Ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Εσθονίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2013 εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος.

Αριθμός 15(ΙΙΙ) του 2013

ΝΟΜΟΣ ΠΟΥ ΚΥΡΩΝΕΙ ΤΗ ΣΥΜΦΩΝΙΑ ΜΕΤΑΞΥ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΚΑΙ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΕΣΘΟΝΙΑΣ ΓΙΑ ΤΗΝ ΑΜΟΙΒΑΙΑ ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η Βουλή των Αντιπροσώπων ψηφίζει ως ακολούθως:

Συνοπτικός τίτλος.

1. Ο παρών Νόμος θα αναφέρεται ως ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Εσθονίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2013.

Ερμηνεία.

2. Στον παρόντα Νόμο, εκτός εάν από το κείμενο προκύπτει διαφορετική έννοια-

«Συμφωνία» σημαίνει τη Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Εσθονίας για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών, η διαπραγμάτευση της οποίας έγινε κατόπιν της Απόφασης του Υπουργικού Συμβουλίου με αριθμό 2/2009 και ημερομηνία 20.5.2009 και η οποία υπογράφηκε στις 27.11.2012, κατόπιν Απόφασης του Υπουργικού Συμβουλίου με αριθμό 73.986 και ημερομηνία 23.8.2012.

Κύρωση της Συμφωνίας. Πίνακας. Μέρος Ι. Μέρος ΙΙ. Μέρος ΙΙΙ.

3. Με τον παρόντα Νόμο κυρώνεται η Συμφωνία, το κείμενο της οποίας εκτίθεται, στην Αγγλική γλώσσα στο Μέρος Ι του Πίνακα, στην Ελληνική γλώσσα στο Μέρος ΙΙ του Πίνακα και στην Εσθονική γλώσσα στο Μέρος ΙΙΙ του Πίνακα.

ΠΙΝΑΚΑΣ
(Άρθρο 3)

Μέρος Ι

Agreement between the Government of the Republic of Cyprus and the Government of the Republic of Estonia on Mutual Protection of Classified Information

The Government of the Republic of Cyprus and the Government of the Republic of Estonia

(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 commonly 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 unauthorised manipulation 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;

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 an individual has the physical and organizational capability to handle and store Classified Information in accordance with the respective national legislation;

g) "**National Security Authority**" 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; the respective authorities of the Parties are referred to in Article 4 Paragraph 1 of this Agreement;

h) "**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;

i) "**Originating Party**" means the Party which has created Classified Information;

j) "**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;

k) "**Receiving Party**" means the Party to which Classified Information of the Originating Party is transmitted;

l) "**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 are equivalent and correspond to the security classification levels specified in their national legislation:

For the Republic of Cyprus	For the Republic of Estonia	Equivalent in English
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TÄIESTI SALAJANE	TOP SECRET
ΑΠΟΡΡΗΤΟ	SALAJANE	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	KONFIDENTSIAALNE	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	PIIRATUD	RESTRICTED

Article 4
Competent 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 Government of the Republic of Estonia:

Department of the National Security Authority
Ministry of Defence of the Republic of Estonia

2. The Parties shall inform each other through diplomatic channels of any modification of the National Security Authorities.

3. Upon request the National Security Authorities shall notify each other about other Competent Authorities.

4. The National Security Authorities shall inform each other of 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 recognise 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 accordance with 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 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 National Security 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 National Security Authorities.

3. If necessary, the intelligence, security and police services of the Parties may, in accordance with national legislation, exchange operative and intelligence information directly with each other.

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 note in the language of the translation indicating that it contains Classified Information received from the Originating Party.

2. Classified Information marked ΑΠΟΡΡΗΤΟ/SALAJANE or above shall be translated or reproduced only upon 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/SALAJANE shall be destroyed in accordance with the national legislation.

3. Classified Information marked ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TÄIESTI SALAJANE shall not be destroyed. It shall be returned to 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 Security Authority of the Originating Party about this destruction as soon as possible.

Article 9
Classified Contracts

1. The National Security Authority of a Party, wishing to place a Classified Contract with a Contractor of other Party, or wishing to authorise one of its own Contractors to place a Classified Contract in the territory of the other Party shall obtain prior written assurance from the National Security Authority of the other Party that the proposed Contractor is granted Facility Security Clearance of the appropriate security classification level.

2. The Contractor shall submit information about potential sub-contractors for approval to the National Security Authority, in whose territory the work is to be performed.

3. 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 authorised in accordance with the national legislation to have access to Classified Information of the equivalent 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 fulfil the same security obligations as the Contractor.

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

5. Copy of each Classified Contract shall be forwarded to the National Security 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. confirmation 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 authorised 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 National Security Authority of the Receiving Party shall inform the National Security 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 National Security 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 application 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.

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 2012 in two original sets, each in the Greek, Estonian 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

DEMETRIS ELIADES
MINISTER OF DEFENCE

For the Government of the Republic of Estonia

MÄRT KRAFT
DIRECTOR OF THE
NATIONAL SECURITY AUTHORITY

Μέρος ΙΙ

Συμφωνία μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Εσθονίας, για την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών

Η Κυβέρνησης της Κυπριακής Δημοκρατίας
και
η Κυβέρνησης της Δημοκρατίας της Εσθονίας

(εφεξής καλούμενες τα «Μέρη»),

Αναγνωρίζοντας την ανάγκη για τον καθορισμό κανόνων σχετικά με την προστασία διαβαθμισμένων πληροφοριών οι οποίες ανταλλάσσονται 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 κράτος και διαβιβάστηκαν στο άλλο κράτος ή που παράγονται από κοινού στα πλαίσια συνεργασίας μεταξύ των Μερών,

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

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

Συμφώνησαν τα ακόλουθα:

Άρθρο 1
Σκοπός

Σκοπός της παρούσας Συμφωνίας είναι η διασφάλιση της αμοιβαίας προστασίας Διαβαθμισμένων Πληροφοριών οι οποίες παράγονται από κοινού ή ανταλλάσσονται μεταξύ των δύο κρατών.

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 γνώστοποίηση, απώλεια, καταστροφή, παράνομη χρήση ή οποιαδήποτε άλλη έκθεση κινδύνου των Διαβαθμισμένων Πληροφοριών.

β) **«Διαβαθμισμένη Σύμβαση»** σημαίνει κάθε συμφωνία μεταξύ δύο ή περισσοτέρων εργολάβων, η οποία περιέχει ή η εφαρμογή της απαιτεί πρόσβαση σε Διαβαθμισμένες Πληροφορίες.

γ) **«Διαβαθμισμένες Πληροφορίες»** σημαίνει κάθε πληροφορία, ανεξαρτήτως τύπου ή φύσεως, που χρήζει προστασίας από μη εξουσιοδοτημένο χειρισμό και διαβαθμίστηκε σύμφωνα με την εθνική νομοθεσία των Μερών και έχει χαρακτηριστεί με κάποιο επίπεδο διαβάθμισης ασφαλείας.

δ) **«Αρμόδια Αρχή»** σημαίνει την 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.

ε) **«Εργολάβος»** σημαίνει το φυσικό ή νομικό πρόσωπο που έχει τη νομική ικανότητα σύναψης Διαβαθμισμένων Συμβάσεων.

στ) **«Έλεγχος Ασφάλειας Φορέα»** σημαίνει την πιστοποίηση της Αρμόδιας Αρχής Ασφαλείας ότι το νομικό ή φυσικό πρόσωπο έχει την φυσική και οργανωτική ικανότητα να χρησιμοποιεί και να αποθηκεύει Διαβαθμισμένες Πληροφορίες σύμφωνα με την αντίστοιχη εθνική νομοθεσία.

ζ) **«Εθνική Αρχή Ασφαλείας»** σημαίνει την αρχή κάθε Μέρους, η οποία σύμφωνα με την εθνική του νομοθεσία είναι υπεύθυνη για την γενική εφαρμογή και εποπτεία της παρούσας Συμφωνίας. Οι αντίστοιχες αρχές των Μερών αναφέρονται στό Άρθρο 4, Παράγραφος 1 της παρούσας Συμφωνίας.

η) **«Ανάγκη για γνώση»** σημαίνει την ανάγκη πρόσβασης σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες στα πλαίσια συγκεκριμένης επίσημης θέσης και για την εκτέλεση συγκεκριμένης εργασίας.

θ) **«Μέρος αποστολέας»** σημαίνει το Μέρος το οποίο έχει δημιουργήσει την Διαβαθμισμένη Πληροφορία.

η) **«Έλεγχος Ασφαλείας Προσωπικού»** σημαίνει την πιστοποίηση της Αρμόδιας Αρχής, σύμφωνα με την αντίστοιχη εθνική νομοθεσία, ότι το φυσικό πρόσωπο δικαιούται να έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες.

θ) **«Μέρος παραλήπτης»** σημαίνει το Μέρος στο οποίο διαβιβάζονται Διαβαθμισμένες Πληροφορίες από το άλλο Μέρος.

ι) «**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 είναι ισοδύναμα και αντιστοιχούν στα επίπεδα διαβάθμισης ασφαλείας τα οποία ορίζονται από την εθνική τους νομοθεσία:

Για την Κυπριακή Δημοκρατία	Για την Δημοκρατία της Εσθονίας	Αντίστοιχη Αγγλική Ορολογία
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TÄIESTI SALAJANE	TOP SECRET
ΑΠΟΡΡΗΤΟ	SALAJANE	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	KONFIDENTSIAALNE	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	PIIRATUD	RESTRICTED

Άρθρο 4
Αρμόδιες Αρχές

1. Η Εθνικές Αρχές Ασφαλείας των Μερών είναι:

   Για την Κυπριακή Δημοκρατία
   Εθνική Αρχή Ασφαλείας
   Υπουργείο Άμυνας της Κυπριακής Δημοκρατίας

   Για την Δημοκρατία της Εσθονίας
   Department of the National Security Authority
   Ministry of Defence of the Republic of Estonia

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

3. Κατόπιν αιτήματος, οι Εθνικές Αρχές Ασφαλείας θα αλληλοενημερώνονται σχετικά με άλλες Αρμόδιες Αρχές,

4. Οι Εθνικές Αρχές Ασφαλείας 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 για την προστασία Διαβαθμισμένων Πληροφοριών.

Άρθρο 5
Μέτρα Προστασίας και Πρόσβαση σε Διαβαθμισμένες Πληροφορίες

1. Σύμφωνα με την εθνική τους νομοθεσία, τα Μέρη λαμβάνουν όλα τα απαραίτητα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών οι οποίες ανταλλάσσονται ή παράγονται βάσει της παρούσας Συμφωνίας. Τουλάχιστον το ίδιο επίπεδο προστασίας θα καθορίζεται στις Διαβαθμισμένες Πληροφορίες, 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 των βαθμών 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 του αντίστοιχου επιπέδου διαβάθμισης ασφαλείας.

4. Στα πλαίσια της παρούσας Συμφωνίας, κάθε Μέρος αναγνωρίζει την πιστοποίηση του Ελέγχου Ασφαλείας Προσωπικού και Φορέα, που παρέχεται σύμφωνα με την εθνική νομοθεσία του κράτους του άλλου Μέρους. Οι έλεγχοι ασφαλείας θα είναι ισοδύναμοι σύμφωνα με το Άρθρο 3.

5. Οι Αρμόδιες Αρχές Ασφαλείας, θα αλληλοβοηθούνται, σύμφωνα με την εθνική νομοθεσία, στην διεξαγωγή των διαδικασιών ελέγχου ασφαλείας για την εφαρμογή της παρούσας Συμφωνίας.

6. Στα πλαίσια της παρούσας Συμφωνίας, οι Αρμόδιες Αρχές των Μερών αλληλοενημερώνονται χωρίς καθυστέρηση σχετικά με τυχόν αλλαγές των Ελέγχων Ασφαλείας Προσωπικού και Φορέα, και πιο συγκεκριμένα όταν πρόκειται για την απόσυρση 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 πληροφορία σύμφωνα με το Άρθρο 3,

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

Άρθρο 6
Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες διαβιβάζονται μέσω της διπλωματικής οδού, εκτός εάν προβλέπεται διαφορετικά από την Εθνική Αρχή Ασφαλείας. Το Μέρος Παραλήπτης επιβεβαιώνει γραπτώς την λήψη των Διαβαθμισμένων Πληροφοριών.

2. Η ηλεκτρονική διαβίβαση Διαβαθμισμένων Πληροφοριών θα γίνεται μέσω πιστοποιημένων κρυπτογραφικών μέσων τα οποία εγκρίνονται από τις Εθνικές Αρχές Ασφαλείας.

3. Εάν είναι απαραίτητο, οι υπηρεσίες πληροφοριών, ασφαλείας και η αστυνομία των Μερών, δύνανται, σύμφωνα με την εθνική νομοθεσία, να ανταλλάζουν επιχειρησιακές πληροφορίες και πληροφορίες ασφαλείας απευθείας μεταξύ τους.

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 τις ακόλουθες διαδικασίες:

   α) οι μεταφράσεις και οι αναπαραγωγές θα διαβαθμίζονται και προστατεύονται όπως και οι πρωτότυπες Διαβαθμισμένες Πληροφορίες,

   β) οι μεταφράσεις και ο αριθμός των αντιγράφων θα περιορίζονται στον αριθμό που απαιτείται για επίσημους σκοπούς,

   γ) οι μεταφράσεις θα φέρουν κατάλληλη σημείωση στην γλώσσα μετάφρασης, υποδεικνύοντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες που λήφθηκαν από το Μέρος Αποστολέα.

2. Οι Πληροφορίες με διαβάθμιση ΑΠΟΡΡΗΤΟ/SALAJANE και άνω, θα μεταφράζονται ή θα αναπαράγονται μόνο κατόπιν γραπτής συγκατάθεσης του Μέρους Αποστολέα.

Άρθρο 8
Καταστροφή Διαβαθμισμένων Πληροφοριών

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

2. Οι Πληροφορίες με διαβάθμιση ΑΠΟΡΡΗΤΟ/SALAJANE καταστρέφονται σύμφωνα με την εθνική νομοθεσία.

3. Οι Πληροφορίες με διαβάθμιση ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TÄIESTI SALAJANE δεν καταστρέφονται. Επιστρέφονται στην Αρμόδια Αρχή Ασφαλείας 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 Εθνική Αρχή Ασφαλείας κάθε Μέρους το οποίο επιθυμεί να υπογράψει Διαβαθμισμένη Σύμβαση με κάποιον Εργολάβο του άλλου Μέρους, ή επιθυμεί να επιτρέψει σε κάποιον από τους Εργολάβους του να υπογράψει Διαβαθμισμένη Σύμβαση στην επικράτεια του άλλου Μέρους, οφείλει να εξασφαλίσει την εκ των προτέρων γραπτή εγγύηση της Εθνικής Αρχής Ασφαλείας του άλλου Μέρους, ότι ο προτεινόμενος Εργολάβος διαθέτει πιστοποίηση Ελέγχου Ασφαλείας Φορέα του κατάλληλου επιπέδου διαβάθμισης ασφαλείας.

2. Ο Εργολάβος οφείλει να υποβάλει πληροφορίες για πιθανούς υπεργολάβους προς έγκριση από την Εθνική Αρχή Ασφαλείας στην επικράτεια της οποίας πρόκειται να εκτελεστεί το έργο.

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

   α) δέσμευση του Εργολάβου με την οποία διασφαλίζεται ότι οι εγκαταστάσεις του τηρούν τις απαραίτητες προϋποθέσεις για τον χειρισμό και αποθήκευση

Διαβαθμισμένων Πληροφοριών στο συγκεκριμένο επίπεδο διαβάθμισης ασφαλείας,

β) δέσμευση του Εργολάβου με την οποία διασφαλίζεται ότι όλα τα άτομα τα οποία εκτελούν καθήκοντα που απαιτούν πρόσβαση σε Διαβαθμισμένες Πληροφορίες, διαθέτουν το κατάλληλο επίπεδο πιστοποίησης Ελέγχου Ασφαλείας Προσωπικού, σύμφωνα με την εθνική νομοθεσία,

γ) δέσμευση του Εργολάβου με την οποία διασφαλίζεται ότι όλα τα άτομα με πρόσβαση σε Διαβαθμισμένες Πληροφορίες έχουν ενημερωθεί για την ευθύνη τους αναφορικά με την προστασία Διαβαθμισμένων Πληροφοριών, σύμφωνα με την εθνική νομοθεσία,

δ) κατάλογο των Διαβαθμισμένων Πληροφοριών και κατάλογο τομέων στους οποίους ενδέχεται να προκύψουν Διαβαθμισμένες Πληροφορίες,

ε) διαδικασίες για την γνωστοποίηση των αλλαγών στα επίπεδα διαβάθμισης ασφαλείας των Διαβαθμισμένων Πληροφοριών,

στ) μέσα επικοινωνίας και ηλεκτρονικά μέσα διαβίβασης,

ζ) διαδικασίες για την μεταφορά Διαβαθμισμένων Πληροφοριών,

η) δέσμευση του Εργολάβου να ενημερώσει για τυχόν πραγματική ή ενδεχόμενη Παραβίαση Ασφαλείας,

θ) δέσμευση του Εργολάβου να προωθήσει αντίγραφο της Διαβαθμισμένης Σύμβασης στην οικία Αρμόδια Αρχή,

ι) δέσμευση του υπεργολάβου να τηρήσει τις ίδιες υποχρεώσεις ασφαλείας με τον Εργολάβο.

4. Μόλις ξεκινήσουν οι διαπραγματεύσεις της σύμβασης μεταξύ των πιθανών Εργολάβων, η Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα ενημερώνει την Εθνική Αρχή Ασφαλείας του άλλου Μέρους, σχετικά με το επίπεδο διαβάθμισης ασφαλείας που δόθηκε στις Διαβαθμισμένες Πληροφορίες οι οποίες σχετίζονται με τις διαπραγματεύσεις αυτές.

5. Αντίγραφο της κάθε Διαβαθμισμένης Σύμβασης θα προωθηθεί στην Εθνική Αρχή Ασφαλείας του Μέρους όπου πρόκειται να διεξαχθούν οι εργασίες, ώστε να επιτραπεί η κατάλληλη επίβλεψη και έλεγχος ασφαλείας.

Άρθρο 10
Επισκέψεις

1. Οι επισκέψεις που αφορούν σε Διαβαθμισμένες Συμβάσεις και προϋποθέτουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες υπόκεινται στην εκ των προτέρων γραπτή έγκριση που παρέχεται από την Αρμόδια Αρχή 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 την θέση του επισκέπτη στο νομικό πρόσωπο,

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

   δ) επιβεβαίωση του πιστοποιητικού Ελέγχου Ασφαλείας Προσωπικού, της εγκυρότητάς του και του επιπέδου του,

   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 κράτους Μέρους υποδοχής αποστέλλει 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 κατευθείαν 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 Εθνική Αρχή Ασφαλείας του Μέρους Παραλήπτη ενημερώνει την Εθνική Αρχή Ασφαλείας του Μέρους Αποστολέα το συντομότερο δυνατόν και ξεκινά την κατάλληλη έρευνα.

2. Εάν η παραβίαση ασφαλείας γίνει σε Τρίτη χώρα, η Εθνική Αρχή Ασφαλείας του Μέρους διανομής θα λάβει 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 τελική έκθεση για τους λόγους και την έκταση της ζημιάς.

Άρθρο 12
Έξοδα

Κάθε Μέρος αναλαμβάνει τα δικά του έξοδα τα οποία θα προκύψουν από την εφαρμογή και επίβλεψη 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.

Άρθρο 14
Τελικές Διατάξεις

1. Η συμφωνία αυτή 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 Συμφωνία αυτή δύναται να τροποποιείται από καιρό σε καιρό βάσει κοινής γραπτής έγκρισης των Μερών. Οι τροποποιήσεις τίθενται σε ισχύ σύμφωνα με την Παράγραφο 1.

3. Κάθε Μέρος δύναται, ανά πάσα στιγμή, να τερματίσει την 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 τον τερματισμό της παρούσας Συμφωνίας, τα Μέρη θα διασφαλίσουν 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 2012 σε δύο πρωτότυπα σετ αντιγράφων, στην ελληνική, εσθονική 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

ΔΗΜΗΤΡΗΣ ΗΛΙΑΔΗΣ

ΥΠΟΥΡΓΟΣ ΑΜΥΝΑΣ

Για την Κυβέρνηση της

Δημοκρατίας της Εσθονίας

MÄRT KRAFT

ΔΙΕΥΘΥΝΤΗΣ ΕΘΝΙΚΗΣ ΑΡΧΗΣ ΑΣΦΑΛΕΙΑΣ

Μέρος III

Küprose Vabariigi valitsuse ja Eesti Vabariigi valitsuse salastatud teabe vastastikuse kaitse kokkulepe

Küprose Vabariigi valitsus ja Eesti Vabariigi valitsus (edaspidi „pooled"),

tunnustades vajadust kehtestada reeglid vastastikku poliitilise, sõjalise, majandusliku, õigusalase, teadusliku ja tehnoloogilise või muu koostöö raames vahetatava ja selle käigus tekkiva salastatud teabe kaitseks,

kavatsedes tagada vastastikuse kaitse kogu salastatud teabele, mis on koostatud või salastatud ühe poole riigis ja edastatud teise poole riigile, või tekkinud pooltevahelise koostöö käigus,

soovides kehtestada pooltevahelise salastatud teabe vastastikuse kaitse korda,

võttes arvesse kummagi poole huve salastatud teabe kaitsmisel ja võttes arvesse poolte õigusakte,

on kokku leppinud järgmises:

Artikkel 1
Eesmärk

Kokkuleppe eesmärk on tagada ühiselt loodud või poolte vahel vahetatud salastatud teabe kaitse.

Artikkel 2
Mõisted

Kokkuleppes kasutatakse järgmisi mõisteid:

a) **salastatud teabe kaitse nõuete rikkumine** – mis tahes tegevus või tegevusetus, mis on vastuolus käesoleva kokkuleppe või poolte riigisiseste õigusaktidega, mille tagajärjeks võib olla salastatud teabe avalikustamine, kadumine, hävimine, omastamine või selle muul moel ohtu seadmine;

b) **salastatud leping** – kokkulepe kahe või enama poole vahel, mis sisaldab salastatud teavet või mille täitmiseks on vajalik juurdepääs salastatud teabele;

c) **salastatud teave** – mis tahes vormis või laadi teave, mida tuleb kummagi poole õigusaktide kohaselt kaitsta omavolilise tegevuse eest ning mis on salastatud ja mille salastatuse tase on asjaomaselt märgistatud;

d) **pädev asutus** – riigi julgeoleku volitatud esindaja või mis tahes muu riigiasutus, kes riigi õigusaktide kohaselt vastutab kokkuleppe rakendamise eest;

e) **lepinglane** – füüsiline või juriidiline isik, kellel on õigus sõlmida salastatud lepinguid;

f) **töötlemisluba** – pädeva asutuse otsus, mille kohaselt on juriidiline või füüsiline isik reaalselt ja korralduslikult suuteline täitma tingimused, mis on vajalikud salastatud teabe ohutuks töötlemiseks ja valdamiseks vastavalt riigi õigusaktidele;

g) **riigi julgeoleku volitatud esindaja** – kummagi poole riigiasutus, kes poole riigisiseste õigusaktide kohaselt vastutab kokkuleppe üldise rakendamise ja järelevalve eest; poolte vastavad asutused on nimetatud käesoleva kokkuleppe artikli 4 lõikes 1.

h) **teadmisvajadus** – vajadus pääseda juurde teatud salastatud teabele teenistuskohustuste tõttu ja teatava ülesande täitmiseks;

i) **päritolupool** – pool, kes on loonud salastatud teabe;

j) **juurdepääsuluba** – pädeva asutuse otsus, mille alusel on füüsilisel isikul lubatud riigi õigusaktide kohaselt pääseda juurde salastatud teabele;

k) **vastuvõttev pool** – pool, kellele edastatakse päritolupoole salastatud teavet;

l) **kolmas isik** – riik, organisatsioon või juriidiline või füüsiline isik, kes ei ole selle kokkuleppe pool.

Artikkel 3
Salastatuse tasemed

Pooled lepivad kokku, et järgmised salastatuse tasemed on samaväärsed ja vastavad asjakohaste riikide õigusaktides sätestatud salastatuse tasemetele.

Küprose Vabariigis	Eesti Vabariigis	Inglise keeles
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TÄIESTI SALAJANE	TOP SECRET
ΑΠΟΡΡΗΤΟ	SALAJANE	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	KONFIDENTSIAALNE	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	PIIRATUD	RESTRICTED

Artikkel 4
Pädevad asutused

1. Poolte riigi julgeoleku volitatud esindajad on järgmised:

   Küprose Vabariigis:
   Riigi julgeoleku volitatud esindaja
   Küprose Vabariigi Kaitseministeerium

   Eesti Vabariigis:
   Riigi julgeoleku volitatud esindaja osakond
   Eesti Vabariigi Kaitseministeerium

2. Pooled teavitavad teineteist diplomaatiliste kanalite kaudu riigi julgeoleku volitatud esindaja muutmisest.

3. Riigi julgeoleku volitatud esindajad teavitavad teineteist taotluse korral muudest pädevatest asutustest.

4. Riigi julgeoleku volitatud esindajad teavitavad teineteist kehtivatest riigi õigusaktidest, mis reguleerivad salastatud teabe kaitset, ja nendesse tehtavatest olulistest muudatustest ning annavad teineteisele teavet oma salastatud teabe kaitse nõuete, korra ja tavade kohta.

Artikkel 5
Kaitsemeetmed ja juurdepääs salastatud teabele

1. Pooled võtavad kooskõlas oma riigi õigusaktidega meetmeid, et kaitsta käesoleva kokkuleppe alusel vahetatud või loodud salastatud teavet. Sellisele salastatud teabele tagatakse vähemalt samasugune kaitse nagu oma teabele, mis on salastatud kokkuleppe artiklis 3 määratud samaväärsel tasemel.

2. Päritolupool teavitab vastuvõtvat poolt edastatud salastatud teabe salastatuse taseme muutustest kirjalikult.

3. Salastatud teabele antakse juurdepääs üksnes isikule, kellel on riigi õigusaktide kohaselt juurdepääs asjakohase salastatuse tasemega teabele ja kellel on teadmisvajadus.

4. Kokkuleppe raames tunnustavad pooled teise poole riigisiseste õigusaktide kohaselt väljastatud juurdepääsulube ja töötlemislube. Vastavalt artiklile 3 on load samaväärsed.

5. Kokkuleppe rakendamiseks vajaliku julgeolekukontrolli läbiviimisel abistavad pädevad asutused teineteist taotluse korral ja kooskõlas riigi õigusaktidega.

6. Kokkuleppe raames teavitavad poolte pädevad asutused teineteist viivitamata juurdepääsuloa ja töötlemisloa muutmisest, eeskätt loa tühistamisest või selles ettenähtud salastatuse taseme langetamisest.

7. Vastuvõttev pool:

   a) edastab salastatud teavet kolmandale isikule ainult päritolupoole eelneval kirjalikul nõusolekul;

   b) märgistab salastatud teabe artiklis 3 määratud salastatuse tasemete vastavuse kohaselt;

   c) kasutab salastatud teavet ainult sel eesmärgil, milleks see on antud.

Artikkel 6
Salastatud teabe edastamine

1. Salastatud teavet edastatakse diplomaatiliste kanalite kaudu, kui riigi julgeoleku volitatud esindajad ei ole kokku leppinud teisiti. Vastuvõttev pool kinnitab salastatud teabe kättesaamist kirjalikult.

2. Elektroonilist salastatud teavet edastatakse riigi julgeoleku volitatud esindajate poolt kokku lepitud volitatud krüpteeritud kanalite kaudu.

3. Vajadusel võivad poolte luure-, julgeoleku- ja politseiasutused kooskõlas riigi õigusaktidega vahetada operatiiv- või luureteavet omavahel otse.

Artikkel 7
Salastatud teabe paljundamine ja tõlkimine

1. Salastatud teavet paljundatakse ja tõlgitakse vastavalt vastuvõtva poole õigusaktidele ja järgmise korra kohaselt:
   a) salastatud teabe paljundusi ja tõlkeid märgistatakse ja kaitstakse samaselt algse salastatud teabega;
   b) tõlgete ja paljunduste arv piirdub ametlikuks otstarbeks nõutavaga;
   c) tõlkele tehakse asjakohane sihtkeelne märge selle kohta, et tõlge sisaldab päritolupoole salastatud teavet.

2. Tasemel ΑΠΟΡΡΗΤΟ/SALAJANE või sellest kõrgemal tasemel salastatud teavet võib paljundada ja tõlkida üksnes päritolupoole eelneval kirjalikul loal.

Artikkel 8
Salastatud teabe hävitamine

1. Salastatud teave hävitatakse viisil, mis ei võimalda seda ei osaliselt ega täielikult taastada.

2. Tasemeni ΑΠΟΡΡΗΤΟ/SALAJANE/ märgitud salastatud teave hävitatakse vastavalt poolte õigusaktidele.

3. Tasemel ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/TÄIESTI SALAJANE salastatud teavet ei hävitata. See tagastatakse päritolupoole riigi pädevale asutusele.

4. Salastatud teabe hävitamise kohta koostatakse aruanne ning selle ingliskeelne tõlge esitatakse päritolupoole pädevale asutusele.

5. Kriisiolukorras, kui salastatud teavet ei ole võimalik kaitsta ega tagastada, hävitatakse salastatud teave otsekohe. Vastuvõttev pool teavitab päritolupoole riigi julgeoleku volitatud esindajat salastatud teabe hävitamisest võimalikult kiiresti.

Artikkel 9
Salastatud lepingud

1. Kui pool soovib sõlmida või volitab oma lepinglast sõlmima salastatud lepingut teise poole lepinglasega teise poole territooriumil, küsib selle poole riigi julgeoleku volitatud esindaja teise poole riigi julgeoleku volitatud esindajalt eelnevalt kirjaliku kinnituse, et pakutud lepinglasel on asjakohase salastatuse tasemega teabe töötlemisluba.

2. Lepinglane esitab teabe potentsiaalsete all-lepinglaste kohta selle riigi julgeoleku volitatud esindajale, mille territooriumil töö teostatakse.

3. Kokkuleppe alusel sõlmitud salajase teabe lepingud peavad sisaldama järgmist:

   a) lepinglase kohustust tagada, et tema ruumides on sobivad tingimused asjaomase salastatuse tasemega salastatud teabe töötlemiseks ja valdamiseks;

   b) lepinglase kohustust tagada, et isikutel, kellele tööülesanded eeldavad juurdepääsu salastatud teabele, on riigi õigusaktide kohaselt asjakohase salastatuse tasemega teabele juurdepääs;

   c) lepinglase kohustust tagada, et kõiki salajasele teabele juurde pääsevaid isikuid on teavitatud nende kohustusest salastatud teavet riigi õigusaktide kohaselt kaitsta;

   d) salastatud teabe loetelu ja valdkondade loetelu, kus salastatud teave võib tekkida;

   e) salastatud teabe salastatuse tasemetega seotud muudatustest teavitamise korda;

   f) suhtluskanaleid ja elektroonilisi teabeedastusvahendeid;

   g) salastatud teabe edastamise korda;

   h) lepinglase kohustust teavitada reaalsest või potentsiaalsest salastatud teabe kaitse nõuete rikkumisest;

   i) lepinglase kohustust edastada salastatud lepingu koopia oma riigi pädevale asutusele;

   j) all-lepinglase kohustust täita lepinglasega samu turvakohustusi.

4. Kohe pärast potentsiaalsete lepinglaste lepingueelsete läbirääkimiste algust teavitab päritolupoole riigi julgeoleku volitatud esindaja teise poole riigi julgeoleku volitatud esindajat vastavate lepingueelsete läbirääkimistega seotud salastatud teabe salastatuse tasemest.

5. Salastatud lepingu koopia edastatakse nõuetekohaseks järelevalveks ja kontrolliks tööde asukohariigi riigi julgeoleku volitatud esindajale.

Artikkel 10
Külastused

1. Salastatud lepinguga seotud külastused, millega kaasneb juurdepääs salastatud teabele, toimuvad vastuvõtva poole pädeva asutuse eelneva kirjaliku loa alusel.

2. Külastustaotlus esitatakse vastuvõtva poole pädevale asutusele hiljemalt kümme päeva enne külastust.

3. Pakilise loomuga juhtude korral tohib külastustaotluse esitada lühema etteteatamisajaga.

4. Külastustaotlus sisaldab järgmist:

   a) külastaja ees- ja perekonnanimi, sünniaeg ja -koht, kodakondsus ja isikutunnistuse/passi number;

   b) külastaja ametikoht ja selle üksuse nimetus, keda ta esindab;

   c) külastatava üksuse nimetus, aadress ja kontaktandmed;

   d) külastaja juurdepääsuloa kinnitus, kehtivus ja tase;

   e) külastuse ese ja eesmärk;

f) külastuse eeldatavad kuupäevad ja kestus; korduvkülastuste puhul kogu periood, mida külastused hõlmavad;

g) pädeva asutuse ametlik pitser, allkiri ja kuupäev.

5. Külastusloa andmisel esitab vastuvõtva poole pädev asutus külastatava üksuse turvaametnikele külastustaotluse koopia.

6. Külastusloa kehtivus ei ole pikem kui üks aasta.

7. Poolte pädevad asutused võivad leppida kokku korduvkülastuse õigusega isikute nimekirjas. Nimekiri kehtib esialgu kaksteist kuud. Vastavate külastuste üksikasjad lepivad külastavad isikud kokkulepitud tingimuste alusel otse kokku külastatavate üksuste esindajatega.

Artikkel 11
Salastatud teabe kaitse nõuete rikkumine

1. Salastatud teabe kaitse nõuete rikkumise korral teavitab selle poole riigi julgeoleku volitatud esindaja, kus nõudeid rikuti, päritolupoole riigi julgeoleku volitatud esindajat võimalikult kiiresti ja algatab asjaomase menetluse.

2. Kui salastatud teabe kaitse nõudeid on rikutud kolmandas riigis, võtab teavet edastava poole riigi julgeoleku volitatud esindaja kõik meetmed, et tagada lõikes 1 sätestatud sammude astumine.

3. Päritolupool teeb vastavalt lõikele 1 taotluse korral uurimise läbiviimisel koostööd.

4. Päritolupoolele teatatakse uurimise tulemustest ning edastatakse lõpparuanne juhtunu põhjuste ja kahju ulatuse kohta.

Artikkel 12
Kulud

Kumbki pool kannab kokkuleppe täitmisega seotud oma kulud.

Artikkel 13
Vaidluste lahendamine

Käesoleva kokkuleppe tõlgendamise või kohaldamisega seotud vaidlused lahendatakse poolte läbirääkimiste käigus.

Artikkel 14
Lõppsätted

1. Kokkulepe on sõlmitud määramata ajaks ja see jõustub järgmise kuu esimesel päeval pärast seda, kui poolte diplomaatiliste kanalite kaudu laekub viimane kirjalik teade selle kohta, et nende riigisisestes õigusaktides kokkuleppe jõustumiseks ettenähtud nõuded on täidetud.

2. Poolte kirjalikul nõusolekul võib kokkulepet igal ajal muuta. Muudatused jõustuvad lõike 1 kohaselt.

3. Kummalgi poolel on õigus kokkulepe igal ajal lõpetada diplomaatiliste kanalite kaudu esitatud kirjaliku teatega. Sellisel juhul lõpeb kokkulepe teiselt poolelt lõpetamisteate kättesaamisest arvates kuue kuu pärast.

4. Olenemata kokkuleppe lõppemisest tagavad pooled kokkuleppe raames edastatud salastatud teabe jätkuva kaitsmise senikaua, kuni päritolupool vabastab vastuvõtva poole sellest kohustusest.

Koostatud Nicosias 27. novembril 2012 kahes eksemplaris kreeka, eesti ja inglise keeles; kõik tekstid on võrdselt autentsed. Tõlgenduserinevuste korral lähtutakse ingliskeelsest tekstist.

Küprose Vabariigi valitsus

.....

Demetris Eliades

Kaitseminister

Eesti Vabariigi valitsus

.....

Märt Kraft

Riigi julgeoleku volitatud esindaja juht