 2022, em dois originais, cada um nas línguas Grega, Portuguesa, e Inglesa, sendo todos os textos autênticos. Em caso de divergência de interpretação o texto na língua Inglesa prevalecerá.

Pela

República de Chipre

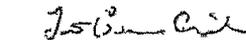


Charalambos Pétrides

Ministro da Defesa

Pela

República Portuguesa



João Gomes Cravinho

Ministro dos Negócios Estrangeiros

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LA RÉPUBLIQUE PORTUGAISE ET LA RÉPUBLIQUE DE CHYPRE RELATIF À L'ÉCHANGE ET LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

La République de Chypre et la République portugaise,

Ci-après dénommées les « Parties »,

Reconnaissant la nécessité de fixer les règles de protection des informations classifiées échangées dans l'intérêt de la sécurité nationale dans le cadre de quelque forme et domaine de coopération, ainsi que toute information classifiée générée dans le cadre d'une telle coopération,

Souhaitant garantir la protection mutuelle des informations classifiées dans un État et transmises à l'autre État dans le cadre de la coopération entre les Parties,

Désireuses d'établir un ensemble de règles relatives à la protection mutuelle des informations classifiées échangées entre les Parties,

Tenant compte de leurs intérêts mutuels en matière de protection des informations classifiées, conformément à la législation des Parties,

Sont convenues de ce qui suit :

Article premier. Objectif

L'objectif du présent Accord est d'assurer la protection des informations classifiées générées par les Parties ou échangées entre elles.

Article 2. Définitions

Aux fins du présent Accord :

- a) le terme « informations classifiées » désigne toute information, quelle que soit sa forme ou sa nature, qui doit être protégée contre les accès et les utilisations non autorisés et qui s'est vue attribuer un niveau de classification de sécurité conformément à la législation nationale des Parties ;
- b) le terme « autorité nationale de sécurité » désigne l'autorité de chaque Partie qui, conformément à sa législation nationale, est responsable de l'application et de la supervision générales du présent Accord ;
- c) le terme « atteinte à la sécurité » désigne un acte ou une omission contraire au présent Accord ou à la législation nationale des Parties pouvant conduire à la divulgation, à la perte, à la destruction, au détournement ou à tout autre type de compromission d'informations classifiées ;
- d) le terme « contrat classifié » désigne un accord entre deux ou plusieurs contractants ou sous-traitants, qui comprend l'accès à des informations classifiées ou la génération de telles informations ;

- e) le terme « autorité de sécurité compétente » désigne toute autorité compétente des Parties autre que l'autorité nationale de sécurité et qui, conformément à sa législation nationale, est responsable de la mise en œuvre du présent Accord ;
- f) le terme « contractant » désigne toute personne physique ou morale dotée de la capacité juridique pour conclure ou exécuter des contrats classifiés ;
- g) le terme « habilitation de sécurité d'établissement » désigne l'avis favorable de l'autorité nationale de sécurité confirmant qu'une personne physique ou morale dispose des capacités physiques et organisationnelles nécessaires pour traiter et stocker des informations classifiées conformément à la législation nationale des deux Parties ;
- h) le terme « besoin d'en connaître » désigne le principe selon lequel l'accès à des informations classifiées n'est accordé que dans le cadre d'une fonction officielle déterminée et pour l'exécution d'une mission spécifique ;
- i) le terme « Partie d'origine » désigne la Partie qui génère ou fournit les informations classifiées à la Partie destinataire ;
- j) le terme « habilitation de sécurité personnelle » désigne l'avis favorable par lequel l'autorité nationale de sécurité confirme que, conformément à la législation nationale des Parties, la personne physique est autorisée à accéder aux informations classifiées jusqu'à un certain niveau de classification et à les traiter ;
- k) le terme « Partie destinataire » désigne la Partie à laquelle des informations classifiées sont transmises ;
- l) le terme « tierce partie » désigne tout État, toute organisation ou toute personne physique ou morale qui n'est pas partie au présent Accord.

Article 3. Niveaux de classification de sécurité

Les Parties conviennent que les niveaux et les marques de classification de sécurité suivants sont équivalents et correspondent aux niveaux de classification de sécurité définis par leur législation nationale respective :

Pour la République de Chypre	Pour la République portugaise	Équivalent en français
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	MUITO SECRETO	TRÈS SECRET
ΑΠΟΡΡΗΤΟ	SECRETO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENCIAL	CONFIDENTIEL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESERVADO	RESTREINT

Article 4. Autorités de sécurité

1. Les autorités nationales de sécurité des Parties sont les suivantes :

Pour la République de Chypre :

Autorité nationale de sécurité

Ministère de la défense de la République de Chypre

Pour la République portugaise :

Autorité nationale de sécurité

Présidence du Conseil des ministres

2. Les autorités nationales de sécurité s'informent mutuellement par écrit, par la voie diplomatique, de toute modification relative à la désignation des autorités nationales de sécurité.

3. Les autorités nationales de sécurité se communiquent leurs coordonnées officielles et s'informent mutuellement de toute modification ultérieure de celles-ci.

4. Toute modification relative aux autorités nationales de sécurité ne saurait constituer une modification du présent Accord.

5. Les autorités nationales de sécurité se tiennent mutuellement informées des dispositions législatives applicables aux informations classifiées dans leur pays ainsi que de toutes les modifications importantes qui leur sont apportées, et échangent des informations sur les normes, les procédures et les pratiques de sécurité visant à assurer la protection des informations classifiées.

Article 5. Mesures de protection et accès aux informations classifiées

1. Conformément à leur législation nationale, les Parties prennent toutes les mesures appropriées pour protéger les informations classifiées qui sont générées ou échangées dans le cadre du présent Accord.

2. Les Parties accordent à ces informations classifiées le même niveau de protection que celui qu'elles accorderaient à leurs propres informations classifiées du niveau de classification de sécurité équivalent selon les dispositions de l'article 3 du présent Accord.

3. La Partie d'origine informe par écrit :

- a) la Partie destinataire de toutes les conditions attachées à la communication des informations classifiées ainsi que des restrictions applicables à leur utilisation ;
- b) la Partie destinataire de toute modification du niveau de classification de sécurité des informations classifiées transmises.

4. Les informations classifiées sont exclusivement mises à la disposition des personnes physiques ou morales qui sont autorisées, conformément à la législation nationale applicable, à avoir accès à des informations classifiées du niveau de classification de sécurité équivalent et qui ont un « besoin d'en connaître ».

5. Dans le cadre du présent Accord, chaque Partie reconnaît les habilitations de sécurité personnelles et d'établissement délivrées par l'autre Partie.

6. Les autorités nationales de sécurité se prêtent mutuellement assistance, sur demande et conformément à leur législation nationale respective, pour l'exécution des procédures de vérification nécessaires à l'application du présent Accord.

7. Dans le cadre du présent Accord, les autorités de sécurité des Parties s'informent mutuellement, sans délai, de toute modification concernant les habilitations de sécurité personnelles et d'établissement, en particulier en ce qui concerne leur retrait ou leur déclassement.

8. La Partie destinataire :

- a) ne transmet des informations classifiées à une tierce partie qu'après la réception de l'accord écrit préalable de la Partie d'origine ;
- b) appose sur les informations classifiées les indications nécessaires conformément à l'article 3 du présent Accord ;
- c) n'utilise les informations classifiées qu'aux fins prévues.

9. À la demande de l'autorité nationale de sécurité de la Partie d'origine, l'autorité nationale de sécurité de la Partie destinataire délivre une confirmation écrite attestant qu'une personne a le droit d'accéder aux informations classifiées.

10. Les autorités de sécurité compétentes des Parties, dans un esprit de compréhension et de bonne volonté en vue d'une coopération mutuelle, peuvent se rendre visite afin de discuter et de procéder à des échanges de vues, d'expériences, d'enseignements et de connaissances techniques dans les domaines de la sécurité physique, de la sécurité électronique, de la sécurité industrielle, des procédures de vérification et de toute autre question liée à la sécurité des informations classifiées.

11. L'accès à des informations classifiées des deux Parties par des personnes physiques d'une tierce partie n'est autorisé qu'après accord écrit de l'autorité nationale de sécurité de la Partie d'origine.

Article 6. Transmission d'informations classifiées

1. Les informations classifiées sont transmises entre les Parties conformément à la législation nationale de la Partie d'origine, ordinairement par la voie diplomatique, ou par d'autres voies convenues par les autorités de sécurité compétentes.

2. La Partie destinataire confirme par écrit la réception des informations classifiées.

3. Les informations classifiées qui portent la mention ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TRÈS SECRET sont transmises par des voies établies entre les gouvernements conformément à la législation nationale des Parties.

4. En tant qu'exigence de sécurité minimale, les informations classifiées qui portent la mention ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TRÈS SECRET sont transmises par un messenger du gouvernement titulaire d'une habilitation de sécurité personnelle du même niveau et sous son contrôle exclusif.

5. La Partie destinataire confirme par écrit la réception des informations classifiées de niveau ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TRÈS SECRET.

6. Les informations classifiées qui portent la mention ΑΠΟΡΡΗΤΟ / SECRETO / SECRET ou ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIEL sont transmises par des voies établies entre les gouvernements conformément à la législation nationale des Parties, ou par d'autres voies sécurisées approuvées par les autorités de sécurité nationales des deux Parties.

7. La Partie destinataire confirme par écrit la réception des informations classifiées de niveau ΑΠΟΡΡΗΤΟ / SECRETO / SECRET et ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIEL.

8. Les informations classifiées qui portent la mention ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTREINT sont transmises par des voies sécurisées, conformément à la législation nationale des Parties.

9. Les procédures relatives au transport des envois de gros volume qui contiennent des informations classifiées sont convenues et évaluées conjointement, au cas par cas, par les autorités nationales de sécurité des deux Parties.

10. Si des informations classifiées qui portent la mention ΑΠΟΡΡΗΤΟ / SECRETO / SECRET, ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIEL ou ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTREINT doivent être transmises par voie électronique entre les Parties, elles ne sont pas envoyées en texte clair.

11. La transmission électronique des informations de niveaux de classification visés à l'article précédent s'effectue au moyen de méthodes certifiées de chiffrement mutuellement approuvées par les autorités nationales de sécurité.

12. Les principaux points d'entrée et de sortie des informations classifiées échangées en vertu du présent Accord sont :

pour la République de Chypre :

le bureau d'ordre central « TRÈS SECRET » du Ministère des affaires étrangères ;

pour la République portugaise :

le bureau d'ordre central de l'autorité nationale de sécurité.

13. Sans préjudice du paragraphe 12 du présent article, lorsque les forces de sécurité, les forces militaires ou la police jugent nécessaire de procéder à un échange d'informations classifiées, celui-ci est effectué conformément à la législation nationale des Parties.

14. Les principaux points d'entrée et de sortie de cette catégorie d'informations classifiées sont convenus par les forces de sécurité, les forces militaires ou la police et l'échange se fait sur la base d'un consentement et d'une approbation écrits préalables des autorités nationales de sécurité des Parties.

Article 7. Reproduction et traduction des informations classifiées

1. Les informations classifiées sont traduites et reproduites conformément à la législation nationale de la Partie destinataire et aux procédures suivantes :

- a) les traductions et reproductions portent la même marque de classification et sont protégées de la même manière que les informations classifiées originales ;
- b) les traductions et le nombre de copies sont limités au strict nécessaire aux fins officielles ;
- c) les traductions contiennent une note appropriée, rédigée dans la langue de la traduction, indiquant que les documents contiennent des informations classifiées provenant de la Partie d'origine.

2. Les informations classifiées qui portent la mention ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TRÈS SECRET ou ΑΠΟΡΡΗΤΟ / SECRETO / SECRET ne peuvent être traduites ou reproduites qu'avec le consentement préalable écrit de la Partie d'origine.

Article 8. Destruction d'informations classifiées

1. Les informations classifiées sont détruites de manière à empêcher leur reconstitution partielle ou intégrale.

2. Les informations classifiées qui portent la mention ΑΠΟΡΡΗΤΟ / SECRETO / SECRET sont détruites conformément à la législation nationale des Parties.

3. Les informations classifiées qui portent la mention ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / MUITO SECRETO / TRÈS SECRET ne sont pas détruites et sont restituées à l'autorité nationale de sécurité de la Partie émettrice.

4. Un rapport sur la destruction des informations classifiées est élaboré et sa traduction en anglais est envoyée à l'autorité nationale de sécurité de la Partie d'origine.

5. En cas de situation de crise rendant impossible la protection ou la restitution des informations classifiées, celles-ci sont détruites immédiatement, et la Partie destinataire avise dès que possible l'autorité nationale de sécurité de la Partie d'origine de ladite destruction.

Article 9. Contrats classifiés

1. L'autorité nationale de sécurité d'une Partie fournit à l'autorité nationale de sécurité de l'autre Partie une confirmation écrite préalable attestant que les contractants ou les sous-traitants qui souhaitent conclure un contrat classifié de niveau ΕΜΠΙΣΤΕΥΤΙΚΟ / CONFIDENCIAL / CONFIDENTIEL ou de niveau ΑΠΟΡΡΗΤΟ / SECRETO / SECRET détiennent ou sont en passe d'obtenir une habilitation de sécurité d'établissement du niveau de classification de sécurité requis.

2. Chaque autorité nationale de sécurité peut demander à l'autre autorité nationale de sécurité qu'une inspection de sécurité soit effectuée dans un établissement situé sur le territoire de son État, pour garantir une conformité continue avec les normes de sécurité, conformément à sa législation nationale.

3. Chaque contrat classifié conclu conformément au présent Accord comprend les éléments suivants :

- a) une déclaration du contractant ou du sous-traitant dans laquelle celui-ci s'engage à respecter les dispositions du présent Accord ;
- b) une déclaration du contractant ou du sous-traitant dans laquelle celui-ci s'engage à faire en sorte que ses installations réunissent les conditions requises pour le traitement et le stockage d'informations classifiées d'un niveau de classification de sécurité donné ;
- c) une déclaration du contractant ou du sous-traitant dans laquelle celui-ci s'engage à garantir que les personnes qui exercent des fonctions nécessitant l'accès à des informations classifiées sont dûment autorisées, conformément à la législation nationale de leur pays, à accéder à des informations classifiées du niveau de

classification de sécurité correspondant et ont régulièrement reçu des informations sur la sécurité ;

- d) une liste des informations classifiées concernées et une liste des domaines dans lesquels elles seront traitées et stockées ;
- e) les procédures à suivre pour le transport des informations classifiées ;
- f) les canaux de communication et les moyens de transmission électronique ;
- g) une déclaration du contractant ou du sous-traitant dans laquelle celui-ci s'engage à informer son autorité nationale de sécurité compétente de toute atteinte réelle ou présumée à la sécurité ;
- h) une déclaration du contractant ou du sous-traitant dans laquelle celui-ci s'engage à transmettre un exemplaire du contrat classifié à l'autorité nationale de sécurité des deux Parties.

4. Une habilitation de sécurité d'établissement et une habilitation de sécurité personnelle ne sont pas requises pour les contrats classifiés portant uniquement sur des informations classifiées de niveau

ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTREINT.

5. Les contrats classifiés visés au paragraphe 4 du présent article contiennent une clause d'exigence de sécurité appropriée définissant l'exigence de sécurité minimale que le contractant doit appliquer aux informations classifiées générées ou fournies dans le cadre du contrat.

6. La clause de sécurité visée au paragraphe 5 du présent article comprend une disposition relative à la désignation, par le contractant, d'une personne assumant la responsabilité générale de la protection des informations classifiées qui portent la mention ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / RESERVADO / RESTREINT.

7. Une copie de la disposition relative à l'exigence de sécurité visée au paragraphe 6 du présent article est fournie, uniquement sur demande, à l'autorité nationale de sécurité.

Article 10. Visites

1. Les visites liées à des contrats classifiés et impliquant l'accès à des informations classifiées doivent être préalablement autorisées par écrit par l'autorité nationale de sécurité de la Partie hôte.

2. La demande de visite est envoyée à l'autorité nationale de sécurité de la Partie hôte au moins vingt jours à l'avance.

3. En cas d'urgence, la demande de visite peut être soumise dans un délai plus court.

4. La demande de visite comprend :

- a) le prénom, le nom, les lieu et date de naissance, la nationalité, le numéro du passeport ou du document d'identité du visiteur ;
- b) le nom de la personne morale représentée par le visiteur et la fonction du visiteur pour la personne morale ;
- c) le nom, l'adresse et les coordonnées de la personne morale et de l'établissement qui font l'objet de la visite ;
- d) la confirmation que le visiteur dispose d'une habilitation de sécurité personnelle, avec mention de sa durée de validité et de son niveau de classification ;

- e) l'objet et la finalité de la visite ainsi que le niveau de classification de sécurité le plus élevé parmi ceux qui ont été accordés aux informations classifiées concernées ;
- f) la date et la durée prévues de la visite demandée, et, en cas de visites répétées, la période totale durant laquelle les visites sont effectuées ;
- g) la date, la signature et le sceau officiel de l'autorité nationale de sécurité.

5. Une fois la visite approuvée, l'autorité nationale de sécurité de la Partie hôte fournit une copie de la demande de visite au responsable de la sécurité de la personne morale concernée.

6. La validité d'une autorisation de visite n'excède pas douze mois.

7. L'autorité nationale de sécurité de la Partie qui reçoit une demande de visite informe en temps voulu l'autorité nationale de sécurité de la Partie requérante de sa décision.

8. Les autorités nationales de sécurité des Parties peuvent établir des listes de personnes autorisées à effectuer des visites récurrentes, qui sont valables pour une période initiale de douze mois. Après accord, la durée de validité de ces listes peut être prolongée pour une nouvelle période ne dépassant pas douze mois.

9. Les modalités des différentes visites sont définies directement avec les points de contact compétents de la personne morale qui fera l'objet de visites, conformément aux clauses et conditions convenues.

Article 11. Atteinte à la sécurité

1. En cas d'atteinte réelle ou présumée à la sécurité, l'autorité nationale de sécurité de la Partie où ladite atteinte à la sécurité s'est produite informe, sans délai et par écrit, l'autorité nationale de sécurité de la Partie d'origine et engage les procédures appropriées conformément aux dispositions législatives et réglementaires nationales afin de déterminer les circonstances de l'atteinte à la sécurité, l'étendue des dommages et les mesures adoptées pour remédier à la situation.

2. Si une atteinte à la sécurité se produit dans une tierce partie, l'autorité nationale de sécurité de la Partie qui a communiqué les informations à la tierce partie prend toutes les dispositions nécessaires pour que les actions prévues au paragraphe 1 du présent article soient engagées.

3. La Partie d'origine coopère, sur demande, à l'enquête conformément au paragraphe 1 du présent article.

4. La Partie d'origine est informée des résultats de l'enquête et reçoit le rapport final relatif aux causes de l'atteinte et à l'étendue des dommages.

Article 12. Frais

Chaque Partie assume les dépenses qu'elle a engagées pour la mise en œuvre et la supervision du présent Accord.

Article 13. Règlement des différends

Tout différend concernant l'interprétation ou l'application du présent Accord est résolu par voie de négociation entre les Parties par la voie diplomatique.

Article 14. Modifications

1. Le présent Accord peut être modifié par consentement écrit mutuel des Parties.
2. Les modifications entrent en vigueur conformément aux modalités prévues à l'article 16 du présent Accord.

Article 15. Durée et résiliation

1. Le présent Accord est conclu pour une durée indéterminée.
2. Chaque Partie peut, à tout moment, dénoncer le présent Accord par notification écrite adressée à l'autre Partie par la voie diplomatique.
3. Le présent Accord prend fin six mois après la date de réception de ladite notification.
4. Nonobstant la dénonciation du présent Accord, les Parties veillent à ce que toutes les informations classifiées restent protégées jusqu'à ce que la Partie émettrice dispense la Partie destinataire de cette obligation.

Article 16. Entrée en vigueur

Le présent Accord entre en vigueur le premier jour du deuxième mois à compter de la date de réception de la dernière notification écrite par laquelle les Parties s'informent, par la voie diplomatique, de l'accomplissement de leurs procédures légales internes nécessaires à cet effet.

Article 17. Enregistrement

Dès l'entrée en vigueur du présent Accord, la Partie sur le territoire de laquelle l'Accord est signé le transmet au Secrétariat de l'Organisation des Nations Unies pour enregistrement, conformément à l'Article 102 de la Charte des Nations Unies, et notifie à l'autre Partie l'accomplissement de cette procédure et le numéro d'enregistrement.

FAIT à Nicosie le 8 octobre 2022 en deux exemplaires, chacun en langues grecque, portugaise et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, le texte anglais prévaut.

Pour la République de Chypre :
CHARALAMBOS PETRIDES
Ministre de la défense (signature)

Pour la République portugaise :
JOAO GOMES CRAVINHO
Ministre des affaires étrangères