Ε.Ε. Παρ. Ι(ΙΙΙ) **Ν. 16(ΙΙΙ)/2014**
Αρ. 4196, 25.7.2014

Ο περί της Συμφωνίας μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Σλοβενίας για την Ανταλλαγή και την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2014 εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος.

Αριθμός 16(ΙΙΙ) του 2014

ΝΟΜΟΣ ΠΟΥ ΚΥΡΩΝΕΙ ΤΗ ΣΥΜΦΩΝΙΑ ΜΕΤΑΞΥ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΚΑΙ ΤΗΣ ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΣΛΟΒΕΝΙΑΣ ΓΙΑ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΚΑΙ 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 Σλοβενίας για την Ανταλλαγή και την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών (Κυρωτικός) Νόμος του 2014.

Ερμηνεία.

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

"Συμφωνία" σημαίνει τη Συμφωνία μεταξύ της μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Σλοβενίας για την Ανταλλαγή και την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών, η διαπραγμάτευση της οποίας έγινε κατόπιν της Απόφασης του Υπουργικού Συμβουλίου με Αριθμό 2/2009 και ημερομηνία 20 Μαΐου 2009 και η οποία υπογράφηκε στις 19 Φεβρουαρίου 2014, κατόπιν της Απόφασης του Υπουργικού Συμβουλίου με Αριθμό 75.445 και ημερομηνία 10 Ιουλίου 2013.

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 στη Σλοβενική γλώσσα στο Μέρος ΙΙΙ του Πίνακα.

ΠΙΝΑΚΑΣ
(Άρθρο 3)

Μέρος Ι
(Αγγλική γλώσσα)

AGREEMENT

Between the Government of the Republic of Cyprus and the Government of the Republic of Slovenia on the Exchange and Mutual Protection of Classified Information

The Government of the Republic of Cyprus and the Government of the Republic of Slovenia hereinafter referred to as ´´the Parties´´;

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

Realizing that good cooperation may require the exchange of Classified Information between the Parties;

Have agreed as follows:

Article 1

Definitions

For the purposes of this Agreement these terms shall mean the following:

1. ´´ Recipient´´ - the Competent Authority receiving the Classified Information;

2. ´´Competent Authority´´ - public or private entity under jurisdiction of any Party authorized to handle and store Classified Information in accordance with the national legislation of its Party, including the Competent Security Authority;

3. ´´Competent Security Authority´´ - state authority, designated by the Party as responsible for the general implementation and the relevant controls of all aspects of this Agreement as referred to in Article 3 Paragraph 1;

4. ´´Contractor´´ - an individual, a legal entity or an organizational unit, which has the capacity to conclude contracts;

5. ´´Classified Contract´´ - a contract or a subcontract, which requires access to Classified Information;

6. ´´Classified Information´´ - any information, regardless of its form, which is transmitted or generated between the Parties or Competent Authorities and requires, under the national legislation of either Party, the protection against unauthorized disclosure or other compromise and is designated as such and marked appropriately by a Party;

7. "Facility Security Clearance" - A determination following an investigative procedure certifying that a contractor which is a legal entity fulfils the conditions of handling Classified Information in accordance with the national legislation of one of the Parties;

8. "Need-to-know" - a principle by which access to specific Classified Information may be granted to an individual only in connection with his/her official duties or for the performance of a specific task;

9. "Personnel Security Clearance" - A determination following an investigative procedure in accordance with the national legislation, on the basis of which an individual is authorised to have access to and to handle Classified Information up to the level defined in the clearance;

10. ''Principal'' - a governmental body, which intends to conclude or concludes a Classified Contract in the territory of the other Party;

11. "Third Party" - a state, including any public or private entity or individual under its jurisdiction, or an international organization which is not a Party to this Agreement.

Article 2

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:

Republic of Cyprus	Republic of Slovenia	English Equivalent
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STROGO TAJNO	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ZAUPNO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	INTERNO	RESTRICTED

Article 3

Competent Security Authorities

1. For the purposes of this Agreement, the Competent Security Authorities shall be:

   a. for the Republic of Cyprus: National Security Authority (Ministry of Defence);

   b. for the Republic of Slovenia: National Security Authority (Government Office for the Protection of Classified Information).

2. The Competent Security Authorities may conclude implementation agreements for the purposes of the implementation of the provisions hereof.

3. The Parties shall inform each other through diplomatic channels of any subsequent changes of the National Security Authorities.

Article 4

Principles of Classified Information Protection

1. In accordance with this Agreement and their national legislation, the Parties shall adopt appropriate measures aimed at the protection of Classified Information.

2. The Parties shall provide for the information referred to in paragraph 1 at least the same protection as applicable to their own Classified Information under the relevant security classification level, pursuant to Article 2.

3. The National Security Authorities designated by the Parties are responsible for the general implementation and the relevant controls of all aspects of this Agreement.

4. Received Classified Information shall be accessible only to those persons who have a need-to-know, who have been security cleared and/or who have been authorized to have access to such information as well as briefed in the scope of Classified Information protection according to the national legislation of their Party.

5. Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and where applicable, non-repudiation and authenticity of Classified Information as well as an appropriate level of accountability and traceability of actions in relation to that information.

6. The security classification level shall be changed or removed only by the Competent Authority, which has granted it. The Recipient shall be immediately notified on every change or removal of security classification level.

7. The Parties shall mutually recognise their respective Personnel and Facility Security Clearances. To this effect, Article 2 regarding the security classification levels shall apply accordingly.

Article 5

Restriction of use of classified information

1. Received Classified Information shall be used exclusively for the purposes and under conditions of release or limitations on the use of the Classified Information, defined at the transmission thereof.

2. Either Party shall not release Classified Information to Third Party without a prior written consent of the Competent Security Authority of the other Party, which granted adequate security classification level.

Article 6

Classified Contracts

1. The Principal may conclude a Classified Contract with the Contractor of the other Party.

2. In the case referred to in Paragraph 1, the Principal shall submit a request to the Competent Security Authority of its Party to ask the Competent Security Authority of the other Party for issuing a written assurance that the Contractor is authorized to have access to Classified Information of the specified security classification level.

3. The issuing of the assurance referred to in Paragraph 2 shall guarantee that the Contractor fulfils the criteria in the scope of the protection of Classified Information, as provided in the applicable national legislation of the Party, in the territory of which the Contractor is located..

4. If the Contractor has not been previously authorized to have access to Classified Information of the specified security classification level, the Competent Security Authority which

is to issue the assurance, shall immediately notify the Competent Security Authority of the other Party, that upon its request, the actions referred to in Paragraph 3 will be undertaken.

5. Classified Information shall not be accessible to the Contractor until the receipt of the assurance referred to in Paragraphs 2 and 3.

6. The Principal shall notify the Contractor of the security requirements necessary to perform the Classified Contract, which include in particular a list of Classified Information and rules of classification of the information originated during the performance of the Classified Contract. The copy of such documents shall be transmitted to the Competent Security Authority.

7. The Competent Security Authority of the Party in whose territory the Classified Contract is to be performed shall ensure that the Contractor protects Classified Information in accordance with the received security requirements and national legislation of its Party.

8. The Competent Security Authorities shall ensure that any possible subcontractors shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted through diplomatic channels or through other secured channels ensuring protection against unauthorized disclosure, agreed upon between the Competent Security Authorities. The Recipient shall confirm the receipt of Classified Information in writing.

2. Information classified as ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/INTERNO/RESTRICTED may be transmitted also by post or another delivery service in accordance with the national legislation.

Article 8

Reproduction and Translation of Classified Information

1. Information classified as ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/STROGO TAJNO/TOP SECRET shall be reproduced only after a prior written permission issued by the Competent Authority of the party which classified this information.

2. Reproduction of Classified Information shall be pursuant to the national legislation of each of the Parties. Reproduced information shall be placed under the same protection as the originals. Number of copies shall be reduced to minimum required for official purposes.

3. Any translation of Classified Information shall be made by properly security cleared individuals. All translations shall bear an appropriate note in the language into which they have been translated, stating that they contain Classified Information of the other Party. The translation shall be placed under the same protection as the originals.

Article 9

Destruction of Classified Information

1. Classified Information shall be destroyed according to the national legislation of the Parties, in such a manner as to eliminate the partial or total reconstruction of the same.

2. Classified Information marked as АКРΩΣ АПОРРНТО/STROGO TAJNO/TOP SECRET shall not be destroyed. It shall be returned to the Competent Authority of the party which classified this information.

3. In case of a crisis situation, in which it is impossible to protect or return Classified Information such information shall be destroyed immediately. The Recipient shall inform the Competent Security Authority of the other Party about this destruction as soon as possible.

Article 10

Visits

1. Visits necessitating access to Classified Information shall be subject to prior permission of the Competent Security Authority of the host Party.

2. The permission referred to in Paragraph 1 shall be granted exclusively to the persons authorized to have access to Classified Information pursuant to the national legislation of the Party designating such a person.

3. A request for visit shall be submitted to the relevant National Security Authority at least 20 days prior to the commencement of the visit. The request for the visit shall include the following data that shall be used for the purpose of the visit only:

a. purpose, date and program of the visit including the highest security classification level of Classified Information to be involved

b. name and surname of the visitor, date and place of birth, citizenship, passport number or identity card number;

c. position of the visitor together with the name of the institution or organization which he or she represents;

d. the validity and certification of the level of Personnel Security Clearance held by the visitor;

e. name and address of the organization to be visited;

f. name, surname, contact data and position of the person to be visited;

g. the date and signature of the Competent Security Authority.

4. The Competent Authorities shall ensure the protection of the personal data of the visitor pursuant to their national legislation.

5. Classified Information accessible during the visit shall be protected pursuant to the provisions of this Agreement.

Article 11

Breach of Security

1. In case of Breach of Security, resulting in unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a breach, the Competent Security Authority of the Recipient shall inform the Competent Security Authority of the other Party, as soon as possible, and initiate the appropriate investigation.

2. If a breach of security arises in a Third Party, the Competent Security Authority of the Party which has provided the information to the Third Party shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 are initiated.

3. The Competent Security Authority of the Party which provided such information shall, upon request, cooperate in the investigation in accordance with Paragraph 1. It 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 cover its own expenses resulting from the implementation of this Agreement.

Article 13

Consultation

1. The Competent Security Authorities of the Parties shall notify each other of any amendments to their national legislation concerning the protection of Classified Information.

2. The Competent Security Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions hereof.

3. Competent Security Authorities of the Parties shall exchange visits to discuss the procedures and standards for the protection of Classified Information.

4. The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized Personnel and Facility Security Clearances.

5. Upon request, the Competent Security Authorities shall assist each other in carrying out security clearance procedures.

Article 14

Settlement of Disputes

1. Any disputes concerning the interpretation or application of this Agreement shall be settled by direct negotiations and/or consultations between the Competent Security Authorities of the Parties.

2. If the settlement of a dispute can not be reached in the manner referred to in Paragraph 1, such a dispute shall be settled through diplomatic channels.

Article 15

Final Provisions

1. This Agreement shall enter into force on the first day of the second month following the date on which the Parties notify each other, through diplomatic channels, that all necessary internal procedures for the entry into force of this Agreement have been completed.

2. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party upon giving a written notice to the other Party. In such a case this Agreement shall expire six months after the date of the termination notice.

3. In case of termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

4. This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1.

Done at Ljubljana on 19 February 2014 in two originals, each in Greek, Slovenian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF CYPRUS

FOR THE GOVERNMENT OF THE REPUBLIC OF SLOVENIA

Μέρος ΙΙ
(Ελληνική γλώσσα)

Συμφωνία
Μεταξύ της Κυβέρνησης της Κυπριακής Δημοκρατίας και της Κυβέρνησης της Δημοκρατίας της Σλοβενίας για την Ανταλλαγή και την Αμοιβαία Προστασία Διαβαθμισμένων Πληροφοριών

Η Κυβέρνηση της Κυπριακής Δημοκρατίας και η Κυβέρνηση της Δημοκρατίας της Σλοβενίας αποκαλούμενες στο εξής τα «Μέρη»,

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

Συνειδητοποιώντας ότι η καλή συνεργασία δύναται να απαιτεί την ανταλλαγή Διαβαθμισμένων Πληροφοριών μεταξύ των Μερών,

Συμφώνησαν στα ακόλουθα:

Άρθρο 1
Ερμηνεία

Για τους σκοπούς της παρούσας Συμφωνίας οι όροι αυτοί θα έχουν την ακόλουθη ερμηνεία:

1. «Παραλήπτης» - την Αρμόδια Αρχή που λαμβάνει Διαβαθμισμένες Πληροφορίες,

2. «Αρμόδια Αρχή» - τον δημόσιο ή ιδιωτικό φορέα που υπάγεται στη δικαιοδοσία του οποιουδήποτε Μέρους που έχει εξουσιοδοτηθεί να χειρίζεται και να αποθηκεύει Διαβαθμισμένες Πληροφορίες σύμφωνα με την εθνική νομοθεσία του Μέρους αυτού, περιλαμβανομένων και των Αρμόδιων Αρχών Ασφαλείας,

3. «Αρμόδια Αρχή Ασφαλείας» - την κρατική αρχή, η οποία έχει υποδειχθεί από το Μέρος ως υπεύθυνη για την γενική εφαρμογή και τους σχετικούς ελέγχους όλων των πτυχών της παρούσας Συμφωνίας, όπως αναφέρεται στο Άρθρο 3 Παράγραφος 1,

4. «Συμβαλλόμενος» - το φυσικό πρόσωπο, τη νομική οντότητα ή οργανωτική μονάδα, που έχει την ικανότητα να συνάπτει συμφωνίες,

5. «Διαβαθμισμένη Σύμβαση» - τη σύμβαση ή τη σύμβαση με υποσυμβαλλόμενο, η οποία απαιτεί πρόσβαση σε Διαβαθμισμένες Πληροφορίες,

6. «Διαβαθμισμένες Πληροφορίες» - οποιεσδήποτε πληροφορίες, ανεξάρτητα από τη μορφή τους, οι οποίες μεταδίδονται ή παράγονται μεταξύ των Μερών ή των Αρμόδιων Αρχών

και οι οποίες, σύμφωνα με την εθνική νομοθεσία έκαστου Μέρους, χρήζουν προστασίας από μη εξουσιοδοτημένη αποκάλυψη ή άλλο κίνδυνο και έχει ορισθεί ως τέτοια και επισημανθεί κατάλληλα από το Μέρος,

7. «Έλεγχος Διαβάθμισης Ασφαλείας» - το θετικό αποτέλεσμα μίας έρευνας η οποία βεβαιώνει ότι ο συμβαλλόμενος, ο οποίος είναι νομικό πρόσωπο, πληροί τις προϋποθέσεις για τον χειρισμό Διαβαθμισμένων Πληροφοριών σύμφωνα με την εθνική νομοθεσία των Μερών,

8. «Αρχή της «Ανάγκης για γνώση» - την αρχή με την οποία η πρόσβαση σε συγκεκριμένες Διαβαθμισμένες Πληροφορίες μπορεί να χορηγηθεί σε άτομο μόνο σε σχέση με τα επίσημα καθήκοντα του/της ή κατά την εκτέλεση συγκεκριμένης εργασίας,

9. «Διαβάθμιση Ασφαλείας Προσωπικού» - το θετικό αποτέλεσμα μίας έρευνας σύμφωνα με την εσωτερική νομοθεσία σύμφωνα με την οποία άτομα έχουν εξουσιοδοτηθεί να έχουν πρόσβαση και να χειρισθούν Διαβαθμισμένες Πληροφορίες μέχρι το συγκεκριμένο επίπεδο που αναφέρεται στη διαβάθμιση ασφαλείας,

10. «Εντολέας» - κυβερνητικό σώμα, το οποίο προτίθεται να συνάψει ή συνάπτει Διαβαθμισμένη Σύμβαση στην επικράτεια του άλλου Μέρους,

11. «Τρίτο Πρόσωπο» - κράτος, συμπεριλαμβανομένου δημόσιου ή ιδιωτικού φορέα ή άτομο που υπάγεται στη δικαιοδοσία του, ή διεθνής οργανισμός που δεν είναι Μέρος της παρούσας Συμφωνίας.

Άρθρο 2
Επισημάνσεις Διαβάθμισης Ασφαλείας

Τα Μέρη συμφωνούν όπως οι ακόλουθες επισημάνσεις διαβάθμισης ασφαλείας είναι ισοδύναμες και αντίστοιχες με τις επισημάνσεις διαβάθμισης ασφαλείας που προσδιορίζονται στην εθνική τους νομοθεσία :

Κυπριακή Δημοκρατία	Δημοκρατία της Σλοβενίας	Αγγλικό ισοδύναμο
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STROGO TAJNO	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ZAUPNO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	INTERNO	RESTRICTED

Άρθρο 3
Αρμόδιες Αρχές Ασφαλείας

1. Για σκοπούς της παρούσας Συμφωνίας, οι Αρμόδιες Αρχές Ασφαλείας θα είναι οι ακόλουθες:

α. Για την Κυπριακή Δημοκρατία: η Εθνική Αρχή Ασφαλείας (Υπουργείο Άμυνας),

β. Για τη Δημοκρατία της Σλοβενίας: η Εθνική Αρχή Ασφαλείας (Κυβερνητικό Γραφείο για την Προστασία Διαβαθμισμένων Πληροφοριών)

2. Οι Αρμόδιες Αρχές Ασφαλείας δύνανται να συνάπτουν συμφωνίες εφαρμογής για την εφαρμογή των προνοιών της παρούσας Συμφωνίας.

3. Τα Μέρη ενημερώνονται αμοιβαία μέσω της διπλωματικής οδού για οποιεσδήποτε αλλαγές στις Εθνικές Αρχές Ασφαλείας.

Άρθρο 4
Αρχές Προστασίας Διαβαθμισμένων Πληροφοριών

1. Σύμφωνα με την παρούσα Συμφωνία και την εθνική νομοθεσία έκαστων των Μερών, τα Μέρη θα υιοθετήσουν τα κατάλληλα μέτρα για την προστασία των Διαβαθμισμένων Πληροφοριών.

2. Τα Μέρη θα διασφαλίσουν ότι οι πληροφορίες που αναφέρονται στην παράγραφο 1 διατηρούν την ίδια προστασία που έχει εφαρμόσει έκαστο των Μερών για τις δικές του Διαβαθμισμένες Πληροφορίες δυνάμει της σχετικής διαβάθμισης ασφαλείας, σύμφωνα με το Άρθρο 2.

3. Οι Εθνικές Αρχές Ασφαλείας που έχουν υποδειχθεί από τα Μέρη είναι υπεύθυνα για την γενική εφαρμογή και τους σχετικούς ελέγχους όλων των πτυχών της παρούσας Συμφωνίας.

4. Πρόσβαση στις Διαβαθμισμένες Πληροφορίες που έχουν ληφθεί θα έχουν μόνο τα πρόσωπα που έχουν ανάγκη για γνώση, που έχουν ελεγχθεί καταλλήλως και τα οποία έχουν εξουσιοδοτηθεί να έχουν πρόσβαση σε τέτοιες πληροφορίες και έχουν ενημερωθεί εντός του πλαισίου για την προστασία Διαβαθμισμένων Πληροφοριών σύμφωνα με την εθνική νομοθεσία έκαστου Μέρους.

5. Έκαστο των μερών θα διασφαλίζει ότι εφαρμόζονται κατάλληλα μέτρα για την προστασία Διαβαθμισμένων Πληροφοριών που επεξεργάζονται, αποθηκεύονται ή διαβιβάζονται σε συστήματα επικοινωνιών και πληροφοριών. Τέτοια μέτρα θα διασφαλίζουν την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, και όπου εφαρμόζεται, την μη αμφισβήτηση και αυθεντικότητα των Διαβαθμισμένων Πληροφοριών καθώς και κατάλληλο επίπεδο ευθύνης και ανίχνευσης ενεργειών σε σχέση με τις εν λόγω πληροφορίες.

6. Οι επισημάνσεις διαβάθμισης ασφαλείας θα αλλάζουν ή αφαιρούνται μόνο από την Αρμόδια Αρχή, η οποία την έχει χορηγήσει. Ο Παραλήπτης θα ενημερώνεται άμεσα για κάθε αλλαγή ή αφαίρεση οποιασδήποτε επισήμανσης διαβάθμισης ασφαλείας.

7. Τα Μέρη αναγνωρίζουν τους αντίστοιχους Ελέγχους Διαβάθμισης Ασφαλείας και Διαβάθμισης Ασφαλείας Προσωπικού. Για το σκοπό αυτό, το Άρθρο 2 αναφορικά με τις επισημάνσεις διαβάθμισης ασφαλείας εφαρμόζεται ανάλογα.

Άρθρο 5
Περιοριστική χρήση διαβαθμισμένων πληροφοριών

1. Οι διαβαθμισμένες πληροφορίες που έχουν ληφθεί θα χρησιμοποιούνται αποκλειστικά για τους σκοπούς και υπό τους όρους έκδοσης ή τους περιορισμούς αναφορικά με τη χρήση των Διαβαθμισμένων Πληροφοριών που ορίζονται κατά το χρόνο μετάδοσης αυτών.

2. Έκαστο των Μερών δεν κοινοποιεί Διαβαθμισμένες Πληροφορίες σε Τρίτο Πρόσωπο χωρίς την προηγούμενη γραπτή συγκατάθεση της Αρμόδιας Αρχής Ασφαλείας του άλλου Μέρους, που χορήγησε την επισήμανση διαβάθμισης ασφαλείας.

Άρθρο 6
Διαβαθμισμένες Συμβάσεις

1. Ο Εντολέας δύναται να συνάψει Διαβαθμισμένη Σύμβαση με τον Συμβαλλόμενο του άλλου Μέρους.

2. Στην περίπτωση που αναφέρεται στην Παράγραφο 1, ο Εντολέας θα υποβάλλει αίτημα προς την Αρμόδια Αρχή Ασφαλείας του δικού του Μέρους για να ζητήσει από την Αρμόδια Αρχή Ασφαλείας του άλλου Μέρους να εκδώσει γραπτή βεβαίωση ότι ο Συμβαλλόμενος είναι εξουσιοδοτημένος να έχει πρόσβαση στις Διαβαθμισμένες Πληροφορίες του καθορισμένου επιπέδου διαβάθμισης ασφαλείας.

3. Η έκδοση της βεβαίωσης που αναφέρεται στην Παράγραφο 2 θα υπόκειται στην διασφάλιση ότι ο Συμβαλλόμενος πληροί τα κριτήρια του πεδίου εφαρμογής της προστασίας Διαβαθμισμένων Πληροφοριών, όπως αυτά καθορίζονται στην εθνική νομοθεσία του Μέρους στην επικράτεια του οποίου ο Συμβαλλόμενος έχει την έδρα του.

4. Αν ο Συμβαλλόμενος δεν έχει προηγουμένως εξουσιοδοτηθεί να έχει πρόσβαση σε Διαβαθμισμένες Πληροφορίες του καθορισμένου επιπέδου διαβάθμισης ασφαλείας, η Αρμόδια Αρχή Ασφαλείας που θα εκδώσει την βεβαίωση, θα ειδοποιήσει άμεσα την Αρμόδια Αρχή Ασφαλείας του άλλου Μέρους ότι, σύμφωνα με το αίτημα του, θα ληφθούν οι ενέργειες που αναφέρονται στην Παράγραφο 3.

5. Ο Συμβαλλόμενος δεν θα έχει πρόσβαση στις Διαβαθμισμένες Πληροφορίες μέχρι την παραλαβή της βεβαίωσης που αναφέρεται στις Παραγράφους 2 και 3.

6. Ο Εντολέας θα ειδοποιήσει τον Συμβαλλόμενο αναφορικά με τις απαιτήσεις ασφαλείας που είναι αναγκαίες για την εκτέλεση της Διαβαθμισμένης Σύμβασης, οι οποίες περιλαμβάνουν κατάλογο των Διαβαθμισμένων Πληροφοριών και τους κανόνες διαβάθμισης των πληροφοριών που παρέχονται κατά την εκτέλεση της Διαβαθμισμένης Σύμβασης. Αντίγραφο των εν λόγω εγγράφων θα διαβιβάζεται στην Αρμόδια Αρχή Ασφαλείας.

7. Η Αρμόδια Αρχή Ασφαλείας του Μέρους στην επικράτεια του οποίου θα εκτελεσθεί η Διαβαθμισμένη Σύμβαση θα διασφαλίσει ότι ο Συμβαλλόμενος προστατεύει τις Διαβαθμισμένες

Πληροφορίες σύμφωνα με τις απαιτήσεις ασφαλείας και την εθνική νομοθεσία του Μέρους αυτού.

8. Οι Αρμόδιες Αρχές Ασφαλείας θα διασφαλίσουν ότι οι πιθανοί υποσυμβαλλόμενοι συμμορφώνονται με τους ίδιους όρους για την προστασία Διαβαθμισμένων Πληροφοριών όπως αυτά εφαρμόζονται για τον Συμβαλλόμενο.

Άρθρο 7
Διαβίβαση Διαβαθμισμένων Πληροφοριών

1. Οι διαβαθμισμένες Πληροφορίες διαβιβάζονται μέσω της διπλωματικής οδού ή μέσω άλλων οδών που διασφαλίζουν την προστασία τους από μη επιτρεπόμενη κοινοποίηση, που συμφωνείται μεταξύ των Αρμόδιων Αρχών Ασφαλείας έκαστου Μέρους. Ο Παραλήπτης θα επιβεβαιώσει γραπτώς την λήψη των Διαβαθμισμένων Πληροφοριών.

2. Πληροφορίες που κατατάσσονται ως ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ / INTERNO / RESTRICTED δύνανται να διαβιβασθούν και με το ταχυδρομείο ή με οποιαδήποτε άλλη υπηρεσία παράδοσης σύμφωνα με την εθνική νομοθεσία.

Άρθρο 8
Αναπαραγωγή και Μετάφραση Διαβαθμισμένων Πληροφοριών

1. Πληροφορίες που κατατάσσονται ως ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / STROGO TAJNO / TOP SECRET θα αναπαράγονται μόνο με την προηγούμενη γραπτή συγκατάθεση της Αρμόδιας Αρχής του Μέρους που παρέχει τις εν λόγω πληροφορίες.

2. Η αναπαραγωγή Διαβαθμισμένων Πληροφοριών θα γίνεται σύμφωνα με την εθνική νομοθεσία έκαστων των Μερών. Οι αναπαραγόμενες πληροφορίες θα υπόκεινται στην ίδια προστασία όπως οι πρωτότυπες πληροφορίες. Ο αριθμός των αντιγράφων θα μειώνεται στον αριθμό που είναι απαραίτητος για επίσημους σκοπούς.

3. Η οποιαδήποτε μετάφραση Διαβαθμισμένων Πληροφοριών θα γίνεται από άτομα στα οποία έχει διενεργηθεί ο κατάλληλος έλεγχος ασφαλείας. Όλες οι μεταφράσεις θα περιέχουν σημείωση στην γλώσσα που έχουν μεταφραστεί δηλώνοντας ότι περιέχουν Διαβαθμισμένες Πληροφορίες της Αρμόδιας Αρχής του άλλου Μέρους. Η μετάφραση θα υπόκειται στην ίδια προστασία όπως οι πρωτότυπες πληροφορίες.

Άρθρο 9
Καταστροφή Διαβαθμισμένων Πληροφοριών

1. Οι Διαβαθμισμένες Πληροφορίες θα καταστρέφονται σύμφωνα με την εθνική νομοθεσία των Μερών, με τέτοιο τρόπο ώστε να εξαλειφθεί ο μερικός ή ο ολικός ανασχηματισμός τους.

2. Διαβαθμισμένες Πληροφορίες με τη σήμανση ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ / STROGO TAJNO / TOP SECRET, δεν θα καταστρέφονται. Θα επιστρέφονται στην Αρμόδια Αρχή του μέρους που παρείχε τις εν λόγω πληροφορίες.

3. Σε περίπτωση κατάστασης κρίσης, στην οποία είναι αδύνατη η προστασία ή η επιστροφή Διαβαθμισμένων Πληροφοριών, τέτοιες πληροφορίες θα καταστρέφονται αμέσως. Ο Παραλήπτης θα ενημερώσει την Αρμόδια Αρχή Ασφαλείας του άλλου Μέρους αναφορικά με την καταστροφή το συντομότερο δυνατό.

Άρθρο 10
Επισκέψεις

1. Επισκέψεις που απαιτούν να έχουν πρόσβαση σε Διαβαθμισμένες Πληροφορίες θα υπόκεινται στην προηγούμενη άδεια της Αρμόδιας Αρχής Ασφαλείας του Μέρους υποδοχής.

2. Η άδεια που αναφέρεται στην Παράγραφο 1 θα χορηγείται μόνο στα άτομα που έχουν εξουσιοδότηση πρόσβασης σε Διαβαθμισμένες Πληροφορίες σύμφωνα με την εθνική νομοθεσία του Μέρους που ορίζει το εν λόγω άτομο.

3. Το αίτημα για επίσκεψη θα υποβάλλεται στη σχετική Εθνική Αρχή Ασφαλείας τουλάχιστον 20 μέρες πριν από την έναρξη της επίσκεψης. Το αίτημα για την επίσκεψη θα περιλαμβάνει τις ακόλουθες πληροφορίες οι οποίες θα χρησιμοποιηθούν μόνο για τους σκοπούς της επίσκεψης:

α. τον σκοπό, την ημερομηνία και το πρόγραμμα της επίσκεψης και το υψηλότερο επίπεδο διαβάθμισης ασφαλείας Διαβαθμισμένων Πληροφοριών,

β. το όνομα και επίθετο του επισκέπτη, την ημερομηνία και τον τόπο γεννήσεως, την υπηκοότητα, τον αριθμό διαβατηρίου ή δελτίου ταυτότητας,

γ. την θέση του επισκέπτη καθώς και το όνομα του ιδρύματος ή οργανισμού που αντιπροσωπεύει,

δ. την εγκυρότητα και πιστοποίηση του βαθμού Ελέγχου Ασφαλείας Προσωπικού που κατέχει ο επισκέπτης,

ε. το όνομα και διεύθυνση του οργανισμού που θα επισκεφθεί,

στ. το όνομα, επίθετο, στοιχεία επικοινωνίας και θέση του ατόμου που θα επισκεφθεί.

ζ. την ημερομηνία και υπογραφή της Αρμόδιας Αρχής Ασφαλείας.

4. Οι Αρμόδιες Αρχές θα διασφαλίσουν την προστασία των προσωπικών δεδομένων του προσώπου που επισκέπτεται σύμφωνα με την εθνική νομοθεσία τους.

5. Η πρόσβαση σε Διαβαθμισμένες Πληροφορίες κατά τη διάρκεια επίσκεψης θα προστατεύεται σύμφωνα με τις πρόνοιες της παρούσας Συμφωνίας.

Άρθρο 11
Παράβαση Ασφαλείας

1. Σε περίπτωση Παράβασης Ασφαλείας που προκύπτει από μη εξουσιοδοτημένη αποκάλυψη, υπεξαίρεση ή απώλεια Διαβαθμισμένων Πληροφοριών ή υποψία τέτοιας παράβασης, η Αρμόδια Αρχή Ασφαλείας του Παραλήπτη θα ενημερώσει την Αρμόδια Αρχή Ασφαλείας του άλλου Μέρους, το συντομότερο δυνατό, και θα κινήσει την ενδεδειγμένη έρευνα.

2. Αν η παράβαση ασφαλείας προκύπτει σε Τρίτο Μέρος, η Αρμόδια Αρχή Ασφαλείας του Μέρους που παρείχε τις πληροφορίες στο Τρίτο Μέρος θα λάβει όλα τα αναγκαία μέτρα προκειμένου να διασφαλίσει ότι οι ενέργειες που αναφέρονται στην Παράγραφο 1 έχουν κινηθεί.

3. Η Αρμόδια Αρχή Ασφαλείας του Μέρους που παρείχε τις εν λόγω πληροφορίες, κατόπιν αιτήματος, θα συνεργασθεί στην έρευνα σύμφωνα με την Παράγραφο 1. Θα ενημερωθεί για τα αποτελέσματα και θα λάβει την τελική έκθεση για τους λόγους και τον βαθμό της ζημιάς.

Άρθρο 12
Δαπάνες

Έκαστο των Μερών καλύπτει τις δαπάνες του οι οποίες προκύπτουν από την εφαρμογή της παρούσας Συμφωνίας.

Άρθρο 13
Διαβουλεύσεις

1. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών θα κοινοποιούν μεταξύ τους τις οποιεσδήποτε τροποποιήσεις στην εθνική τους νομοθεσία αναφορικά με την προστασία Διαβαθμισμένων Πληροφοριών.

2. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών θα διαβουλεύονται μεταξύ τους, κατόπιν αιτήματος εκατέρου εξ αυτών, για την στενή συνεργασία σχετικά με την εφαρμογή των προνοιών της παρούσας Συμφωνίας.

3. Οι Αρμόδιες Αρχές Ασφαλείας των Μερών θα ανταλλάσουν επισκέψεις για να συζητήσουν τις διαδικασίες και τα πρότυπα για την προστασία Διαβαθμισμένων Πληροφοριών.

4. Οι Αρμόδιες Αρχές Ασφαλείας θα ενημερώνουν αμέσως ο ένας τον άλλο για οποιεσδήποτε αλλαγές στην αμοιβαία αναγνώριση της Διαβάθμισης Ασφαλείας Προσωπικού και στον Έλεγχο Διαβάθμισης Ασφαλείας.

5. Κατόπιν αιτήματος, οι Αρμόδιες Αρχές Ασφαλείας θα συνεργάζονται μεταξύ τους κατά τη διενέργεια των διαδικασιών ελέγχου ασφαλείας.

Άρθρο 14
Επίλυση Διαφορών

1. Οποιεσδήποτε διαφορές που αφορούν την ερμηνεία ή την εφαρμογή της παρούσας Συμφωνίας θα επιλύονται με απευθείας διαβουλεύσεις μεταξύ των Αρμόδιων Αρχών Ασφαλείας των Μερών.

2. Αν η επίλυση οποιασδήποτε διαφοράς δεν μπορεί να επιτευχθεί με τον τρόπο που αναφέρεται στην Παράγραφο 1, η εν λόγω διαφορά θα επιλυθεί μέσω της διπλωματικής οδού.

Άρθρο 15
Τελικές Διατάξεις

1. Η παρούσα Συμφωνία θα τεθεί σε ισχύ την πρώτη μέρα του δεύτερου μήνα που έπεται της ημερομηνίας κατά την οποία τα Μέρη κοινοποιούν το ένα στο άλλο, μέσω της διπλωματικής οδού, ότι όλες οι αναγκαίες εσωτερικές διαδικασίες για την έναρξη ισχύος της παρούσας Συμφωνίας έχουν ολοκληρωθεί.

2. Η παρούσα Συμφωνία συνομολογήθηκε για απεριόριστο χρόνο. Δύναται να τερματισθεί από εκατέρωθεν των Μερών κατόπιν γραπτής ειδοποίησης προς το άλλο Μέρος. Σε τέτοια περίπτωση η παρούσα Συμφωνία θα λήξη έξι μήνες μετά την ημερομηνία της ειδοποίησης τερματισμού.

3. Σε περίπτωση τερματισμού της παρούσας Συμφωνίας, οποιεσδήποτε Διαβαθμισμένες Πληροφορίες που έχουν διαβιβασθεί δυνάμει της παρούσας Συμφωνίας εξακολουθούν να προστατεύονται σύμφωνα με τις διατάξεις που αναφέρονται στην παρούσα.

4. Η παρούσα Συμφωνία δύναται να τροποποιηθεί με την γραπτή αμοιβαία συμφωνία αμφότερων των Μερών. Οι τροποποιήσεις θα τεθούν σε ισχύ σύμφωνα με τις πρόνοιες της Παραγράφου 1.

Έγινε στην [illegible] στις [illegible] και συντάχθηκε σε δύο αντίτυπα, το κάθε ένα στην Ελληνική, Σλοβενική και Αγγλική γλώσσα, όλα δε τα κείμενα είναι εξίσου αυθεντικά. Σε περίπτωση απόκλισης στην ερμηνεία θα υπερισχύει το Αγγλικό κείμενο.

ΕΚ ΜΕΡΟΥΣ ΤΗΣ
ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ
ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΕΚ ΜΕΡΟΥΣ ΤΗΣ
ΚΥΒΕΡΝΗΣΗΣ ΤΗΣ
ΔΗΜΟΚΡΑΤΙΑΣ ΤΗΣ ΣΛΟΒΕΝΙΑΣ

Μέρος III
(Σλοβενική γλώσσα)

SPORAZUM

med Vlado Republike Ciper in Vlado Republike Slovenije o izmenjavi in medsebojnem varovanju tajnih podatkov

Vlada Republike Ciper in Vlada Republike Slovenije, v nadaljevanju "pogodbenici", sta se

v želji, da bi zagotovili varovanje tajnih podatkov, izmenjanih med njima ali med javnimi in zasebnimi subjekti v njuni pristojnosti,

ob spoznanju, da lahko dobro sodelovanje zahteva izmenjavo tajnih podatkov med pogodbenicama,

dogovorili:

1. člen

Pomen izrazov

V tem sporazumu izrazi pomenijo:

1. "prejemnik" – pristojni organ, ki prejme tajne podatke;

2. "pristojni organ" – javni ali zasebni subjekt v pristojnosti pogodbenice, ki je pooblaščen za ravnanje s tajnimi podatki in njihovo hrambo v skladu z notranjo zakonodajo te pogodbenice, vključno s pristojnim varnostnim organom;

3. "pristojni varnostni organ" – državni organ iz prvega odstavka 3. člena, ki ga določi pogodbenica za splošno izvajanje tega sporazuma in ustrezen nadzor nad vsemi njegovimi vidiki;

4. "izvajalec" – posameznik, pravna oseba ali organizacijska enota s sposobnostjo za sklepanje pogodb;

5. "pogodba s tajnimi podatki" – pogodba ali podpogodba, ki zahteva dostop do tajnih podatkov;

6. "tajni podatek" – podatek v kakršni koli obliki, ki se prenese ali nastane med pogodbenicama ali pristojnima organoma in ga je treba po notranji zakonodaji pogodbenice varovati pred nepooblaščenim razkritjem ali drugim ogrožanjem ter ga je kot takega določila in ustrezno označila pogodbenica;

7. "varnostno dovoljenje organizacije" – odločitev po varnostnem preverjanju organizacije, da izvajalec, ki je pravna oseba, izpolnjuje pogoje za ravnanje s tajnimi podatki v skladu z notranjo zakonodajo pogodbenice;

8. "potreba po seznanitvi" – načelo, po katerem se posamezniku lahko dovoli dostop do določenih tajnih podatkov le v povezavi z njegovimi uradnimi dolžnostmi ali zaradi opravljanja določene naloge;

9. "dovoljenje za dostop do tajnih podatkov" – odločitev po varnostnem preverjanju osebe v skladu z notranjo zakonodajo, na podlagi katere je posameznik pooblaščen za dostop do tajnih podatkov stopnje tajnosti, ki je navedena na dovoljenju, in za ravnanje z njimi;

10. "naročnik" – vladni organ, ki namerava skleniti ali sklene pogodbo s tajnimi podatki na ozemlju druge pogodbenice;

11. "tretja stran" – država, vključno z javnim ali zasebnim subjektom ali posameznikom v njeni pristojnosti, ali mednarodna organizacija, ki ni pogodbenica tega sporazuma.

2. člen

Stopnje tajnosti

Pogodbenici soglašata, da so naslednje stopnje tajnosti enakovredne in ustrezajo stopnjam tajnosti, določenim v njuni notranji zakonodaji:

Republika Ciper	Republika Slovenija	Angleška ustreznica
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	STROGO TAJNO	TOP SECRET
ΑΠΟΡΡΗΤΟ	TAJNO	SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	ZAUPNO	CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	INTERNO	RESTRICTED

3. člen

Pristojna varnostna organa

1. Pristojna varnostna organa za namen tega sporazuma sta:

   a. za Republiko Ciper: nacionalni varnostni organ (Ministrstvo za obrambo).

   b. za Republiko Slovenijo: nacionalni varnostni organ (Urad Vlade Republike Slovenije za varovanje tajnih podatkov);

2. Pristojna varnostna organa lahko sklepata dogovore o izvajanju določb tega sporazuma.

3. Pogodbenici se po diplomatski poti obveščata o vseh poznejših spremembah nacionalnih varnostnih organov.

4. člen

Načela varovanja tajnih podatkov

1. Pogodbenici v skladu s tem sporazumom in svojo notranjo zakonodajo sprejmeta ustrezne ukrepe za varovanje tajnih podatkov.

2. Pogodbenici za podatke iz prvega odstavka zagotovita najmanj enako varovanje, kot ga uporabljata za svoje tajne podatke ustrezne stopnje tajnosti iz 2. člena.

3. Za splošno izvajanje tega sporazuma in ustrezen nadzor nad vsemi njegovimi vidiki sta odgovorna pristojna nacionalna varnostna organa, ki ju določita pogodbenici.

4. Do prejetih tajnih podatkov lahko dostopajo le osebe, ki imajo potrebo po seznanitvi, so bile varnostno preverjene in/ali pooblaščene za dostop do tovrstnih podatkov ter ustrezno poučene o varovanju tajnih podatkov v skladu z notranjo zakonodajo pogodbenice.

5. Pogodbenica zagotovi, da se izvajajo ustrezni ukrepi za varovanje tajnih podatkov, ki se obdelujejo, hranijo ali prenašajo v komunikacijskih in informacijskih sistemih. Ti ukrepi zagotavljajo zaupnost, celovitost, razpoložljivost, in kadar je mogoče, nezatajljivost in verodostojnost tajnih podatkov ter ustrezno raven odgovornosti in sledljivosti dejanj, povezanih s temi podatki.

6. Stopnjo tajnosti spremeni ali prekliče le pristojni organ, ki jo je določil. O vsaki spremembi ali preklicu stopnje tajnosti je prejemnik nemudoma obveščen.

7. Pogodbenici si priznavata dovoljenja za dostop do tajnih podatkov in varnostna dovoljenja organizacij. Pri tem se glede stopenj tajnosti uporablja 2. člen.

5. člen

Omejitve pri uporabi tajnih podatkov

1. Prejeti tajni podatki se uporabljajo izključno za namene in po pogojih za dajanje tajnih podatkov ali v skladu z omejitvami njihove uporabe, kot se določi ob prenosu tajnih podatkov.

2. Pogodbenica tajnih podatkov ne sme dati tretji strani brez predhodnega pisnega soglasja pristojnega varnostnega organa druge pogodbenice, ki je določila ustrezno stopnjo tajnosti.

6. člen

Pogodbe s tajnimi podatki

1. Naročnik lahko sklene pogodbo s tajnimi podatki z izvajalcem druge pogodbenice.

2. V primeru iz prvega odstavka naročnik pristojnemu varnostnemu organu svoje pogodbenice predloži zaprosilo, naj pristojni varnostni organ druge pogodbenice zaprosi za

pisno potrdilo, da je izvajalec pooblaščen za dostop do tajnih podatkov določene stopnje tajnosti.

3. Potrdilo iz drugega odstavka zagotavlja, da izvajalec izpolnjuje merila za varovanje tajnih podatkov, določena v notranji zakonodaji pogodbenice, na ozemlju katere je izvajalec.

4. Če izvajalec prej ni bil pooblaščen za dostop do tajnih podatkov določene stopnje tajnosti, pristojni varnostni organ, ki naj bi izdal potrdilo, nemudoma uradno obvesti pristojni varnostni organ druge pogodbenice, da bodo na njegovo zahtevo izvedena dejanja v skladu s tretjim odstavkom.

5. Izvajalec do prejema potrdila iz drugega in tretjega odstavka nima dostopa do tajnih podatkov.

6. Naročnik izvajalca uradno obvesti o varnostnih zahtevah, ki so potrebne za izvajanje pogodbe s tajnimi podatki ter še zlasti vključujejo seznam tajnih podatkov in pravila o določanju stopnje tajnosti podatkov, ki nastanejo med izvajanjem pogodbe s tajnimi podatki. Izvod takih dokumentov se pošlje pristojnemu varnostnemu organu.

7. Pristojni varnostni organ pogodbenice, na katere ozemlju se bo izvajala pogodba s tajnimi podatki, zagotovi, da izvajalec varuje tajne podatke v skladu s prejetimi varnostnimi zahtevami in notranjo zakonodajo svoje pogodbenice.

8. Pristojna varnostna organa zagotovita, da vsi morebitni podizvajalci izpolnjujejo enake pogoje za varovanje tajnih podatkov, kot so bili predpisani za izvajalca.

7. člen

Prenos tajnih podatkov

1. Prenos tajnih podatkov poteka po diplomatski poti ali drugih zaščitenih poteh, ki zagotavljajo varovanje pred nepooblaščenim razkritjem in o katerih se dogovorita pristojna varnostna organa. Prejemnik pisno potrdi prejem tajnih podatkov.

2. Tajni podatki ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ/INTERNO/RESTRICTED se lahko pošiljajo po pošti ali z drugo dostavno službo v skladu z notranjo zakonodajo.

8. člen

Razmnoževanje in prevajanje tajnih podatkov

1. Podatki stopnje ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/STROGO TAJNO/TOP SECRET se razmnožujejo le s predhodnim pisnim dovoljenjem pristojnega organa pogodbenice, ki je tem podatkom določil stopnjo tajnosti.

2. Tajni podatki se razmnožujejo v skladu z notranjo zakonodajo pogodbenic. Razmnoženi podatki se varujejo enako kot izvirniki. Število izvodov je omejeno na najmanjšo količino, potrebno za uradne namene.

3. Tajne podatke prevajajo ustrezno varnostno preverjeni posamezniki. Vsak prevod vsebuje ustrezno navedbo v jeziku prevoda, da prevod vsebuje tajne podatke druge pogodbenice. Prevod se varuje enako kot izvirnik.

9. člen

Uničevanje tajnih podatkov

1. Tajni podatki se uničijo v skladu z notranjo zakonodajo pogodbenice, tako da jih ni mogoče več delno ali v celoti obnoviti.

2. Tajni podatki z oznako ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ/ STROGO TAJNO/TOP SECRET se ne smejo uničiti. Vrnejo se pristojnemu organu pogodbenice, ki je podatkom določil stopnjo tajnosti.

3. V kriznih razmerah, ko ni mogoče varovati ali vrniti tajnih podatkov, se ti takoj uničijo. Prejemnik o uničenju čim prej obvesti pristojni varnostni organ druge pogodbenice.

10. člen

Obiski

1. Za obiske, pri katerih je potreben dostop do tajnih podatkov, se zahteva predhodno dovoljenje pristojnega varnostnega organa pogodbenice gostiteljice.

2. Dovoljenje iz prvega odstavka se izda samo osebam, ki jih je določila pogodbenica in so v skladu z njeno notranjo zakonodajo pooblaščene za dostop do tajnih podatkov

3. Zaprosilo za obisk se predloži ustreznemu nacionalnemu varnostnemu organu vsaj 20 dni pred začetkom obiska. Vsebuje te podatke, ki se uporabljajo samo za obisk:

a. namen, datum in program obiska, vključno z najvišjo stopnjo tajnosti podatkov, ki bodo obravnavani;

b. ime in priimek obiskovalca, datum in kraj rojstva, državljanstvo ter številko potnega lista ali osebne izkaznice;

c. položaj obiskovalca skupaj z imenom institucije ali organizacije, ki jo obiskovalec zastopa;

d. veljavnost in stopnjo tajnosti obiskovalčevega dovoljenja za dostop do tajnih podatkov;

e. ime in naslov organizacije, ki bo obiskana;

f. ime in priimek, podatki za stike ter položaj osebe, ki bo obiskana;

g. datum in podpis pristojnega varnostnega organa.

4. Pristojni organi zagotovijo varstvo osebnih podatkov obiskovalca v skladu s svojo notranjo zakonodajo.

5. Tajni podatki, ki so dostopni med obiskom, se varujejo v skladu z določbami tega sporazuma.

11. člen

Kršitev varovanja tajnosti

1. Ob kršitvi varovanja tajnosti, katere posledica je nepooblaščeno razkritje, odtujitev ali izguba tajnih podatkov, ali sumu take kršitve pristojni varnostni organ prejemnika čim prej obvesti pristojni varnostni organ druge pogodbenice in začne ustrezno preiskavo.

2. Kadar varovanje tajnosti krši tretja stran, pristojni varnostni organ pogodbenice, ki je dala podatke, sprejme vse potrebne ukrepe, s katerimi zagotovi začetek dejanj, predpisanih v prvem odstavku.

3. Pristojni varnostni organ pogodbenice, ki je dala tajne podatke, na podlagi zaprosila sodeluje pri preiskavi v skladu s prvim odstavkom. Obveščen mora biti o ugotovitvah preiskave in prejeti končno poročilo o razlogih za škodo in njenih razsežnostih.

12. člen

Stroški

Vsaka pogodbenica krije svoje stroške, ki nastanejo pri izvajanju tega sporazuma.

13. člen

Posvetovanja

1. Pristojna varnostna organa pogodbenic se uradno obveščata o vseh spremembah svoje notranje zakonodaje, ki se nanaša na varovanje tajnih podatkov.

2. Pristojna varnostna organa pogodbenic se na zaprosilo enega od njiju med seboj posvetujeta, da zagotovita tesno sodelovanje pri izvajanju določb tega sporazuma.

3. Pristojna varnostna organa pogodbenic se obiskujeta zaradi dogovarjanja o postopkih in standardih varovanja tajnih podatkov.

4. Pristojna varnostna organa se takoj obvestita o vsaki spremembi medsebojno priznanih dovoljenj za dostop do tajnih podatkov in varnostnih dovoljenj organizacij.

5. Na zaprosilo si pristojna varnostna organa pomagata pri izvajanju postopkov varnostnega preverjanja.

14. člen

Reševanje sporov

1. Spori zaradi razlage ali uporabe tega sporazuma se rešujejo neposredno s pogajanji in/ali posvetovanji med pristojnima varnostnima organoma pogodbenic.

2. Če spora ni mogoče rešiti v skladu s prvim odstavkom, se reši po diplomatski poti.

15. člen

Končne določbe

1. Sporazum začne veljati prvi dan drugega meseca po datumu, ko se pogodbenici po diplomatski poti uradno obvestita, da so bili končani vsi potrebni notranjepravni postopki za začetek njegove veljavnosti.

2. Sporazum je sklenjen za nedoločen čas. Pogodbenica ga lahko odpove s pisnim obvestilom drugi pogodbenici. V tem primeru sporazum preneha veljati šest mesecev po datumu obvestila o odpovedi.

3. Ob prenehanju veljavnosti tega sporazuma se vsi tajni podatki, preneseni na njegovi podlagi, še naprej varujejo v skladu z njegovimi določbami

4. Sporazum se lahko spremeni s pisnim soglasjem pogodbenic. Spremembe začnejo veljati v skladu s prvim odstavkom.

Sestavljeno v Ljubljani 19. februarja 2014 v dveh izvirnikih v grškem, slovenskem in angleškem jeziku, pri čemer so vsa besedila enako verodostojna. Pri različni razlagi prevlada angleško besedilo.

Za Vlado
Republike Ciper

Za Vlado
Republike Slovenije