No. 56015*

Cyprus
and
Serbia

Agreement between the Government of the Republic of Cyprus and the Government of the Republic of Serbia on the exchange and on mutual protection of classified information. Nicosia, 27 November 2017

Entry into force: *1 October 2019, in accordance with article 14*

Authentic texts: *English, Greek and Serbian*

Registration with the Secretariat of the United Nations: *Cyprus, 21 November 2019*

*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
Serbie

Accord entre le Gouvernement de la République de Chypre et le Gouvernement de la République de Serbie relatif à l'échange et à la protection mutuelle des informations classifiées. Nicosie, 27 novembre 2017

Entrée en vigueur : *1er octobre 2019, conformément à l'article 14*

Textes authentiques : *anglais, grec et serbe*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Chypre, 21 novembre 2019*

*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.

[ENGLISH TEXT – TEXTE ANGLAIS]

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

The Government of the Republic of Cyprus
and
the Government of the Republic of Serbia

(hereinafter referred to as "the Parties"),

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

Intending to ensure the mutual protection of all Classified Information, which has been classified by one Party and transferred to the other Party or commonly generated 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 interests in the protection of Classified Information, in accordance with the legislation of the Parties,

Have agreed as follows:

Article 1
Objective

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

Article 2
Definitions

For the purposes of this Agreement:

a) „Breach of Security" means an act or an omission which is contrary to this Agreement or 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;

b) „Classified Contract" means an agreement between two or more Contractors, which contains or the implementation of which requires access to Classified Information;

c) „Classified Information" means any information, irrespective of its form or nature, which requires protection against unauthorized use and has been classified in accordance with the national legislation of the Parties and has been so designated by a security classification level;

d) „Competent Authority" means National Security Authority and any other competent entity which, according to the national legislation of the Parties, is responsible for the implementation of this Agreement as referred to in, Article 4 Paragraph 1 of this Agreement;

e) „Contractor" means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;

f) „Facility Security Clearance" means the determination by the Competent Authority confirming, that the legal entity or and individual has the physical and organizational capability to handle and store Classified Information in accordance with the respective national legislation;

g) „Need-to-know" means the necessity to have access to specific Classified Information in the scope of a given official position and for the performance of a specific task;

h) „Originating Party" means the Party which has created Classified Information;

i) „Personnel Security Clearance" means the determination by the Competent Authority confirming, in accordance with the respective national legislation, that the individual is eligible to have access to Classified Information;

j) „Receiving Party" means the Party to which Classified Information of the Originating Party is transmitted;

k) „Third Party" means any state, organization, legal entity or individual 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 national legislation:

For the Republic of Cyprus	For the Republic of Serbia	Equivalent in English
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	ДРЖАВНА ТАЈНА	TOP SECRET
ΑΠΟΡΡΗΤΟ	СТРОГО ПОВЕРЉИВО	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ПОВЕРЉИВО	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	ИНТЕРНО	RESTRICTED

Article 4
Competent Authorities

1. The Competent Authorities of the Parties are:

For the Government of the Republic of Cyprus:
National Security Authority
Ministry of Defence of the Republic of Cyprus

For the Government of the Republic of Serbia:
Office of the Council on National Security and Classified Information Protection

2. The Parties shall inform each other through diplomatic channels about any changes or modifications regarding their Competent Authority.

3. The Competent Authorities shall inform each other of the 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 appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. At least the same level of protection shall be assigned to such Classified Information as is provided for the national Classified Information of the equivalent security classification level in accordance with Article 3.

2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information.

3. Access to Classified Information shall be limited to persons on a Need-to-know basis who are authorised in accordance with the national legislation of the Parties to have access to Classified Information of the equivalent security classification level.

4. Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearances and Facility Security Clearances granted in accordance with the national legislation of the other Party. The security clearances shall be equivalent in within Article 3.

5. The Competent Authorities shall, in accordance with the national legislation, assist each other upon request at carrying out vetting procedures necessary for the application of this Agreement.

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

7. The Receiving Party shall:

a) Submit Classified Information to any Third Party only upon the prior written consent of the Originating Party;

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

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

Article 6
Transmission of Classified Information

1. Classified Information shall be transmitted through diplomatic channels unless otherwise approved by the Competent Authorities. The Receiving Party shall confirm the receipt of Classified Information in writing.

2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed by the Competent Authorities.

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

For the Republic of Cyprus:
The Central Registry "TOP SECRET" at the Ministry of Foreign Affairs
Presidential Palace Avenue
1447, Nicosia

For the Republic of Serbia:
Office of the National Security Council and Classified Information Protection
Nemanjina 22-26
11 000 Belgrade

4. The intelligence, security and police services of the Parties may in accordance with their respective national legislation, exchange operational and/or intelligence information directly between each other.

Article 7
Reproduction and translation of Classified Information

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

a) translations and reproductions shall be marked and protected as original Classified Information;

b) translations and the number of copies shall be limited to that required for official purposes;

c) translations shall bear an appropriate note in the language of the translation, indicating that it contains Classified Information received from the Originating Party.

2. Classified Information marked АПОРРНТО / СТРОГО ПОВЕРЉИВО / SECRET or above shall be translated or reproduced only upon a prior written consent of the Originating Party.

Article 8
Destruction of Classified Information

1. Classified Information shall be destroyed in a manner that prevents its partial or total reconstruction.

2. Classified Information marked up to ΑΠΟΡΡΗΤΟ / СТРОГО ПОВЕРЉИВО / SECRET shall be destroyed in accordance with the national legislation.

3. Classified Information marked ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / ДРЖАВНА ТАЈНА / TOP SECRET shall not be destroyed. It shall be returned to the Competent Authority of the Originating Party.

4. A report on destruction of Classified Information shall be made and its translation in English shall be delivered to the Competent Authority of the Originating Party.

5. In case of a crisis situation in which it is impossible to protect or return Classified Information it shall be destroyed immediately. The Receiving Party shall inform the Competent Authority of the Originating Party about this destruction as soon as possible.

Article 9
Classified Contracts

1. The Competent Authority of a Party shall provide to the Competent Authority of the other Party prior written assurance that a contractor or a sub-contractor, wishing to undertake a classified contract marked as ΑΠΟΡΡΗΤΟ/СТРОГО ПОВЕРЉИВО/ SECRET and ΕΜΠΙΣΤΕΥΤΙΚΟ/ПОВЕРЉИВО/CONFIDENTIAL level with such other Party, holds or is in the process of obtaining a Facility Security Clearance of the appropriate security classification level.

2. Each Classified Contract concluded in accordance with this Agreement shall include:

a) Commitment of the Contractor to ensure that its premises have necessary conditions for handling and storing Classified Information of appropriate security classification level;

b) Commitment of the Contractor to ensure that persons who perform duties requiring access to Classified Information are authorized in accordance with the national legislation to have access to Classified Information of appropriate security classification level;

c) Requirement that the Contractor shall ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national legislation;

d) List of Classified Information and list of areas in which Classified Information can arise;

e) Procedure for communication of changes in the security classification level of Classified Information;

f) Communication means and electronic means for transmission;

g) Procedure for the transmission of Classified Information;

h) Commitment of the Contractor to notify of any actual or suspected Breach of Security;

i) Commitment of the Contractor to forward a copy of the Classified Contract to its own Competent Authority;

j) Commitment of the subcontractor to fulfill the same security obligations as the Contractor.

3. As soon as pre-contractual negotiations begin between potential Contractors, the Competent Authority of the Originating Party shall inform the Competent Authority of the other Party of the security classification level given to the Classified Information related to those pre-contractual negotiations.

4. Copy of each Classified Contract shall be forwarded to the Competent Authority of the Party where the work is to be performed, to allow adequate security supervision and control.

Article 10
Visits

1. Visits related to Classified Contracts and involving access to Classified Information are subject to prior written approval given by the Competent Authority of the host Party.

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

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

4. The request for visit shall include:

a) visitor's name and surname, place and date of birth, citizenship, passport or identification document number;

b) name of the legal entity represented by the visitor and position of the visitor in the legal entity;

c) name, address and contact information of the legal entity to be visited;

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

e) object and purpose of the visit;

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

g) the date, signature and the official seal of the Competent Authority.

5. Once the visit has been approved the Competent Authority of the host Party shall provide a copy of the request for visit to the security officers of the legal entity to be visited.

6. The validity of visit approval shall not exceed one year.

7. The Competent Authorities of the Parties may draw up lists of individuals authorized to make recurring visits. The lists are valid for an initial period of twelve months. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.

Article 11
Breach of Security

1. In case of Breach of Security the Competent Authority of the Receiving Party shall inform the Competent Authority of the Originating Party, as soon as possible, and initiate the appropriate investigation.

2. If a breach of security arises in a third state, the Competent Authority of the dispatching Party shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 are initiated.

3. The Originating Party shall, upon request, co-operate in the investigation in accordance with Paragraph 1.

4. The Originating Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damage.

Article 12
Expenses

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

Article 13
Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiations between the Parties. During the negotiations both Parties shall continue to fulfil all other obligations under this Agreement.

Article 14
Final Provisions

1. This Agreement is concluded for an indefinite period of time and enters into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

2. This Agreement may be amended any time on the basis of mutual written approval of the Parties. The amendments shall enter into force in accordance with Paragraph 1.

3. Each Party may, at any time, terminate this Agreement by written notification to the other Party, through diplomatic channels. In this case, the termination takes effect six months after the date of the receipt of the respective notification.

4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Originating Party dispenses the Receiving Party from this obligation.

Done at Nicosia ...on 27 November 2017 in two original sets, each in the Greek, Serbian, and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the Republic of Cyprus

.....

For the Government of the Republic of Serbia

.....

[GREEK TEXT – TEXTE GREC]

ΣΥΜΦΩΝΙΑ ΜΕΤΑΞΥ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΚΑΙ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΣΕΡΒΙΑΣ ΓΙΑ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΚΑΙ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η Κυβέρνηση της Κυπριακής Δημοκρατίας
και
Η Κυβέρνηση της Δημοκρατίας της Σερβίας

(εφεξής καλούμενες τα «Μέρη»),

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

Σκοπεύοντας να διασφαλίσουν την αμοιβαία προστασία όλων των Διαβαθμισμένων Πληροφοριών οι οποίες διαβαθμίστηκαν στο ένα Μέρος και διαβιβάστηκαν στο άλλο Μέρος ή που παράγονται από κοινού στα πλαίσια 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 τα ακόλουθα:

Άρθρο 1
Σκοπός

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

Άρθρο 2
Ορισμοί

Για τους σκοπούς της παρούσας Συμφωνίας:

α) «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 στην γνωστοποίηση, απώλεια, καταστροφή, παράνομη χρήση ή οποιαδήποτε άλλη διαρροή των Διαβαθμισμένων Πληροφοριών;

β) «Διαβαθμισμένη Σύμβαση» σημαίνει κάθε Συμφωνία μεταξύ δύο ή περισσοτέρων Εργολάβων, η εκτέλεση της οποίας απαιτεί ή περιλαμβάνει πρόσβαση σε Διαβαθμισμένες Πληροφορίες;

γ) «Διαβαθμισμένες Πληροφορίες» σημαίνει κάθε πληροφορία, ανεξαρτήτως τύπου ή φύσεως, η οποία χρήζει προστασίας από μη εξουσιοδοτημένη χρήση και διαβαθμίστηκε με κάποιο επίπεδο διαβάθμισης ασφαλείας, σύμφωνα με την εθνική νομοθεσία των Μερών;

δ) «Αρμόδια Αρχή» σημαίνει οποιαδήποτε Εθνική Αρχή Ασφαλείας και οποιονδήποτε άλλο αρμόδιο φορέα ο οποίος, σύμφωνα με την εθνική νομοθεσία των Μερών, είναι υπεύθυνος για την εφαρμογή της παρούσας Συμφωνίας όπως προβλέπεται στο Άρθρο 4 Παράγραφος 1 της παρούσας Συμφωνίας;

ε) «Εργολάβος» σημαίνει το φυσικό ή νομικό πρόσωπο που έχει τη νομική ικανότητα σύναψης Διαβαθμισμένων συμβάσεων;

στ) «Εξουσιοδότηση Ασφάλειας Φορέα» σημαίνει τη θετική απόφαση της Αρμόδιας Αρχής, με την οποία επιβεβαιώνεται ότι το νομικό πρόσωπο έχει την φυσική και οργανωτική ικανότητα να χειρίζεται και να αποθηκεύει Διαβαθμισμένες Πληροφορίες σύμφωνα με την αντίστοιχη εθνική νομοθεσία των Μερών;

ζ) «Ανάγκη για Γνώση» σημαίνει την ανάγκη πρόσβασης σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες στα πλαίσια συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας;

η) «Μέρος Αποστολέας» σημαίνει το Μέρος το οποίο παράγει Διαβαθμισμένες Πληροφορίες;

θ) «Εξουσιοδότηση Ασφάλειας Προσωπικού» σημαίνει τη θετική απόφαση της Αρμόδιας Αρχής, σύμφωνα με την αντίστοιχη εθνική νομοθεσία των Μερών, κατά την οποία το πρόσωπο δικαιούται να έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες;

ι) «Μέρος Παραλήπτης» σημαίνει το Μέρος στο οποίο διαβιβάζονται Διαβαθμισμένες Πληροφορίες;

ια) «Τρίτο Μέρος» σημαίνει το κράτος, τον οργανισμό, το 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 εθνική τους νομοθεσία:

Για την Κυπριακή Δημοκρατία	Για τη Δημοκρατία της Σερβίας	Αντίστοιχη αγγλική ορολογία
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	ДРЖАВНА ТАЈНА	TOP SECRET
ΑΠΟΡΡΗΤΟ	СТРОГО ПОВЕРЉИВО	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ПОВЕРЉИВО	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	ИНТЕРНО	RESTRICTED

Άρθρο 4
Αρμόδιες Αρχές Ασφαλείας

1. Οι Αρμόδιες Αρχές των Μερών είναι:

Για την Κυβέρνηση της Κυπριακής Δημοκρατίας:
Εθνική Αρχή Ασφαλείας
Υπουργείο Άμυνας της Κυπριακής Δημοκρατίας

Για την Κυβέρνηση της Δημοκρατίας της Σερβίας:
Υπηρεσία Εθνικής Ασφαλείας και Προστασίας Διαβαθμισμένων Πληροφοριών.

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

3. Οι Αρμόδιες Αρχές θα αλληλοενημερώνονται για την αντίστοιχη εθνική νομοθεσία περί Διαβαθμισμένων Πληροφοριών και για τυχόν σημαντικές τροποποιήσεις σε αυτή και θα ανταλλάσσουν πληροφορίες σχετικά με τα πρότυπα ασφαλείας, 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 ανταλλάσσουν ή παράγουν βάσει της παρούσας Συμφωνίας. Οι Διαβαθμισμένες Πληροφορίες θα διαβαθμίζονται με το ίδιο τουλάχιστον επίπεδο ασφαλείας, όπως προβλέπεται για τις εθνικές Διαβαθμισμένες Πληροφορίες του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας σύμφωνα με το Άρθρο 3.

2. Το Μέρος Αποστολέας ενημερώνει γραπτώς το Μέρος Παραλήπτη για τυχόν αλλαγή στο επίπεδο διαβάθμισης ασφαλείας των διαβιβασθέντων Διαβαθμισμένων Πληροφοριών.

3. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες περιορίζεται σε πρόσωπα, βάσει της αρχής της Ανάγκης για Γνώση, τα οποία είναι εξουσιοδοτημένα σύμφωνα με την εθνική νομοθεσία των Μερών, να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας.

4. Στο πλαίσιο της παρούσας Συμφωνίας, κάθε Μέρος αναγνωρίζει την Εξουσιοδότηση Ασφάλειας Προσωπικού και την Εξουσιοδότηση Ασφάλειας Φορέα η οποία παρέχεται σύμφωνα με την εθνική νομοθεσία του άλλου Μέρους. Οι εξουσιοδοτήσεις ασφαλείας θα είναι ισοδύναμες σύμφωνα με το Άρθρο 3.

5. Οι Αρμόδιες Αρχές, κατόπιν αιτήματος και σύμφωνα με την εθνική νομοθεσία, αλληλοβοηθούνται στη διεξαγωγή των διαδικασιών ελέγχου ασφαλείας για την εφαρμογή της παρούσας Συμφωνίας.

6. Στο πλαίσιο της παρούσας Συμφωνίας, οι Αρμόδιες Αρχές των Μερών αλληλοενημερώνονται χωρίς καθυστέρηση σχετικά με τυχόν αλλαγές των Εξουσιοδοτήσεων Ασφαλείας Προσωπικού και Φορέα και πιο συγκεκριμένα όταν πρόκειται για την ανάκληση ή την υποβάθμισή τους.

7. Το Μέρος Παραλήπτης:

α) Υποβάλλει Διαβαθμισμένες Πληροφορίες σε τυχόν Τρίτο Πρόσωπο μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα;

β) Διαβαθμίζει την παραληφθείσα Διαβαθμισμένη Πληροφορία σύμφωνα με το Άρθρο 3;

γ) χρησιμοποιεί Διαβαθμισμένες Πληροφορίες μόνο για τους σκοπούς για τους οποίους προβλέπονται.

Άρθρο 6
Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται μέσω της διπλωματικής οδού εκτός εάν οι Αρμόδιες Αρχές αποφασίσουν διαφορετικά. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς τη λήψη των Διαβαθμισμένων Πληροφοριών.

2. Η ηλεκτρονική διαβίβαση Διαβαθμισμένων Πληροφοριών διεξάγεται μέσω πιστοποιημένων κρυπτογραφικών μέσων τα οποία εγκρίνονται αμοιβαία από τις Αρμόδιες Αρχές.

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

Για την Κυπριακή Δημοκρατία:
Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ του Υπουργείο Εξωτερικών.
Λεωφόρος Προεδρικού Μεγάρου
1447, Λευκωσία

Για τη Δημοκρατία της Σερβίας:
Υπηρεσία Εθνικής Ασφαλείας και Προστασίας Διαβαθμισμένων Πληροφοριών
Nemanjina 22-26
11 000 Belgrade

4. Οι υπηρεσίες πληροφοριών, ασφαλείας και οι αστυνομικές υπηρεσίες των Μερών δύνανται, σύμφωνα με την αντίστοιχη εθνική τους νομοθεσία, να ανταλλάσσουν απευθείας μεταξύ τους επιχειρησιακές πληροφορίες και/ή πληροφορίες ασφαλείας.

Άρθρο 7
Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες μεταφράζονται και αναπαράγονται σύμφωνα με την εθνική νομοθεσία του Μέρους Παραλήπτη και υπό 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. Οι Διαβαθμισμένες Πληροφορίες επιπέδου ΑΠΟΡΡΗΤΟ / СТРОГО ПОВЕРЉИВО / SECRET και άνω, μεταφράζονται ή αναπαράγονται μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα.

Άρθρο 8
Καταστροφή Διαβαθμισμένων Πληροφοριών

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

2. Οι Διαβαθμισμένες Πληροφορίες έως το επίπεδο ΑΠΟΡΡΗΤΟ / СТРОГО ПОВЕРЉИВО / SECRET καταστρέφονται σύμφωνα με την εθνική νομοθεσία των Μερών.

3. Οι Διαβαθμισμένες Πληροφορίες επιπέδου ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / ДРЖАВНА ТАЈНА / TOP SECRET δεν καταστρέφονται. Επιστρέφονται στην Αρμόδια Αρχή του Μέρους Αποστολέα.

4. Συντάσσεται έκθεση για την καταστροφή των Διαβαθμισμένων Πληροφοριών και η μετάφρασή της στην Αγγλική γλώσσα αποστέλλεται στην Αρμόδια Αρχή 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 Αρμόδια Αρχή του Μέρους Αποστολέα σχετικά με την εν λόγω καταστροφή το συντομότερο δυνατόν.

Άρθρο 9
Διαβαθμισμένες Συμβάσεις

1. Η Αρμόδια Αρχή του ενός Μέρους παρέχει στην Αρμόδια Αρχή του άλλου Μέρους, γραπτή εγγύηση ότι ο εργολάβος ή ο υπεργολάβος, που επιθυμεί να αναλάβει διαβαθμισμένη σύμβαση επιπέδου ΑΠΟΡΡΗΤΟ/СТРОГО ПОВЕРЉИВО / SECRET και επιπέδου ΕΜΠΙΣΤΕΥΤΙΚΟ / ПОВЕРЉИВО/ CONFIDENTIAL με αυτό το άλλο Μέρος, είναι κάτοχος ή διεξάγει τις απαραίτητες ενέργειες για την εξασφάλιση Εξουσιοδότησης Ασφάλειας Φορέα με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας.

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

α) Δέσμευση του Εργολάβου, με την οποία διασφαλίζεται ότι οι εγκαταστάσεις τους τηρούν τις απαραίτητες προϋποθέσεις για τον χειρισμό και την αποθήκευση Διαβαθμισμένων Πληροφοριών με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας;

β) Δέσμευση του Εργολάβου με την οποία διασφαλίζεται ότι τα άτομα που εκτελούν καθήκοντα τα οποία απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες είναι δεόντως εξουσιοδοτημένα, σύμφωνα με την εθνική νομοθεσία, να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες με το αντίστοιχο επίπεδο διαβάθμισης ασφαλείας;

γ) Απαίτηση ότι ο Εργολάβος διασφαλίζει ότι όλα τα άτομα που έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες είναι ενημερωμένα σχετικά με τις ευθύνες τους για προστασία των Διαβαθμισμένων Πληροφοριών σύμφωνα με την εθνική νομοθεσία;

δ) Κατάλογο με τις Διαβαθμισμένες Πληροφορίες και κατάλογο με τους χώρους στους οποίους ενδέχεται να προκύψουν Διαβαθμισμένες Πληροφορίες;

ε) Διαδικασία γνωστοποίησης των αλλαγών στο επίπεδο διαβάθμισης ασφαλείας των Διαβαθμισμένων Πληροφοριών;

στ) Μέσα επικοινωνίας και ηλεκτρονικά μέσα διαβίβασης;

ζ) Τις διαδικασίες διαβίβασης Διαβαθμισμένων Πληροφοριών;

η) Δέσμευση του Εργολάβου ότι θα ενημερώσει για τυχόν πραγματική ή ενδεχόμενη Παραβίαση Ασφαλείας;

θ) Δέσμευση του Εργολάβου ότι θα προωθήσει αντίγραφο της Διαβαθμισμένης Σύμβασης στην οικεία Αρμόδια Αρχή;

ι) Δέσμευση του υπεργολάβου ότι θα εκπληρώσει τις ίδιες υποχρεώσεις ασφαλείας με τον Εργολάβο.

3. Μόλις ξεκινήσουν οι διαπραγματεύσεις με τους πιθανούς Εργολάβους, η Αρμόδια Αρχή του Μέρους Αποστολέα ενημερώνει την Αρμόδια Αρχή του άλλου Μέρους σχετικά με το επίπεδο διαβάθμισης ασφαλείας των Διαβαθμισμένων Πληροφοριών που σχετίζονται με τις εν λόγω διαπραγματεύσεις.

4. Αντίγραφο κάθε Διαβαθμισμένης Σύμβασης αποστέλλεται στην Αρμόδια Αρχή του Μέρους όπου θα διεξαχθούν οι εργασίες, για την κατάλληλη επίβλεψη και έλεγχο ασφαλείας.

Άρθρο 10
Διαβαθμισμένες Επισκέψεις

1. Επισκέψεις που σχετίζονται με Διαβαθμισμένες Συμβάσεις και συνεπάγονται πρόσβαση σε Διαβαθμισμένες Πληροφορίες υπόκεινται στη εκ των προτέρων γραπτή έγκριση της Αρμόδιας Αρχής του Μέρους Υποδοχής.

2. Η Αρμόδια Αρχή του Μέρους Υποδοχής θα πρέπει να λάβει αίτηση επίσκεψης τουλάχιστον δέκα ημέρες νωρίτερα.

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

4. Η αίτηση επίσκεψης περιλαμβάνει:

α) ονοματεπώνυμο του επισκέπτη, τόπο και ημερομηνία γέννησης, υπηκοότητα και αριθμό διαβατηρίου ή ταυτότητας;

β) επωνυμία του νομικού προσώπου το οποίο εκπροσωπεί ο επισκέπτης και τη θέση του επισκέπτη στο νομικό πρόσωπο;

γ) επωνυμία, διεύθυνση και στοιχεία επικοινωνίας του νομικού προσώπου που πρόκειται να δεχθεί την επίσκεψη;

δ) πληροφορίες για την Εξουσιοδότηση Ασφάλειας Προσωπικού, της εγκυρότητάς της και του επιπέδου της;

ε) σκοπό και λόγους της επίσκεψης;

στ) αναμενόμενη ημερομηνία και διάρκεια της επίσκεψης. Σε περίπτωση επαναλαμβανόμενων επισκέψεων, αναφέρεται η συνολική διάρκεια των επισκέψεων;

ζ) ημερομηνία, υπογραφή και επίσημη σφραγίδα της Αρμόδιας Αρχής.

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

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

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

Άρθρο 11
Παραβίαση Ασφαλείας

1. Σε περίπτωση παραβίασης ασφαλείας, η Αρμόδια Αρχή του Μέρους Παραλήπτη ενημερώνει την Αρμόδια Αρχή του Μέρους Αποστολέα, το συντομότερο δυνατόν, και ξεκινά την κατάλληλη έρευνα.

2. Εάν η παραβίαση ασφαλείας επέλθει σε τρίτη χώρα, η Αρμόδια Αρχή του Μέρους Αποστολέα λαμβάνει όλα τα απαραίτητα μέτρα για να διασφαλίσει ότι οι δράσεις που περιγράφονται στην Παράγραφο 1 έχουν τεθεί σε εφαρμογή.

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

4. Το Μέρος Αποστολέας ενημερώνεται για τα αποτελέσματα της έρευνας και λαμβάνει την τελική έκθεση για τους λόγους και την έκταση της ζημιάς.

Άρθρο 12
Έξοδα

Κάθε Μέρος αναλαμβάνει τα δικά του έξοδα που προκύπτουν κατά την εφαρμογή και εποπτεία της παρούσας Συμφωνίας.

Άρθρο 13
Διευθέτηση Διαφορών

Τυχόν διαφορά αναφορικά με την ερμηνεία ή εφαρμογή της παρούσας Συμφωνίας διευθετείται με διαπραγματεύσεις μεταξύ των Μερών. Κατά την διάρκεια των διαπραγματεύσεων και τα δύο Μέρη συνεχίζουν να εκπληρώνουν όλες τις υπόλοιπες υποχρεώσεις τους που απορρέουν από την παρούσα Συμφωνία.

Άρθρο 14
Τελικές Πρόνοιες

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

2. Η παρούσα Συμφωνία δύναται να τροποποιείται ανά πάσα στιγμή, κατόπιν αμοιβαίας γραπτής έγκρισης των Μερών. Οι τροποποιήσεις τίθενται σε ισχύ σύμφωνα με την Παράγραφο 1.

3. Κάθε Μέρος δύναται, ανά πάσα στιγμή, να καταγγείλει τη Συμφωνία με γραπτή ειδοποίηση προς το άλλο Μέρος, μέσω της διπλωματικής οδού. Στην περίπτωση αυτή, η λήξη της Συμφωνίας θα ισχύει έξι μήνες μετά την ημερομηνία λήψης της αντίστοιχης ανακοίνωσης.

4. Παρά την καταγγελία της παρούσας Συμφωνίας, τα Μέρη διασφαλίζουν ώστε όλες οι Διαβαθμισμένες Πληροφορίες θα συνεχίσουν να προστατεύονται έως ότου το Μέρος Αποστολέας απαλλάξει το Μέρος Παραλήπτη από τις υποχρεώσεις του.

Συντάχθηκε στην Λευκωσία στις 27 Νοεμβρίου 2017 σε δύο πρωτότυπα σετ αντιγράφων, στην Ελληνική, Σερβική και Αγγλική γλώσσα, και όλα τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση διαφωνίας στην ερμηνεία, το Αγγλικό κείμενο υπερισχύει.

Για την κυβέρνηση της Κυπριακής Δημοκρατίας

.....

Για την κυβέρνηση της Δημοκρατίας της Σερβίας

.....

[SERBIAN TEXT – TEXTE SERBE]

Споразум између Владе Републике Кипра и Владе Републике Србије о размени и узајамној заштити тајних података

Влада Републике Кипра и Влада Републике Србије (у даљем тексту: „Стране"),

увиђајући потребу да утврде правила за заштиту тајних података које узајамно размене у оквиру своје политичке, војне, привредне, правне, научно-технолошке или било које друге сарадње, као и правила за заштиту тајних података које створе у процесу те сарадње,

у намери да осигурају узајамну заштиту свих тајних података које је једна страна одредила као тајне и пренела их другој страни, односно тајних података који су заједнички створени у процесу сарадње између Страна,

у жељи да створе скуп правила о узајамној заштити тајних података који се размене између Страна,

с обзиром на обострани интерес за заштиту тајних података у складу са законодавством Страна,

споразумеле су се о следећем:

Члан 1.
Циљ

Циљ овог споразума је да осигура заштиту тајних података које стране заједнички створе или размене.

Члан 2.
Дефиниције

У сврху овог споразума наведени термини имају следеће значење:

а) **„повреда безбедности"**- радња или пропуст супротан овом споразуму или националном законодавству страна који може да доведе до откривања, губитка, уништења, противправног присвајања, односно било који други вид угрожавања безбедности тајних података;

б) **„уговор с тајним подацима”**- споразум између два или више уговорача који садржи тајне податке или чија примена захтева приступ тајним подацима;

ц) **„тајни подаци”** - сви подаци, независно од њихове форме или природе, који захтевају заштиту од неовлашћеног руковања и који су одређени као тајни у складу са националним законодавством обе Стране, односно сви подаци који су означени одређеним степеном тајности;

д) **„надлежни орган”**- национални безбедносни орган и свако друго надлежно тело које је, према националном законодавству Страна, одговорно за примену овог споразума, као што се наводи у члану 4. став 1. овог споразума;

е) **„уговарач”** - физичко или правно лице које поседује правну способност да закључује уговоре с тајним подацима;

ф) **„безбедносни сертификат за правно лице”** - решење надлежног органа којим се потврђује да правно или/и физичко лице поседује физичку и организациону способност да рукује тајним подацима и чува их у складу са националним законодавством;

г) **„потребно да зна”** - потреба да се оствари приступ конкретним тајним подацима у оквиру одређеног радног места и ради извршења конкретног задатка;

х) **„страна давалац”**- страна која је створила тајне податке;

и) **„безбедносни сертификат за физичка лица”**- решење надлежног органа којим се потврђује, у складу са националним законодавством, да физичко лице испуњава услове да оствари приступ тајним подацима;

ј) **„страна прималац”** - страна којој се преносе тајни подаци стране даваоца;

к) **„трећа страна”** - свака држава, организација, правно или физичко лице који није страна у овом споразуму.

Члан 3.
Степени тајности

Стране су сагласне да су наведени степени и ознаке тајности еквивалентни и подударни са степенима тајности утврђеним њиховим националним законодавством:

За Републику Кипар	За Републику Србију	енглески екивалент
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	ДРЖАВНА ТАЈНА	TOP SECRET
ΑΠΟΡΡΗΤΟ	СТРОГО ПОВЕРЉИВО	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ПОВЕРЉИВО	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	ИНТЕРНО	RESTRICTED

Члан 4.
Надлежни органи

1. Надлежни органи страна су:

За Владу Републике Кипра:
National Security Authority
Ministry of Defense of the Republic of Cyprus

За Владу Републике Србије:
Канцеларија Савета за националну безбедност и заштиту тајних података

2. Стране се међусобно обавештавају дипломатским путем о свакој промени у вези са својим надлежним органима.

3. Надлежни органи се међусобно обавештавају о својим националним законима о тајним подацима и свим значајним изменама и допунама тих закона и размењују информације о безбедносним стандардима, процедурама и праксама у заштити тајних података.

Члан 5.

Мере заштите и приступ тајним подацима

1. У складу са својим националним законодавством, стране предузимају све потребне мере за заштиту тајних података који ће бити размењени или створени на основу овог споразума. Тим тајним подацима биће додељен најмање исти степен заштите који се обезбеђује националним тајним подацима еквивалентног степена тајности у складу са чланом 3. овог споразума.

2. Страна давалац обавештава писаним путем страну примаоца о свакој измени степена тајности података које је доставила.

3. Приступ тајним подацима ограничен је на лица која поступају по принципу „потребно да зна" и која су овлашћена да остваре приступ тајним подацима еквивалентног степена тајности у складу са националним законодавством обе Стране.

4. У оквиру примене овог споразума свака страна признаје безбедносне сертификате за правна и физичка лица који се издају у складу с националним законодавством друге стране. Безбедносни сертификати су еквивалентни у складу са чланом 3 овог споразума.

5. У складу са националним законодавством, надлежни органи, на захтев, пружају узајамну помоћ у вези са спровођењем процедура безбедносних провера потребних ради примене овог споразума.

6. У оквиру примене овог споразума надлежни органи обе Стране међусобно се обавештавају о свакој промени у вези са безбедносним сертификатима за физичка и правна лица, посебно о његовом опозиву или снижењу степена тајности.

7. Страна прималац:

а) доставља тајне податке било којој трећој страни само уз претходну писану сагласност стране даваоца;

б) означава примљене тајне податке у складу са чланом 3 овог споразума;

ц) користи тајне податке искључиво у сврхе у које су достављени.

Члан 6.
Пренос тајних података

1. Тајни подаци се преносе дипломатским путем, осим ако другачије не одоборе надлежни органи. Страна прималац потврђује пријем тајних података писаним путем.

2. Електронски пренос тајних података врши се уз помоћ сертификованих криптографских средстава о којима се договоре надлежни органи.

3. Главне улазно-излазне тачке за размену тајних података према овом споразумом су:

За Републику Кипар:
Централни регистар „ДРЖАВНА ТАЈНА" при Министарству спољних послова.
Presidential Palace Avenue, 1447 Nicosia

За Републику Србију:
Централни регистар за стране тајне податке у Канцеларији Савета за националну безбедност и заштиту тајних података

4. Безбедносно-обавештајне и полицијске службе држава Страна могу сарађивати и непосредно размењивати оперативне и/или обавештајне податке у складу са националним законодавством.

Члан 7.
Умножавање и превођење тајних података

1. Превођење и умножавање тајних података врши се у складу са националним законодавством стране примаоца и следећим процедурама:

а) преводи и умножени примерци се означавају и штите као оригинали тајних података;

б) преводи и умножени примерци се ограничавају на број који се захтева у службене сврхе;

ц) на преводе се ставља одговарајућа напомена на језику превода у којој се наводи да садрже тајне податке добијене од стране даваоца.

2. Подаци с ознаком тајности АПОРРНТО/ СТРОГО ПОВЕРЉИВО/ SECRET или вишом преводе се или умножавају само уз претходну писану сагласност стране даваоца.

Члан 8.
Уништавање тајних података

1. Тајни подаци се уништавају на начин који онемогућава њихову делимичну или потпуну реконструкцију.

2. Подаци с ознаком тајности АПОРРНТО/ СТРОГО ПОВЕРЉИВО/ SECRET се уништавају у складу с националним законодавством.

3. Подаци с ознаком тајности АКРΩΣ АПОРРНТО/ ДРЖАВНА ТАЈНА/ TOP SECRET се не уништавају, него се враћају надлежном органу стране даваоца.

4. О уништавању тајних података саставља се записник чији се енглески превод доставља надлежном органу стране даваоца.

5. Тајни подаци се неодложно уништавају у случају кризне ситуације, када их није могуће заштитити или вратити. Страна прималац, што је могуће пре, обавештава надлежни орган стране даваоца о том уништењу.

Члан 9.
Уговор који садржи тајне податке

1. Како би са другом страном закључио уговор с тајним подацима с ознаком АПОРРНТО/ СТРОГО ПОВЕРЉИВО/ SECRET и ΕΜΠΙΣΤΕΥΤΙΚΟ/ ПОВЕРЉИВО / CONFIDENTIAL, надлежни безбедносни орган једне стране претходно доставља националном безбедносном органу друге стране писану гаранцију да уговарач или подуговарач поседује безбедносни сертификат за правна лица одговарајућег степена тајности односно да је поступак прибављања тог сертификата у току.

2. Сваки уговор који садржи тајне податке закључен у складу са овим споразумом треба да садржи:

а) обавезу уговарача да у својим објектима обезбеди потребне услове за руковање и чување тајних података одговарајућег степена тајности;

б) обавезу уговарача да обезбеди да лица која обављају дужности које захтевају приступ тајним подацима буду овлашћена да остваре приступ тајним подацима одговарајућег степена тајности у складу са националним законодавством;

ц) захтев да уговарач обезбеди да сва лица са приступом тајним подацима буду обавештена о својим обавезама у вези са заштитом тајних података у складу с националним законодавством;

д) списак тајних података и списак области у којима могу настати тајни подаци;

е) процедуру за достављање измена у вези са степеном тајности података;

ф) средства комуникације и електронског преноса;

г) процедуру преноса тајних података;

х) обавезу уговарача да обавести о свим стварним или могућим повредама безбедности;

и) обавезу уговарача да проследи примерак уговора с тајним подацима свом надлежном органу;

ј) обавезу подуговарача да испуни исте безбедносне обавезе као уговарач.

3. Чим започну преговори за закључење уговора између потенцијалних уговарача, надлежни орган стране даваоца обавестиће надлежни орган друге стране о степену тајности додељеном тајним подацима који се односе на преговоре за закључење уговора.

4. Примерак сваког уговора који садржи тајне податке прослеђује се надлежном органу стране на чијој територији треба да се изврши тај посао, како би се омогућио одговарајући безбедносни надзор и контрола.

Члан 10.

Посете

1. Посете у вези са уговорима са тајним подацима које укључују приступ тајним подацима подлежу претходном писаном одобрењу надлежног органа стране домаћина.

2. Надлежни орган стране домаћина прима захтев за посету најмање десет дана унапред.

3. У хитним случајевима, захтев за посету може се доставити у краћем року.

4. Захтев за посете треба да садржи:

а) име и презиме, место и датум рођења, држављанство и број путне или личне исправе посетиоца;

б) назив правног лица чији је посетилац представник и функцију посетиоца у том правном лицу;

ц) име, адреса и контакт информације правног лица које треба посетити;

д) потврду о безбедносном сертификату за физичка лица, њено важење и степен тајности;

е) предмет и сврху посете;

ф) очекивани датум и трајање посете која се захтева; у случају периодичних посета, треба навести укупан период који ће бити обухваћен тим посетама;

г) датум, потпис и службени печат надлежног органа.

5. Када посета буде одобрена, надлежни орган стране домаћина доставља примерак захтева за посету руковаоцима тајним подацима у правном лицу које треба посетити.

6. Важење одборења за посету не сме бити дуже од годину дана.

7. Надлежни органи страна могу да направе спискове физичких лица која су овлашћена да реализују периодичне посете. Ти спискови важе за почетни период од дванаест месеци. Услови под којима се обављају те посете биће непосредно договорени са надлежним лицима за контакт код правног лица које ће та физичка лица посетити у складу са договореним условима.

Члан 11.
Повреда безбедности

1. У случају повреде безбедности, надлежни орган стране примаоца ће, што је пре могуће, обавестити надлежни орган стране даваоца и покренути одговарајућу истрагу.

2. У случају да повреда безбедности наступи у трећој држави, надлежни орган стране пошиљаоца предузеће све потребне мере да обезбеди покретање радњи предвиђених у ставу 1. овог члана.

3. На захтев, страна давалац сарађује у истрази у складу са ставом 1. овог члана.

4. Страна давалац ће бити обавештена о резултатима истраге и добити завршни извештај о узроцима и обиму штете.

Члан 12.
Трошкови

Свака страна сноси трошкове који настану током примене и надзора примене овог споразума.

Члан 13.
Решавање спорова

Сваки спор у вези са тумачењем односно применом овог споразума решава се преговорима између страна. Током трајања тих преговора обе стране настављају да испуњавају све друге обавезе према овом споразуму.

Члан 14.
Завршне одредбе

1. Овај споразум се закључује на неодређено време, а ступа на снагу првог дана другог месеца после датума пријема последњег писаног обавештења којим се стране међусобно обавештавају дипломатским путем о испуњењу свих унутрашњих правних претпоставки за ступање на снагу овог споразума.

2. Овај споразум може у сваком тренутку бити измењен и допуњен на основу обостране писане сагласности страна. Измене и допуне ступају на снагу у складу са ставом 1. овог члана.

3. Свака страна може у сваком тренутку отказати овај споразум достављањем писаног обавештења другој страни дипломатским путем. У том случају, отказ ступа на снагу шест месеци после датума пријема таквог обавештења.

4. Без обзира на отказ овог споразума, стране су дужне да обезбеде континуирану заштиту тајних података, све док страна давалац не ослободи страну примаоца те обавезе.

Сачињено у Никозији дана 27 јануара 2017 у два оригинална примерка, сваки на грчком, српском и енглеском језику, при чему су сви текстови подједнако веродостојни. У случају неслагања у тумачењу, биће меродаван текст Споразума на енглеском језику.

За Владу
Републике Кипар

.....

За Владу
Републике Србије

.....

[TRANSLATION – TRADUCTION]

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

Le Gouvernement de la République de Chypre
et
le Gouvernement de la République de Serbie

(ci-après dénommés les « Parties contractantes »),

Reconnaissant la nécessité d'établir des règles relatives à la protection des informations classifiées échangées dans le cadre d'une coopération politique, militaire, économique, juridique, scientifique et technologique ou autre, ainsi que des informations classifiées issues de cette coopération,

Souhaitant garantir la protection réciproque de toutes les informations classifiées qui ont été classifiées par une Partie et transmises à l'autre Partie ou qui ont été générées conjointement dans le cadre de la coopération entre les Parties,

Désireux de définir un ensemble de règles en matière de 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 convenus de ce qui suit :

Article premier
Objectif

Le présent Accord a pour objectif de garantir la protection des informations classifiées qui sont générées mutuellement par les Parties ou échangées entre ces dernières.

Article 2
Définitions

Aux fins du présent Accord :

a) le terme « atteinte à la sécurité » s'entend d'un acte ou d'une omission contraire au présent Accord ou à la législation nationale des Parties, dont le résultat peut conduire à la divulgation, la perte, la destruction, le détournement ou tout autre type de compromission d'informations classifiées;

b) le terme « contrat classifié » s'entend d'un accord entre deux ou plusieurs contractants, qui contient des informations classifiées, ou dont la réalisation nécessite d'avoir accès à celles-ci;

c) le terme « informations classifiées » s'entend des informations, quelle que soit leur forme ou leur nature, qui doivent être protégées contre l'utilisation non autorisée, qui ont été classifiées conformément à la législation nationale des Parties, et qui, par conséquent, se sont vu attribuer un niveau de classification de sécurité;

d) le terme « autorité compétente » s'entend de l'Agence nationale de sécurité et toute autre entité compétente qui, en vertu de la législation des Parties, est chargée de la mise en œuvre du présent Accord, comme indiqué au paragraphe 1 de l'article 4 de celui-ci ;

e) le terme « contractant » s'entend d'une personne physique ou morale dotée de la capacité juridique de conclure des contrats classifiés ;

f) le terme « habilitation de sécurité des installations » s'entend de l'attestation par une autorité compétente qu'une personne physique ou morale dispose des capacités physiques et organisationnelles nécessaires pour traiter et stocker des informations classifiées conformément à la législation interne de la Partie concernée;

g) le terme « besoin d'en connaître » s'entend de la nécessité d'avoir accès à des informations classifiées spécifiques dans le cadre d'une fonction officielle déterminée et pour l'exécution d'une mission spécifique;

h) le terme « Partie d'origine » s'entend de la Partie qui est à l'origine des informations classifiées;

i) le terme « habilitation individuelle de sécurité » s'entend de l'autorisation donnée par une autorité compétente attestant, conformément à la législation interne respective des Parties, qu'une personne est habilitée à avoir accès à des informations classifiées ;

j) le terme « Partie destinataire » s'entend de la Partie à laquelle les informations classifiées de la Partie d'origine sont transmises;

k) le terme « tierce partie » s'entend de tout État, toute organisation, toute personne morale ou toute personne physique qui n'est pas partie au présent Accord.

Article 3
Niveaux de classification de sécurité

Les Parties conviennent que les niveaux de classification de sécurité et les marquages suivants sont équivalents et correspondent aux niveaux de classification de sécurité spécifiés dans leur législation nationale : Pour la République de Chypre	Pour la République de Serbie	Équivalent en français
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	ДРЖАВНА ТАЈНА	TRÈS SECRET
ΑΠΟΡΡΗΤΟ	СТРОГО ПОВЕРЉИВО	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ПОВЕРЉЉИВО	CONFIDENTIEL

ΠΕΡΙΟΡΙΕΜΕΝΗ 2 XPH2HX	ИНТЕРНО	RESTREINT

Article 4
Autorités compétentes

1. Les autorités compétentes des Parties sont :

Pour le Gouvernement de la République de Chypre :

Agence nationale de sécurité

Ministère de la défense de la République de Chypre

Pour le Gouvernement de la République de Serbie :

Bureau du Conseil de la sécurité nationale et de la protection des informations classifiées

2. Les Parties s'informent mutuellement, par voie diplomatique, de tout changement ou modification concernant leur autorité compétente.

3. Les autorités compétentes s'informent mutuellement de la législation nationale respective sur les informations classifiées et de toute modification importante de celle-ci, et échangent des informations sur les normes, procédures et pratiques de sécurité visant 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 échangées ou générées en vertu du présent Accord. Ces informations classifiées bénéficient au moins du même niveau de protection que celui prévu pour les informations nationales classifiées d'un niveau de classification de sécurité équivalent conformément à l'article 3.

2. La Partie d'origine informe par écrit la Partie destinataire de toute modification du niveau de classification de sécurité des informations classifiées transmises.

3. L'accès à des informations classifiées n'est accordé, selon le principe du besoin d'en connaître, qu'aux personnes habilitées, en vertu de la législation nationale des Parties, à accéder aux informations classifiées d'un niveau de classification de sécurité équivalent.

4. Dans le cadre du présent Accord, chaque Partie reconnaît les habilitations individuelles de sécurité et les habilitations de sécurité des installations délivrées conformément à la législation nationale de l'autre Partie. Les habilitations de sécurité sont équivalentes dans le cadre de l'article 3.

5. Les autorités compétentes, conformément à la législation nationale, se prêtent mutuellement assistance, sur demande, pour l'exécution des procédures d'agrément nécessaires à l'application du présent Accord.

6. Dans le cadre du présent Accord, les autorités compétentes des Parties s'informent mutuellement et sans délai de toute modification relative aux habilitations individuelles de sécurité et aux habilitations de sécurité des installations, notamment de leur retrait ou de leur déclassement.

7. La Partie destinataire :

a) transmet les informations classifiées à une tierce partie uniquement si elle a reçu l'accord préalable écrit de la Partie d'origine;

b) appose sur les informations classifiées les indications nécessaires conformément à l'article 3;

c) utilise les informations classifiées aux seules fins pour lesquelles celles-ci ont été fournies.

Article 6
Transmission des informations classifiées

1. Les informations classifiées sont transmises par la voie diplomatique, sauf modalité contraire autorisée par les autorités compétentes. La Partie destinataire confirme par écrit la réception des informations classifiées.

2. La transmission électronique des informations classifiées s'effectue au moyen de méthodes certifiées de chiffrement dont conviennent les autorités compétentes.

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

Pour la République de Chypre :

Le Groupe central de l'enregistrement (des textes administratifs) « TRÈS SECRET » au Ministère des affaires étrangères

Avenue du Palais présidentiel

1447, Nicosie

Pour la République de Serbie :

Bureau du Conseil de la sécurité nationale et de la protection des informations classifiées

Nemanjina 22-26

11 000 Belgrade

4. Les services de renseignement, de sécurité et de police des Parties peuvent, conformément à leurs législations nationales respectives, s'échanger directement des informations opérationnelles et/ou des renseignements.

Article 7
Reproduction et traduction d'informations classifiées

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

a) les traductions et les 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 reproductions sont limités au nombre requis à des fins officielles;

c) les traductions portent une mention 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 portant la marque de classification АПОРРНТО/СТРОГО ПОВЕРЈтИВО/SECRET ou une marque de classification supérieure ne sont traduites ou reproduites qu'avec le consentement préalable écrit de la Partie d'origine.

Article 8
Destruction des informations classifiées

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

2. Les informations classifiées portant la marque de classification АПОРРНТО/СТРОГО ПОВЕРЈЛИВО/SECRET sont détruites conformément à la législation nationale.

3. Les informations classifiées portant la marque de classification AKPQS АПОРРНТО/ДРЖАВНА ТАЈНА/TOP SECRET ne sont pas détruites. Elles sont restituées à l'autorité compétente de la Partie d'origine.

4. Un rapport sur la destruction des informations classifiées est établi et sa traduction anglaise est remise à l'autorité compétente 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 immédiatement détruites. La Partie destinataire informe l'autorité compétente de la Partie d'origine de cette destruction dans les meilleurs délais.

Article 9
Contrats classifiés

1. L'autorité compétente d'une Partie fournit à l'autorité compétente de l'autre Partie l'assurance écrite préalable qu'un contractant ou un sous-traitant, souhaitant entreprendre un contrat classifié de niveau АНОРРНТО/СТРОГО ПОВЕРЈЛИВО/SECRET et ΕΜΠΙΣΤΕΥΤΙΚΟ/ΠΟΒΕΡΙΛΗΒΟ/CONFIDENTIEL avec cette autre Partie, détient ou est en passe d'obtenir une habilitation de sécurité des installations du niveau de classification de sécurité approprié.

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

a) une preuve de l'engagement du contractant à veiller à ce que ses locaux réunissent les conditions nécessaires au traitement et au stockage d'informations classifiées au niveau de classification de sécurité approprié;

b) une preuve de l'engagement du contractant à faire en sorte que les personnes qui exercent des fonctions nécessitant l'accès à des informations classifiées sont autorisées, conformément à la

législation nationale, à accéder à des informations classifiées du niveau de classification de sécurité approprié;

c) une obligation du contractant à veiller à ce que toutes les personnes ayant accès aux informations classifiées soient informées de leur responsabilité en matière de protection des informations classifiées conformément à la législation nationale;

d) la liste des informations classifiées et la liste des domaines dans lesquels des informations classifiées peuvent être produites;

e) la procédure de communication des changements de niveau de classification de sécurité des informations classifiées;

f) la liste des moyens de communication et des moyens électroniques de transmission;

g) la procédure de transmission des informations classifiées ;

h) une déclaration du contractant par laquelle celui-ci s'engage à notifier toute atteinte réelle ou présumée à la sécurité;

i) une preuve de l'engagement du contractant à transmettre à sa propre autorité compétente un exemplaire du contrat classifié;

j) une déclaration du sous-traitant dans laquelle celui-ci s'engage à respecter les mêmes obligations en matière de sécurité que le contractant.

3. Dès que des négociations précontractuelles sont engagées entre des contractants éventuels, l'autorité compétente de la Partie d'origine informe l'autorité compétente de l'autre Partie du niveau de classification de sécurité attribué aux informations classifiées visées par ces négociations précontractuelles.

4. Un exemplaire de chaque contrat classifié est également transmis à l'autorité compétente de la Partie dans laquelle les travaux seront réalisés, de façon à permettre un suivi et un contrôle adéquats en matière de sécurité.

Article 10
Visites

1. Les visites relatives à des contrats classifiés et impliquant l'accès à des informations classifiées sont soumises à une autorisation préalable écrite de l'autorité compétente de la Partie hôte.

2. L'autorité compétente de la Partie hôte reçoit la demande de visite au moins dix jours à l'avance.

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

4. La demande de visite comporte les informations suivantes :

a) le prénom, le nom, le lieu et la date de naissance, la nationalité, le numéro du passeport ou du document d'identité du visiteur;

b) nom de la personne morale représentée par le visiteur et la fonction du visiteur à l'égard de la personne morale;

c) le nom, l'adresse et les coordonnées de la personne morale faisant l'objet de la visite;

d) la preuve que le visiteur dispose d'une habilitation individuelle de sécurité, et les informations concernant la validité de celle-ci et le niveau de classification de sécurité dont il est question;

e) l'objet et le but de la visite;

f) la date et la durée prévues de la visite demandée. Dans le cas de visites répétées, la période totale au cours de laquelle les visites seront effectuées est indiquée;

g) la date, la signature et le cachet officiel de l'autorité compétente.

5. Une fois la visite approuvée, l'autorité compétente de la Partie hôte fournit une copie de la demande de visite aux agents responsables de la sécurité de la personne morale faisant l'objet de la visite.

6. La durée de validité de l'autorisation de visite ne dépasse pas un an.

7. Les autorités compétentes des Parties peuvent établir des listes de personnes autorisées à effectuer des visites régulières. Les listes sont valables pour une période initiale de douze mois. Les modalités des différentes visites sont définies directement avec les points de contact compétents de la personne morale qui fera l'objet des visites par ces personnes, conformément aux conditions convenues.

Article 11
Atteinte à la sécurité

1. En cas d'atteinte à la sécurité, l'autorité compétente de la Partie destinataire en informe dès que possible l'autorité compétente de la Partie d'origine et ouvre une enquête appropriée.

2. Si une atteinte à la sécurité se produit dans un État tiers, l'autorité compétente de la Partie expéditrice prend toutes les dispositions nécessaires pour que les actions prévues au paragraphe 1 soient engagées.

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

4. La Partie d'origine est informée des résultats de l'enquête et reçoit le rapport définitif quant aux raisons et à l'étendue des dégâts provoqués.

Article 12
Charges

Chaque Partie prend en charge les dépenses qu'elle a encourues dans le cadre de la mise en œuvre et de la supervision du présent Accord.

Article 13
Règlement des différends

Tout litige relatif à l'interprétation ou à la mise en application du présent Accord est réglé par voie de négociation entre les Parties. Pendant les négociations, les deux Parties continuent à remplir toutes les autres obligations découlant du présent Accord.

Article 14
Dispositions finales

1. Le présent Accord est conclu pour une durée indéterminée et entre en vigueur le premier jour du deuxième mois suivant la date de réception de la dernière notification écrite par laquelle les Parties se sont mutuellement informées, par la voie diplomatique, que leurs exigences juridiques nationales nécessaires à son entrée en vigueur ont été remplies.

2. Le présent Accord peut être modifié à tout moment sur la base d'un accord mutuel écrit des Parties. Ces modifications entrent en vigueur conformément aux dispositions du paragraphe 1.

3. Chaque Partie peut, à tout moment, dénoncer le présent Accord par une notification écrite adressée à l'autre Partie par la voie diplomatique. Dans ce cas, la dénonciation prend effet six mois après la date de réception de la notification correspondante.

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 d'origine dispense la Partie destinataire de cette obligation.

FAIT à Nicosie, le 27 novembre 2017, en deux exemplaires originaux, chacun en langues grecque, serbe et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, la version anglaise prévaut.

Pour le Gouvernement de la République de Serbie :

[SIGNÉ]

Pour le Gouvernement de la République de Chypre :

[SIGNÉ]