ΑΠΟΦΑΣΗ (ΕΕ, ΕΥΡΑΤΟΜ) 2021/259 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 10ης Φεβρουαρίου 2021

για τη θέσπιση κανόνων εφαρμογής για τη βιομηχανική ασφάλεια όσον αφορά τις διαβαθμισμένες συμφωνίες επιδότησης

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 249,

Έχοντας υπόψη τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, και ιδίως το άρθρο 106,

Έχοντας υπόψη τον κανονισμό (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουλίου 2018, σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης, την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1296/2013, (ΕΕ) αριθ. 1301/2013, (ΕΕ) αριθ. 1303/2013, (ΕΕ) αριθ. 1304/2013, (ΕΕ) αριθ. 1309/2013, (ΕΕ) αριθ. 1316/2013, (ΕΕ) αριθ. 223/2014, (ΕΕ) αριθ. 283/2014 και της απόφασης αριθ. 541/2014/ΕΕ και για την κατάργηση του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 966/2012 ([1]),

Έχοντας υπόψη την απόφαση (ΕΕ, Ευρατόμ) 2015/443 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με την ασφάλεια στην Επιτροπή ([2]),

Έχοντας υπόψη την απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ ([3]),

Έχοντας υπόψη την απόφαση (ΕΕ, Ευρατόμ) 2017/46 της Επιτροπής, της 10ης Ιανουαρίου 2017, σχετικά με την ασφάλεια των συστημάτων επικοινωνίας και πληροφοριών στην Ευρωπαϊκή Επιτροπή ([4]),

Αφού ζήτησε τη γνώμη της ομάδας εμπειρογνωμόνων ασφαλείας της Επιτροπής, σύμφωνα με το άρθρο 41 παράγραφος 5 της απόφασης (ΕΕ, Ευρατόμ) 2015/444,

Εκτιμώντας τα ακόλουθα:

(1) Τα άρθρα 41, 42, 47 και 48 της απόφασης (ΕΕ, Ευρατόμ) 2015/444 προβλέπουν ότι, προς συμπλήρωση και υποστήριξη των διατάξεων του κεφαλαίου 6 της εν λόγω απόφασης, πρέπει να θεσπιστούν λεπτομερέστερες διατάξεις μέσω κανόνων εφαρμογής για τη βιομηχανική ασφάλεια, που θα διέπουν ζητήματα όπως οι διαβαθμισμένες συμφωνίες επιδότησης [επιχορήγησης], οι εξουσιοδοτήσεις ασφαλείας φορέα, οι εξουσιοδοτήσεις ασφαλείας προσωπικού, οι επισκέψεις και η διαβίβαση και μεταφορά διαβαθμισμένων πληροφοριών της Ευρωπαϊκής Ένωσης («ΔΠΕΕ»).

(2) Η απόφαση (ΕΕ, Ευρατόμ) 2015/444 ορίζει ότι οι διαβαθμισμένες συμφωνίες επιδότησης πρέπει να εκτελούνται σε στενή συνεργασία με την εθνική αρχή ασφαλείας, την καθορισμένη αρχή ασφαλείας ή οποιαδήποτε άλλη αρμόδια αρχή των οικείων κρατών μελών. Τα κράτη μέλη έχουν συμφωνήσει να εξασφαλίζουν ότι κάθε οντότητα υπό την αρμοδιότητά τους η οποία λαμβάνει ή παράγει διαβαθμισμένες πληροφορίες που προέρχονται από την Επιτροπή έχει υποβληθεί στον δέοντα έλεγχο ασφαλείας και είναι σε θέση να παρέχει προστασία κατάλληλη και αντίστοιχη εκείνης που παρέχουν οι κανόνες ασφαλείας του Συμβουλίου της Ευρωπαϊκής Ένωσης για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ που φέρουν αντίστοιχη ένδειξη διαβάθμισης, όπως προβλέπεται στη συμφωνία των αντιπροσώπων των κρατών μελών της Ευρωπαϊκής Ένωσης, που συνήλθαν στο πλαίσιο του Συμβουλίου, σχετικά με την προστασία διαβαθμισμένων πληροφοριών οι οποίες ανταλλάσσονται προς το συμφέρον της Ευρωπαϊκής Ένωσης (2011/C 202/05) ([5]).

([1]) ΕΕ L 193 της 30.7.2018, σ. 1.
([2]) ΕΕ L 72 της 17.3.2015, σ. 41.
([3]) ΕΕ L 72 της 17.3.2015, σ. 53.
([4]) ΕΕ L 6 της 11.1.2017, σ. 40.
([5]) ΕΕ C 202 της 8.7.2011, σ. 13.

(3) Το Συμβούλιο, η Επιτροπή και ο ύπατος εκπρόσωπος της Ένωσης για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας συμφώνησαν να μεριμνούν για τη διασφάλιση της μέγιστης δυνατής συνοχής κατά την εφαρμογή κανόνων ασφαλείας όσον αφορά την εκ μέρους τους προστασία των ΔΠΕΕ, συνεκτιμώντας τις ειδικές θεσμικές και οργανωτικές τους ανάγκες, σύμφωνα με τις δηλώσεις που επισυνάπτονται στα πρακτικά της συνόδου του Συμβουλίου κατά την οποία εγκρίθηκε η απόφαση 2013/488/ΕΕ του Συμβουλίου ([6]) σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ.

(4) Ως εκ τούτου, οι κανόνες εφαρμογής της Επιτροπής για τη βιομηχανική ασφάλεια όσον αφορά τις διαβαθμισμένες συμφωνίες επιδότησης θα πρέπει επίσης να διασφαλίζουν τη μέγιστη δυνατή συνοχή και να συνεκτιμούν τις κατευθυντήριες γραμμές για τη βιομηχανική ασφάλεια που εγκρίθηκαν από την Επιτροπή Ασφαλείας του Συμβουλίου στις 13 Δεκεμβρίου 2016.

(5) Στις 4 Μαΐου 2016, η Επιτροπή εξέδωσε απόφαση ([7]) με την οποία εξουσιοδοτεί το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής να εκδώσει, εξ ονόματος της Επιτροπής και υπό την ευθύνη της, τους κανόνες εφαρμογής που προβλέπονται στο άρθρο 60 της απόφασης (ΕΕ, Ευρατόμ) 2015/444,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

ΚΕΦΑΛΑΙΟ 1

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο και πεδίο εφαρμογής

1. Η παρούσα απόφαση θεσπίζει κανόνες εφαρμογής για τη βιομηχανική ασφάλεια όσον αφορά τις διαβαθμισμένες συμφωνίες επιδότησης, κατά την έννοια της απόφασης (ΕΕ, Ευρατόμ) 2015/444, και ιδίως του κεφαλαίου 6 της εν λόγω απόφασης.

2. Η παρούσα απόφαση καθορίζει ειδικές απαιτήσεις για τη διασφάλιση της προστασίας των διαβαθμισμένων πληροφοριών της ΕΕ (ΔΠΕΕ) κατά τη δημοσίευση προσκλήσεων υποβολής προτάσεων, καθώς και κατά τη χορήγηση επιδοτήσεων και την εκτέλεση διαβαθμισμένων συμφωνιών επιδότησης που συνάπτει η Ευρωπαϊκή Επιτροπή.

3. Η παρούσα απόφαση εφαρμόζεται σε συμφωνίες επιδότησης οι οποίες εμπεριέχουν πληροφορίες που έχουν διαβαθμιστεί σε ένα από τα ακόλουθα επίπεδα:

α) RESTREINT UE/EU RESTRICTED·

β) CONFIDENTIEL UE/EU CONFIDENTIAL·

γ) SECRET UE/EU SECRET.

4. Η παρούσα απόφαση εφαρμόζεται με την επιφύλαξη ειδικών κανόνων που καθορίζονται σε άλλες νομικές πράξεις, όπως είναι οι κανόνες που αφορούν το ευρωπαϊκό πρόγραμμα βιομηχανικής ανάπτυξης στον τομέα της άμυνας.

Άρθρο 2

Αρμοδιότητες εντός της Επιτροπής

1. Στο πλαίσιο των αρμοδιοτήτων του διατάκτη της χορηγούσας αρχής που αναφέρονται στον κανονισμό (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ο διατάκτης διασφαλίζει ότι η διαβαθμισμένη συμφωνία επιδότησης συμμορφώνεται με την απόφαση (ΕΕ, Ευρατόμ) 2015/444 και τους κανόνες εφαρμογής της.

([6]) Απόφαση 2013/488/ΕΕ του Συμβουλίου, της 23ης Σεπτεμβρίου 2013, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 274 της 15.10.2013, σ. 1)

([7]) Απόφαση της Επιτροπής της 4.5.2016 για εξουσιοδότηση σχετική με την ασφάλεια [C(2016) 2797 final].

2. Προς τον σκοπό αυτόν, ο οικείος διατάκτης ζητεί, σε όλα τα στάδια, τη γνώμη της Αρχής Ασφαλείας της Επιτροπής σχετικά με τα ζητήματα που αφορούν τα στοιχεία ασφάλειας σε διαβαθμισμένη συμφωνία επιδότησης, πρόγραμμα ή έργο και ενημερώνει τον τοπικό υπεύθυνο ασφαλείας σχετικά με τις συναφθείσες διαβαθμισμένες συμφωνίες επιδότησης. Η απόφαση σχετικά με το επίπεδο διαβάθμισης συγκεκριμένων ζητημάτων εναπόκειται στη χορηγούσα αρχή και λαμβάνεται λαμβανομένου δεόντως υπόψη του οδηγού διαβάθμισης ασφαλείας.

3. Όταν εφαρμόζονται οι εντολές ασφαλείας του προγράμματος/έργου που αναφέρονται στο άρθρο 5 παράγραφος 3, η χορηγούσα αρχή και η Αρχή Ασφαλείας της Επιτροπής εκτελούν τα καθήκοντα που τους ανατίθενται στις εν λόγω εντολές.

4. Για την εκπλήρωση των απαιτήσεων των παρόντων κανόνων εφαρμογής, η Αρχή Ασφαλείας της Επιτροπής συνεργάζεται στενά με τις εθνικές αρχές ασφαλείας (ΕΑΑ) και τις καθορισμένες αρχές ασφαλείας (ΚΑΑ) των οικείων κρατών μελών, ιδίως όσον αφορά τις εξουσιοδοτήσεις ασφαλείας φορέα (FSC) και τις εξουσιοδοτήσεις ασφαλείας προσωπικού (ΕΑΠ), τις διαδικασίες επισκέψεων και τα σχέδια μεταφορών.

5. Όταν η διαχείριση των επιδοτήσεων αναλαμβάνεται από εκτελεστικούς οργανισμούς της ΕΕ ή άλλους χρηματοδοτικούς φορείς και οι ειδικοί κανόνες που καθορίζονται σε άλλες νομικές πράξεις όπως αναφέρονται στο άρθρο 1 παράγραφος 4 δεν εφαρμόζονται:

α) η εξουσιοδοτούσα υπηρεσία της Επιτροπής ασκεί τα δικαιώματα του φορέα προέλευσης των ΔΠΕΕ που γεννώνται στο πλαίσιο των συμφωνιών επιδότησης εάν αυτό προβλέπεται στις ρυθμίσεις εξουσιοδότησης·

β) η εξουσιοδοτούσα υπηρεσία της Επιτροπής είναι αρμόδια για τον προσδιορισμό της διαβάθμισης ασφαλείας·

γ) αιτήσεις για πληροφορίες εξουσιοδότησης ασφαλείας και κοινοποιήσεις σε ΕΑΑ και/ή ΚΑΑ αποστέλλονται μέσω της Αρχής Ασφαλείας της Επιτροπής.

ΚΕΦΑΛΑΙΟ 2

ΧΕΙΡΙΣΜΟΣ ΤΩΝ ΠΡΟΣΚΛΗΣΕΩΝ ΥΠΟΒΟΛΗΣ ΠΡΟΤΑΣΕΩΝ ΓΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΦΩΝΙΕΣ ΕΠΙΔΟΤΗΣΗΣ

Άρθρο 3

Βασικές αρχές

1. Διαβαθμισμένα μέρη των συμφωνιών επιδότησης εκτελούνται μόνον από δικαιούχους που έχουν την έδρα τους σε κράτος μέλος ή από δικαιούχους που έχουν την έδρα τους σε τρίτη χώρα ή που έχουν συσταθεί από διεθνή οργανισμό, υπό τον όρο ότι η εν λόγω τρίτη χώρα ή ο εν λόγω διεθνής οργανισμός έχει συνάψει συμφωνία για την ασφάλεια των πληροφοριών με την Ένωση ή έχει συνάψει διοικητικό διακανονισμό με την Επιτροπή ([8]).

2. Πριν από την έναρξη διαδικασίας πρόσκλησης υποβολής προτάσεων για διαβαθμισμένη συμφωνία επιδότησης, η χορηγούσα αρχή καθορίζει τη διαβάθμιση ασφαλείας κάθε πληροφορίας που θα μπορούσε να παρασχεθεί στους αιτούντες. Η χορηγούσα αρχή καθορίζει επίσης την ανώτατη διαβάθμιση ασφαλείας των πληροφοριών που τυχόν θα χρησιμοποιηθούν ή θα παραχθούν κατά την εκτέλεση της συμφωνίας επιδότησης ή του προγράμματος ή του έργου, ή τουλάχιστον τον προβλεπόμενο όγκο και το προβλεπόμενο είδος των πληροφοριών που θα παραχθούν ή θα αποτελέσουν αντικείμενο χειρισμού, καθώς και την ανάγκη για σύστημα διαβαθμισμένων επικοινωνιών και πληροφοριών (CIS).

3. Η χορηγούσα αρχή διασφαλίζει ότι οι προσκλήσεις υποβολής προτάσεων για διαβαθμισμένες συμφωνίες επιδότησης παρέχουν πληροφορίες σχετικά με τις ειδικές υποχρεώσεις ασφαλείας που σχετίζονται με διαβαθμισμένες πληροφορίες. Τα έγγραφα της πρόσκλησης περιλαμβάνουν διευκρινίσεις σχετικά με το χρονοδιάγραμμα βάσει του οποίου οι δικαιούχοι πρέπει να εξασφαλίσουν τις εξουσιοδοτήσεις ασφαλείας φορέα, εφόσον απαιτούνται. Στα παραρτήματα I και II περιλαμβάνονται υποδείγματα για πληροφορίες όσον αφορά τους όρους της πρόσκλησης.

([8]) Ο κατάλογος των συμφωνιών που έχει συνάψει η ΕΕ και των διοικητικών διακανονισμών που έχει συνάψει η Ευρωπαϊκή Επιτροπή, βάσει των οποίων είναι δυνατή η ανταλλαγή διαβαθμισμένων πληροφοριών της ΕΕ με τρίτες χώρες και διεθνείς οργανισμούς, διατίθεται στον ιστότοπο της Επιτροπής.

4. Η χορηγούσα αρχή διασφαλίζει ότι οι πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET κοινοποιούνται στους αιτούντες μόνο αφού υπογράψουν συμφωνία τήρησης του απορρήτου, η οποία υποχρεώνει τους αιτούντες να χειρίζονται και να προστατεύουν τις ΔΠΕΕ σύμφωνα με την απόφαση (ΕΕ, Ευρατόμ) 2015/444, τους κανόνες εφαρμογής της και τους εφαρμοστέους εθνικούς κανόνες.

5. Όταν παρέχονται πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED σε αιτούντες, οι ελάχιστες προδιαγραφές που αναφέρονται στο άρθρο 5 παράγραφος 7 της παρούσας απόφασης περιλαμβάνονται στην πρόσκληση ή στις συμφωνίες τήρησης του απορρήτου που συνάπτονται κατά το στάδιο της υποβολής προτάσεων.

6. Όλοι οι αιτούντες και οι δικαιούχοι που καλούνται να χειριστούν ή να αποθηκεύσουν πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET εντός των εγκαταστάσεών τους, είτε κατά το στάδιο της υποβολής προτάσεων είτε κατά καθαυτή την εκτέλεση της διαβαθμισμένης συμφωνίας επιδότησης, διαθέτουν εξουσιοδότηση ασφαλείας φορέα του απαιτούμενου επιπέδου, εξαιρουμένων των περιπτώσεων που αναφέρονται στην παράγραφο 9. Ακολούθως προσδιορίζονται τα τρία σενάρια που ενδέχεται να προκύψουν κατά το στάδιο της υποβολής προτάσεων για διαβαθμισμένη συμφωνία επιδότησης που αφορά ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET:

α) Μη πρόσβαση σε ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET κατά το στάδιο της υποβολής προτάσεων:

Εάν η πρόσκληση υποβολής προτάσεων αφορά επιδότηση που θα περιλαμβάνει ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, αλλά δεν απαιτεί από τον αιτούντα να χειριστεί τέτοιες πληροφορίες κατά το στάδιο της υποβολής προτάσεων, αιτών που δεν διαθέτει εξουσιοδότηση ασφαλείας φορέα του απαιτούμενου επιπέδου δεν αποκλείεται από τη διαδικασία υποβολής αιτήσεων επειδή δεν διαθέτει εξουσιοδότηση ασφαλείας φορέα.

β) Πρόσβαση σε ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET στις εγκαταστάσεις της χορηγούσας αρχής κατά το στάδιο της υποβολής προτάσεων:

Πρόσβαση παρέχεται σε προσωπικό του αιτούντος το οποίο διαθέτει εξουσιοδότηση ασφαλείας προσωπικού του απαιτούμενου επιπέδου και το οποίο έχει ανάγκη γνώσης.

γ) Χειρισμός ή αποθήκευση ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET στις εγκαταστάσεις του αιτούντος κατά το στάδιο της υποβολής προτάσεων:

Εάν η πρόσκληση υποβολής προτάσεων απαιτεί από τους αιτούντες να χειριστούν ή να αποθηκεύσουν ΔΠΕΕ στις εγκαταστάσεις τους, ο αιτών διαθέτει εξουσιοδότηση ασφαλείας φορέα του απαιτούμενου επιπέδου. Στις περιπτώσεις αυτές, η χορηγούσα αρχή εξασφαλίζει, μέσω της Αρχής Ασφαλείας της Επιτροπής, διαβεβαίωση από την αρμόδια εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας ότι έχει χορηγηθεί στον αιτούντα κατάλληλη εξουσιοδότηση ασφαλείας φορέα, πριν από την παροχή οποιουδήποτε υλικού ΔΠΕΕ στον αιτούντα. Πρόσβαση παρέχεται σε προσωπικό του αιτούντος το οποίο διαθέτει εξουσιοδότηση ασφαλείας προσωπικού του απαιτούμενου επιπέδου και το οποίο έχει ανάγκη γνώσης.

7. Καταρχήν, δεν απαιτείται εξουσιοδότηση ασφαλείας φορέα ή εξουσιοδότηση ασφαλείας προσωπικού για πρόσβαση σε πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED, ούτε στο στάδιο της υποβολής προτάσεων ούτε στο πλαίσιο της εκτέλεσης της συμφωνίας επιδότησης. Στις περιπτώσεις που κράτη μέλη, βάσει των εθνικών νομοθετικών και κανονιστικών διατάξεών τους, απαιτούν εξουσιοδότηση ασφαλείας φορέα ή εξουσιοδότηση ασφαλείας προσωπικού για συμφωνίες επιδότησης ή συμβάσεις υπεργολαβίας επιπέδου RESTREINT UE/EU RESTRICTED, όπως παρατίθενται στο παράρτημα IV, οι εν λόγω εθνικές απαιτήσεις δεν επιβάλλουν πρόσθετες υποχρεώσεις σε άλλα κράτη μέλη και δεν αποκλείουν αιτούντες, δικαιούχους ή υπεργολάβους από κράτη μέλη που δεν επιβάλλουν τέτοιες απαιτήσεις για εξουσιοδότηση ασφαλείας φορέα ή εξουσιοδότηση ασφαλείας προσωπικού για την πρόσβαση σε πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED από σχετικές συμφωνίες επιδότησης ή συμβάσεις υπεργολαβίας ή διαγωνισμούς για τέτοιες συμφωνίες. Οι εν λόγω συμφωνίες επιδότησης εκτελούνται στα κράτη μέλη σύμφωνα με τις οικείες εθνικές νομοθετικές και κανονιστικές διατάξεις.

8. Εάν απαιτείται εξουσιοδότηση ασφαλείας φορέα στο πλαίσιο του χειρισμού πρόσκλησης υποβολής προτάσεων ή για την εκτέλεση διαβαθμισμένης συμφωνίας επιδότησης, η χορηγούσα αρχή υποβάλλει, μέσω της Αρχής Ασφαλείας της Επιτροπής, αίτηση στην εθνική αρχή ασφαλείας ή στην καθορισμένη αρχή ασφαλείας του δικαιούχου χρησιμοποιώντας δελτίο πληροφοριών εξουσιοδότησης ασφαλείας φορέα (FSCIS) ή οποιοδήποτε εγκεκριμένο αντίστοιχο ηλεκτρονικό έντυπο. Το παράρτημα III προσάρτημα Δ περιλαμβάνει παράδειγμα δελτίου πληροφοριών εξουσιοδότησης ασφαλείας φορέα ([9]). Η απάντηση σε δελτίο πληροφοριών εξουσιοδότησης ασφαλείας φορέα παρέχεται, στο μέτρο του δυνατού, εντός δέκα εργάσιμων ημερών από την ημερομηνία της αίτησης.

9. Εάν κρατικές επιχειρήσεις ή επιχειρήσεις που βρίσκονται υπό κρατικό έλεγχο κράτους μέλους συμμετέχουν σε διαβαθμισμένες συμφωνίες επιδότησης που απαιτούν εξουσιοδότηση ασφαλείας φορέα, και όταν οι εξουσιοδοτήσεις ασφαλείας φορέα δεν εκδίδονται για τις εν λόγω επιχειρήσεις βάσει των εθνικών νομοθετικών διατάξεων, η χορηγούσα αρχή επαληθεύει από την οικεία εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας, μέσω της Αρχής Ασφαλείας της Επιτροπής, αν οι εν λόγω κρατικές επιχειρήσεις είναι σε θέση να χειριστούν ΔΠΕΕ στο απαιτούμενο επίπεδο.

([9]) Άλλα χρησιμοποιούμενα έντυπα είναι δυνατόν να διαφέρουν στη μορφή τους από το παράδειγμα που παρέχεται με τους παρόντες κανόνες εφαρμογής.

10. Εάν απαιτείται εξουσιοδότηση ασφαλείας φορέα για την εκτέλεση διαβαθμισμένης συμφωνίας επιδότησης και εάν, σύμφωνα με τους εθνικούς κανόνες, απαιτείται εξουσιοδότηση ασφαλείας φορέα για την έκδοση εξουσιοδότησης ασφαλείας προσωπικού, η χορηγούσα αρχή επαληθεύει από την οικεία εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας, μέσω της Αρχής Ασφαλείας της Επιτροπής, χρησιμοποιώντας δελτίο πληροφοριών εξουσιοδότησης ασφαλείας φορέα, ότι ο δικαιούχος διαθέτει εξουσιοδότηση ασφαλείας φορέα ή ότι βρίσκεται σε εξέλιξη η διαδικασία έκδοσης εξουσιοδότησης ασφαλείας φορέα. Στην περίπτωση αυτή, η Επιτροπή δεν εκδίδει αιτήσεις για εξουσιοδοτήσεις ασφαλείας προσωπικού με χρήση δελτίου πληροφοριών εξουσιοδότησης ασφαλείας προσωπικού (PSCIS).

Άρθρο 4

Υπεργολαβία σε διαβαθμισμένες συμφωνίες επιδότησης

1. Οι όροι υπό τους οποίους δικαιούχος μπορεί να αναθέτει υπεργολαβικά καθήκοντα δράσης που αφορούν ΔΠΕΕ καθορίζονται στην πρόσκληση υποβολής προτάσεων και στη συμφωνία επιδότησης. Στους όρους αυτούς περιλαμβάνεται η απαίτηση υποβολής όλων των δελτίων πληροφοριών εξουσιοδότησης ασφαλείας προσωπικού μέσω της Αρχής Ασφαλείας της Επιτροπής. Η υπεργολαβική ανάθεση καθηκόντων υπόκειται στην προηγούμενη έγγραφη συναίνεση της χορηγούσας αρχής. Κατά περίπτωση, η υπεργολαβική ανάθεση καθηκόντων συμμορφώνεται με τη βασική πράξη θέσπισης του προγράμματος.

2. Διαβαθμισμένα μέρη των συμφωνιών επιδότησης ανατίθενται υπεργολαβικά μόνο σε οντότητες που έχουν την έδρα τους σε κράτος μέλος ή σε οντότητες που έχουν την έδρα τους σε τρίτη χώρα ή που έχουν συσταθεί από διεθνή οργανισμό, υπό τον όρο ότι η εν λόγω τρίτη χώρα ή ο εν λόγω διεθνής οργανισμός έχει συνάψει συμφωνία για την ασφάλεια των πληροφοριών με την ΕΕ ή έχει προβεί σε διοικητικό διακανονισμό με την Επιτροπή ([10]).

ΚΕΦΑΛΑΙΟ 3

ΧΕΙΡΙΣΜΟΣ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΣΥΜΦΩΝΙΩΝ ΕΠΙΔΟΤΗΣΗΣ

Άρθρο 5

Βασικές αρχές

1. Κατά τη σύναψη διαβαθμισμένης συμφωνίας επιδότησης, η χορηγούσα αρχή, από κοινού με την Αρχή Ασφαλείας της Επιτροπής, διασφαλίζει ότι οι υποχρεώσεις του δικαιούχου όσον αφορά την προστασία των ΔΠΕΕ που θα χρησιμοποιηθούν ή θα παραχθούν κατά την εκτέλεση της συμφωνίας επιδότησης αποτελούν αναπόσπαστο μέρος της συμφωνίας αυτής. Οι προδιαγραφές ασφαλείας της εκάστοτε επιδότησης έχουν τη μορφή εγγράφου θεμάτων ασφαλείας (ΕΘΑ). Υπόδειγμα εγγράφου θεμάτων ασφαλείας παρατίθεται στο παράρτημα ΙΙΙ.

2. Πριν από την υπογραφή διαβαθμισμένης συμφωνίας επιδότησης, η χορηγούσα αρχή εγκρίνει οδηγό διαβάθμισης ασφαλείας (ΟΔΑ) για τα προς εκτέλεση καθήκοντα και τις πληροφορίες που θα παραχθούν κατά την εκτέλεση της συμφωνίας ή, αν συντρέχει περίπτωση, σε επίπεδο προγράμματος ή έργου. Ο οδηγός διαβάθμισης ασφαλείας αποτελεί τμήμα του εγγράφου θεμάτων ασφαλείας.

3. Οι προδιαγραφές ασφαλείας προγράμματος ή έργου έχουν τη μορφή εντολών ασφαλείας προγράμματος (ή έργου) (PSI). Οι εντολές ασφαλείας προγράμματος/έργου μπορούν να συνταχθούν με βάση τις διατάξεις του υποδείγματος εγγράφου θεμάτων ασφαλείας που παρατίθεται στο παράρτημα ΙΙΙ. Οι εντολές ασφαλείας προγράμματος/έργου εκπονούνται από την υπηρεσία της Επιτροπής που διαχειρίζεται το οικείο πρόγραμμα ή έργο, σε στενή συνεργασία με την Αρχή Ασφαλείας της Επιτροπής, και υποβάλλονται προς διατύπωση γνώμης στην ομάδα εμπειρογνωμόνων ασφαλείας της Επιτροπής. Όταν συμφωνία επιδότησης αποτελεί μέρος προγράμματος ή έργου με δικές του εντολές ασφαλείας προγράμματος/έργου, το έγγραφο θεμάτων ασφαλείας της συμφωνίας επιδότησης λαμβάνει απλουστευμένη μορφή και περιλαμβάνει παραπομπή στις διατάξεις για την ασφάλεια που ορίζονται στις εντολές ασφαλείας προγράμματος/έργου του προγράμματος ή του έργου.

4. Εξαιρουμένων των περιπτώσεων που προβλέπονται στο άρθρο 3 παράγραφος 9, η διαβαθμισμένη συμφωνία επιδότησης δεν υπογράφεται προτού η εθνική αρχή ασφαλείας ή η καθορισμένη αρχή ασφαλείας του αιτούντος επιβεβαιώσει την εξουσιοδότηση ασφαλείας φορέα του αιτούντος, ή, όταν η διαβαθμισμένη συμφωνία επιδότησης συνάπτεται με κοινοπραξία, προτού η εθνική αρχή ασφαλείας ή η καθορισμένη αρχή ασφαλείας ενός τουλάχιστον αιτούντος εντός της κοινοπραξίας, ή περισσοτέρων εάν κριθεί αναγκαίο, επιβεβαιώσει την εξουσιοδότηση ασφαλείας φορέα του εν λόγω αιτούντος.

5. Καταρχήν, και εκτός εάν προβλέπεται διαφορετικά σε άλλους σχετικούς κανόνες, η χορηγούσα αρχή θεωρείται φορέας προέλευσης των ΔΠΕΕ που παράγονται κατά την εκτέλεση της συμφωνίας επιδότησης.

([10]) Ο κατάλογος των συμφωνιών που έχει συνάψει η ΕΕ και των διοικητικών διακανονισμών που έχει συνάψει η Ευρωπαϊκή Επιτροπή, βάσει των οποίων είναι δυνατή η ανταλλαγή διαβαθμισμένων πληροφοριών της ΕΕ με τρίτες χώρες και διεθνείς οργανισμούς, διατίθεται στον ιστότοπο της Επιτροπής.

6. Η χορηγούσα αρχή, μέσω της Αρχής Ασφαλείας της Επιτροπής, ενημερώνει τις εθνικές αρχές ασφαλείας και/ή τις καθορισμένες αρχές ασφαλείας όλων των δικαιούχων και υπεργολάβων για τη σύναψη διαβαθμισμένων συμφωνιών επιδότησης ή συμβάσεων υπεργολαβίας και για κάθε τυχόν επέκταση ή πρόωρη λύση των εν λόγω συμφωνιών επιδότησης ή συμβάσεων υπεργολαβίας. Κατάλογος των σχετικών απαιτήσεων ανά χώρα παρατίθεται στο παράρτημα IV.

7. Οι συμφωνίες επιδότησης που σχετίζονται με πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED περιλαμβάνουν ρήτρα για την ασφάλεια η οποία καθιστά τις διατάξεις του παραρτήματος III προσάρτημα Ε δεσμευτικές για τους δικαιούχους. Οι εν λόγω συμφωνίες επιδότησης περιλαμβάνουν έγγραφο θεμάτων ασφαλείας το οποίο καθορίζει τουλάχιστον τις προδιαγραφές για τον χειρισμό πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED, συμπεριλαμβανομένων των πτυχών που αφορούν τη διασφάλιση των πληροφοριών, καθώς και των ειδικών προδιαγραφών που πρέπει να πληρούν οι δικαιούχοι όσον αφορά την πιστοποίηση των οικείων συστημάτων επικοινωνίας και πληροφοριών (CIS) που χειρίζονται πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED.

8. Εάν απαιτείται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις των κρατών μελών, οι εθνικές αρχές ασφαλείας ή καθορισμένες αρχές ασφαλείας διασφαλίζουν ότι οι δικαιούχοι ή οι υπεργολάβοι που υπάγονται στη δικαιοδοσία τους συμμορφώνονται προς τις ισχύουσες διατάξεις που αφορούν την ασφάλεια για την προστασία των πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED και διενεργούν επισκέψεις επαλήθευσης στις εγκαταστάσεις δικαιούχων ή υπεργολάβων που βρίσκονται στο έδαφός τους. Εάν η εθνική αρχή ασφαλείας ή η καθορισμένη αρχή ασφαλείας δεν υπέχει τέτοια υποχρέωση, η χορηγούσα αρχή διασφαλίζει ότι οι δικαιούχοι εφαρμόζουν τις απαιτούμενες διατάξεις για την ασφάλεια που ορίζονται στο παράρτημα III προσάρτημα Ε.

Άρθρο 6

Πρόσβαση του προσωπικού δικαιούχων και υπεργολάβων σε ΔΠΕΕ

1. Η χορηγούσα αρχή διασφαλίζει ότι οι διαβαθμισμένες συμφωνίες επιδότησης περιλαμβάνουν διατάξεις που ορίζουν ότι στα μέλη του προσωπικού των δικαιούχων ή των υπεργολάβων τα οποία, για την εκτέλεση της διαβαθμισμένης συμφωνίας επιδότησης ή σύμβασης υπεργολαβίας, χρειάζονται πρόσβαση σε ΔΠΕΕ η εν λόγω πρόσβαση χορηγείται μόνο εάν:

α) έχει διαπιστωθεί ότι έχουν ανάγκη γνώσης·

β) όσον αφορά τις πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, έχουν υποβληθεί σε έλεγχο ασφαλείας αντίστοιχου επιπέδου από την αρμόδια εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας ή από οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας·

γ) έχουν ενημερωθεί για τους ισχύοντες κανόνες ασφαλείας για την προστασία των ΔΠΕΕ και έχουν αναγνωρίσει τις ευθύνες τους όσον αφορά την προστασία των πληροφοριών αυτών.

2. Κατά περίπτωση, η πρόσβαση σε ΔΠΕΕ συμμορφώνεται επίσης με τη βασική πράξη για τη θέσπιση του προγράμματος και λαμβάνει υπόψη τυχόν πρόσθετες σημάνσεις στον οδηγό διαβάθμισης ασφαλείας.

3. Εάν δικαιούχος ή υπεργολάβος επιθυμεί να προσλάβει υπήκοο τρίτης χώρας σε θέση η οποία απαιτεί πρόσβαση σε ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, αποτελεί ευθύνη του δικαιούχου ή υπεργολάβου να κινήσει τη διαδικασία ελέγχου ασφαλείας του εν λόγω προσώπου, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις που ισχύουν στον τόπο όπου πρόκειται να χορηγηθεί πρόσβαση σε ΔΠΕΕ.

Άρθρο 7

Πρόσβαση εμπειρογνωμόνων που συμμετέχουν σε εξακριβώσεις, επισκοπήσεις ή ελέγχους

1. Όταν συμμετέχουν εξωτερικά πρόσωπα («εμπειρογνώμονες») σε εξακριβώσεις, επισκοπήσεις ή ελέγχους που διενεργούνται από τη χορηγούσα αρχή ή σε διαδικασίες επανεξέτασης επιδόσεων των δικαιούχων για τις οποίες απαιτείται πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, στα πρόσωπα αυτά παρέχεται σύμβαση μόνο αφού υποβληθούν σε έλεγχο ασφαλείας αντίστοιχου επιπέδου από την αρμόδια εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας ή από οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας. Η χορηγούσα αρχή, μέσω της Αρχής Ασφαλείας της Επιτροπής, ελέγχει και, κατά περίπτωση, ζητεί από την εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας να κινήσει τη διαδικασία ελέγχου των εμπειρογνωμόνων τουλάχιστον έξι μήνες πριν από την έναρξη ισχύος των αντίστοιχων συμβάσεων.

2. Πριν προβούν στην υπογραφή της σύμβασής τους, οι εμπειρογνώμονες ενημερώνονται για τους ισχύοντες κανόνες ασφαλείας για την προστασία των ΔΠΕΕ και αναγνωρίζουν τις ευθύνες τους όσον αφορά την προστασία των πληροφοριών αυτών.

ΚΕΦΑΛΑΙΟ 4

ΕΠΙΣΚΕΨΕΙΣ ΣΕ ΣΥΝΑΡΤΗΣΗ ΜΕ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΦΩΝΙΕΣ ΕΠΙΔΟΤΗΣΗΣ

Άρθρο 8

Βασικές αρχές

1. Όταν η χορηγούσα αρχή, οι εμπειρογνώμονες, οι δικαιούχοι ή οι υπεργολάβοι χρειάζονται πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET στις εκατέρωθεν εγκαταστάσεις τους στο πλαίσιο της εκτέλεσης της διαβαθμισμένης συμφωνίας επιδότησης, διοργανώνονται επισκέψεις σε συνεργασία με τις οικείες εθνικές αρχές ασφαλείας ή καθορισμένες αρχές ασφαλείας ή οποιεσδήποτε άλλες αρμόδιες αρχές ασφαλείας.

2. Οι επισκέψεις της παραγράφου 1 υπόκεινται στις ακόλουθες απαιτήσεις:

α) η επίσκεψη έχει επίσημο σκοπό που σχετίζεται με τη διαβαθμισμένη συμφωνία επιδότησης·

β) κάθε επισκέπτης διαθέτει εξουσιοδότηση ασφαλείας προσωπικού του απαιτούμενου επιπέδου και έχει ανάγκη γνώσης προκειμένου να του χορηγηθεί πρόσβαση σε ΔΠΕΕ που έχουν χρησιμοποιηθεί ή παραχθεί κατά την εκτέλεση της διαβαθμισμένης συμφωνίας επιδότησης.

Άρθρο 9

Αιτήσεις επίσκεψης

1. Οι επισκέψεις από δικαιούχους ή υπεργολάβους στις εγκαταστάσεις άλλων δικαιούχων ή υπεργολάβων ή σε εγκαταστάσεις της χορηγούσας αρχής, οι οποίες περιλαμβάνουν πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET διεκπεραιώνονται σύμφωνα με την ακόλουθη διαδικασία:

α) ο υπεύθυνος ασφαλείας της εγκατάστασης αποστολής του επισκέπτη συμπληρώνει όλα τα σχετικά σημεία του εντύπου αίτησης επίσκεψης (RFV) και υποβάλλει την αίτηση στην εθνική αρχή ασφαλείας ή στην καθορισμένη αρχή ασφαλείας της εγκατάστασης. Υπόδειγμα εντύπου αίτησης επίσκεψης παρατίθεται στο παράρτημα III προσάρτημα Γ·

β) η εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας της εγκατάστασης αποστολής πρέπει να επιβεβαιώσει την εξουσιοδότηση ασφαλείας προσωπικού του επισκέπτη προτού υποβάλει την αίτηση επίσκεψης στην εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας της εγκατάστασης υποδοχής (ή στην Αρχή Ασφαλείας της Επιτροπής, εάν η επίσκεψη πρόκειται να πραγματοποιηθεί στις εγκαταστάσεις της χορηγούσας αρχής)·

γ) στη συνέχεια, ο υπεύθυνος ασφαλείας της εγκατάστασης αποστολής λαμβάνει από την εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας του την απάντηση της εθνικής αρχής ασφαλείας ή καθορισμένης αρχής ασφαλείας της εγκατάστασης υποδοχής (ή της Αρχής Ασφαλείας της Επιτροπής), με την οποία η αίτηση επίσκεψης είτε γίνεται δεκτή είτε απορρίπτεται·

δ) η αίτηση επίσκεψης θεωρείται ότι έχει γίνει δεκτή εάν δεν διατυπωθούν αντιρρήσεις έως πέντε εργάσιμες ημέρες πριν από την ημερομηνία της επίσκεψης.

2. Οι επισκέψεις από υπαλλήλους της χορηγούσας αρχής ή εμπειρογνώμονες ή ελεγκτές στις εγκαταστάσεις δικαιούχων ή υπεργολάβων οι οποίες περιλαμβάνουν πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET διεκπεραιώνονται σύμφωνα με την ακόλουθη διαδικασία:

α) ο επισκέπτης συμπληρώνει όλα τα σχετικά σημεία του εντύπου αίτησης επίσκεψης και το υποβάλλει στην Αρχή Ασφαλείας της Επιτροπής·

β) η Αρχή Ασφαλείας της Επιτροπής επιβεβαιώνει την εξουσιοδότηση ασφαλείας προσωπικού του επισκέπτη προτού υποβάλει την αίτηση επίσκεψης στην εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας της εγκατάστασης υποδοχής·

γ) η Αρχή Ασφαλείας της Επιτροπής λαμβάνει απάντηση από την εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας της εγκατάστασης υποδοχής, με την οποία η αίτηση επίσκεψης είτε γίνεται δεκτή είτε απορρίπτεται·

δ) η αίτηση επίσκεψης θεωρείται ότι έχει γίνει δεκτή εάν δεν διατυπωθούν αντιρρήσεις έως πέντε εργάσιμες ημέρες πριν από την ημερομηνία της επίσκεψης.

3. Η αίτηση επίσκεψης μπορεί να καλύπτει είτε μία μόνο επίσκεψη είτε επαναλαμβανόμενες επισκέψεις. Στην περίπτωση επαναλαμβανόμενων επισκέψεων, η αίτηση επίσκεψης μπορεί να έχει διάρκεια ισχύος έως ένα έτος από τη ζητούμενη ημερομηνία έναρξης.

4. Η διάρκεια ισχύος οποιασδήποτε αίτησης επίσκεψης δεν υπερβαίνει τη διάρκεια ισχύος της εξουσιοδότησης ασφαλείας προσωπικού του επισκέπτη.

5. Κατά γενικό κανόνα, η αίτηση επίσκεψης θα πρέπει να υποβάλλεται στην αρμόδια αρχή ασφαλείας της εγκατάστασης υποδοχής το αργότερο 15 εργάσιμες ημέρες πριν από την ημερομηνία της επίσκεψης.

Άρθρο 10

Διαδικασίες επισκέψεων

1. Προτού επιτρέψει σε επισκέπτη πρόσβαση σε ΔΠΕΕ, το γραφείο ασφαλείας της εγκατάστασης υποδοχής εφαρμόζει όλες τις διαδικασίες και τους κανόνες ασφαλείας που αφορούν επισκέψεις και που έχουν καθοριστεί από την εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας του.

2. Οι επισκέπτες αποδεικνύουν την ταυτότητά τους κατά την άφιξή τους στην εγκατάσταση υποδοχής, με την επίδειξη ισχύοντος δελτίου ταυτότητας ή διαβατηρίου. Τα εν λόγω στοιχεία ταυτοποίησης αντιστοιχούν στα στοιχεία που έχουν παρασχεθεί με την αίτηση επίσκεψης.

3. Η εγκατάσταση υποδοχής εξασφαλίζει ότι τηρούνται αρχεία για όλους τους επισκέπτες, στα οποία καταγράφονται το όνομά τους, ο οργανισμός τον οποίο εκπροσωπούν, η ημερομηνία λήξης της εξουσιοδότησης ασφαλείας προσωπικού, η ημερομηνία της επίσκεψης και τα ονόματα των προσώπων τα οποία οι επισκέπτες επισκέφθηκαν. Τα εν λόγω αρχεία φυλάσσονται για διάστημα τουλάχιστον πέντε ετών, ή για μεγαλύτερο διάστημα εάν αυτό απαιτείται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις της χώρας στην οποία βρίσκεται η εγκατάσταση υποδοχής.

Άρθρο 11

Απευθείας διοργάνωση επισκέψεων

1. Στο πλαίσιο συγκεκριμένων έργων, οι αρμόδιες εθνικές αρχές ασφαλείας ή καθορισμένες αρχές ασφαλείας και η Αρχή Ασφαλείας της Επιτροπής μπορούν να συμφωνήσουν διαδικασία βάσει της οποίας οι επισκέψεις για συγκεκριμένη διαβαθμισμένη συμφωνία επιδότησης μπορούν να διοργανώνονται απευθείας μεταξύ του υπευθύνου ασφαλείας του επισκέπτη και του υπευθύνου ασφαλείας της εγκατάστασης στην οποία πρόκειται να πραγματοποιηθεί η επίσκεψη. Υπόδειγμα του εντύπου που πρέπει να χρησιμοποιείται για τον σκοπό αυτόν παρατίθεται στο παράρτημα ΙΙΙ προσάρτημα Γ. Η εν λόγω κατ' εξαίρεση διαδικασία καθορίζεται στις εντολές ασφαλείας προγράμματος/έργου ή σε άλλες ειδικές ρυθμίσεις. Στις περιπτώσεις αυτές, οι διαδικασίες του άρθρου 9 και του άρθρου 10 παράγραφος 1 δεν εφαρμόζονται.

2. Οι επισκέψεις που περιλαμβάνουν πρόσβαση σε πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED διοργανώνονται απευθείας μεταξύ της αποστέλλουσας οντότητας και της οντότητας προορισμού, χωρίς να χρειάζεται να τηρηθούν οι διαδικασίες του άρθρου 9 και του άρθρου 10 παράγραφος 1.

ΚΕΦΑΛΑΙΟ 5

ΔΙΑΒΙΒΑΣΗ ΚΑΙ ΜΕΤΑΦΟΡΑ ΔΠΕΕ ΚΑΤΑ ΤΗΝ ΕΚΤΕΛΕΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΣΥΜΦΩΝΙΩΝ ΕΠΙΔΟΤΗΣΗΣ

Άρθρο 12

Βασικές αρχές

Η χορηγούσα αρχή διασφαλίζει ότι όλες οι αποφάσεις που αφορούν διαβίβαση και μεταφορά ΔΠΕΕ συνάδουν με την απόφαση (ΕΕ, Ευρατόμ) 2015/444 και τους κανόνες εφαρμογής της, καθώς και με τους όρους της διαβαθμισμένης συμφωνίας επιδότησης, συμπεριλαμβανομένης της συναίνεσης του φορέα προέλευσης.

Άρθρο 13

Ηλεκτρονικός χειρισμός

1. Ο ηλεκτρονικός χειρισμός και η ηλεκτρονική διαβίβαση ΔΠΕΕ πραγματοποιούνται σύμφωνα με τα κεφάλαια 5 και 6 της απόφασης (ΕΕ, Ευρατόμ) 2015/444 και τους κανόνες εφαρμογής της.

Τα συστήματα επικοινωνίας και πληροφοριών που ανήκουν σε δικαιούχο και χρησιμοποιούνται για τον χειρισμό ΔΠΕΕ για την εκτέλεση της συμφωνίας επιδότησης (CIS του δικαιούχου) υπόκεινται σε πιστοποίηση από την αρμόδια αρχή πιστοποίησης της ασφάλειας (ΑΠΑ). Κάθε ηλεκτρονική διαβίβαση ΔΠΕΕ προστατεύεται με κρυπτογραφικά προϊόντα που έχουν εγκριθεί σύμφωνα με το άρθρο 36 παράγραφος 4 της απόφασης (ΕΕ, Ευρατόμ) 2015/444. Εφαρμόζονται μέτρα ασφαλείας TEMPEST σύμφωνα με το άρθρο 36 παράγραφος 6 της εν λόγω απόφασης.

2. Η πιστοποίηση ασφαλείας των CIS του δικαιούχου που χειρίζονται ΔΠΕΕ επιπέδου RESTREINT UE/EU RESTRICTED και κάθε τυχόν διασύνδεσής τους μπορεί να ανατίθεται στον υπεύθυνο ασφαλείας του δικαιούχου, εάν αυτό επιτρέπεται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις. Εάν το καθήκον αυτό ανατεθεί στον υπεύθυνο ασφαλείας, ο δικαιούχος είναι υπεύθυνος για την εφαρμογή των ελάχιστων προδιαγραφών ασφαλείας που περιγράφονται στο έγγραφο θεμάτων ασφαλείας κατά τον χειρισμό πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED στα CIS του. Ωστόσο, οι αρμόδιες εθνικές αρχές ασφαλείας ή καθορισμένες αρχές ασφαλείας και αρχές πιστοποίησης της ασφάλειας διατηρούν την ευθύνη για την προστασία των πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED τις οποίες χειρίζεται ο δικαιούχος, καθώς και το δικαίωμα να επιθεωρούν τα μέτρα ασφαλείας που εφαρμόζει ο δικαιούχος. Επιπροσθέτως, ο δικαιούχος υποβάλλει στη χορηγούσα αρχή και, εάν απαιτείται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις, στην αρμόδια εθνική αρχή πιστοποίησης της ασφάλειας δήλωση συμμόρφωσης με την οποία βεβαιώνεται ότι τα CIS του δικαιούχου και οι σχετικές διασυνδέσεις έχουν πιστοποιηθεί για τον χειρισμό ΔΠΕΕ επιπέδου RESTREINT UE/EU RESTRICTED ([11]).

Άρθρο 14

Μεταφορά από παρόχους εμπορικών υπηρεσιών ταχυμεταφοράς

Η μεταφορά ΔΠΕΕ από παρόχους εμπορικών υπηρεσιών ταχυμεταφοράς πραγματοποιείται σε συμμόρφωση προς τις συναφείς διατάξεις της απόφασης (ΕΕ, Ευρατόμ) 2019/1962 της Επιτροπής ([12]) σχετικά με τους κανόνες εφαρμογής για τον χειρισμό πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED και της απόφασης (ΕΕ, Ευρατόμ) 2019/1961 της Επιτροπής ([13]) σχετικά με τους κανόνες εφαρμογής για τον χειρισμό πληροφοριών με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET.

Άρθρο 15

Ιδιόχειρη μεταφορά

1. Η ιδιόχειρη μεταφορά διαβαθμισμένων πληροφοριών υπόκειται σε αυστηρές προδιαγραφές ασφαλείας.

2. Πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED μπορούν να μεταφέρονται ιδιοχείρως από προσωπικό του δικαιούχου εντός της ΕΕ, υπό την προϋπόθεση ότι πληρούνται οι ακόλουθες απαιτήσεις:

α) ο φάκελος ή η συσκευασία που χρησιμοποιείται είναι αδιαφανής και δεν φέρει καμία ένδειξη για τη διαβάθμιση του περιεχομένου του/της·

β) οι διαβαθμισμένες πληροφορίες παραμένουν συνεχώς στην κατοχή του κομιστή τους·

γ) ο φάκελος ή η συσκευασία δεν ανοίγεται καθ' οδόν.

3. Όσον αφορά τις πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET, η ιδιόχειρη μεταφορά από προσωπικό του δικαιούχου εντός κράτους μέλους διοργανώνεται εκ των προτέρων μεταξύ της αποστέλλουσας οντότητας και της οντότητας προορισμού. Η αρχή ή εγκατάσταση αποστολής ενημερώνει την αρχή ή εγκατάσταση προορισμού για τις λεπτομέρειες της αποστολής, συμπεριλαμβανομένων των στοιχείων αναφοράς, της διαβάθμισης, της αναμενόμενης ώρας άφιξης και του ονόματος του μεταφορέα. Η εν λόγω ιδιόχειρη μεταφορά επιτρέπεται, υπό την προϋπόθεση ότι πληρούνται οι ακόλουθες απαιτήσεις:

α) οι διαβαθμισμένες πληροφορίες μεταφέρονται σε διπλό φάκελο ή διπλή συσκευασία·

β) ο εξωτερικός φάκελος ή η εξωτερική συσκευασία είναι σφραγισμένος/-η και δεν φέρει καμία ένδειξη για τη διαβάθμιση του περιεχομένου του/της, ενώ ο εσωτερικός φάκελος φέρει το επίπεδο διαβάθμισης·

γ) οι ΔΠΕΕ παραμένουν συνεχώς στην κατοχή του κομιστή τους·

δ) ο φάκελος ή η συσκευασία δεν ανοίγεται καθ' οδόν·

ε) ο φάκελος ή η συσκευασία μεταφέρεται σε χαρτοφύλακα ή παρόμοιο εγκεκριμένο περιέκτη ο οποίος μπορεί να κλειδωθεί και ο οποίος έχει μέγεθος και βάρος τα οποία επιτρέπουν τη διαρκή διατήρησή του στην προσωπική κατοχή του κομιστή και δεν επιβάλλουν να παραδίδεται ως παραδιδόμενη αποσκευή·

στ) ο μεταφορέας είναι εφοδιασμένος με πιστοποιητικό αγγελιαφόρου που έχει εκδοθεί από την αρμόδια αρχή ασφαλείας και που επιτρέπει στον μεταφορέα να φέρει το διαβαθμισμένο φορτίο όπως έχει προσδιοριστεί.

([11]) Οι ελάχιστες προδιαγραφές για τα συστήματα επικοινωνίας και πληροφοριών που χειρίζονται ΔΠΕΕ επιπέδου RESTREINT UE/EU RESTRICTED καθορίζονται στο παράρτημα ΙΙΙ προσάρτημα Ε.

([12]) Απόφαση (ΕΕ, Ευρατόμ) 2019/1962 της Επιτροπής, της 17ης Οκτωβρίου 2019, σχετικά με τους κανόνες εφαρμογής για τον χειρισμό πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED (ΕΕ L 311 της 2.12.2019, σ. 21).

([13]) Απόφαση (ΕΕ, Ευρατόμ) 2019/1961 της Επιτροπής, της 17ης Οκτωβρίου 2019, σχετικά με τους κανόνες εφαρμογής για τον χειρισμό πληροφοριών με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET (ΕΕ L 311 της 2.12.2019, σ. 1).

4. Για την ιδιόχειρη μεταφορά, από προσωπικό του δικαιούχου, πληροφοριών με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET από ένα κράτος μέλος σε άλλο, εφαρμόζονται οι ακόλουθοι πρόσθετοι κανόνες:

α) ο μεταφορέας είναι υπεύθυνος για την ασφαλή φύλαξη του διαβαθμισμένου υλικού έως ότου παραδοθεί στον παραλήπτη·

β) σε περίπτωση παραβίασης της ασφάλειας, η εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας του αποστολέα μπορεί να ζητήσει από τις αρχές της χώρας στην οποία επήλθε η παραβίαση να διενεργήσουν έρευνα, να της κοινοποιήσουν τα πορίσματά τους και να λάβουν τα δέοντα νομικά ή άλλα μέτρα·

γ) ο μεταφορέας έχει ενημερωθεί για όλες τις υποχρεώσεις ασφαλείας που πρέπει να τηρούνται κατά τη διάρκεια της μεταφοράς και έχει υπογράψει κατάλληλη σχετική δήλωση·

δ) οι οδηγίες για τον μεταφορέα επισυνάπτονται στο πιστοποιητικό αγγελιαφόρου·

ε) στον μεταφορέα έχει παρασχεθεί περιγραφή του φορτίου και δρομολόγιο·

στ) τα έγγραφα επιστρέφονται στην εθνική αρχή ασφαλείας ή καθορισμένη αρχή ασφαλείας έκδοσης κατά την ολοκλήρωση του/των ταξιδιού/-ών ή φυλάσσονται από τον παραλήπτη για σκοπούς παρακολούθησης·

ζ) εάν οι τελωνειακές αρχές, οι αρχές μετανάστευσης ή η συνοριακή αστυνομία ζητήσουν να εξετάσουν και να επιθεωρήσουν το φορτίο, τους επιτρέπεται να ανοίξουν και να παρατηρήσουν επαρκή τμήματα του φορτίου ώστε να διαπιστώσουν ότι δεν περιέχει υλικό πέραν αυτού που δηλώνεται·

η) οι τελωνειακές αρχές θα πρέπει να καλούνται να σεβαστούν το δημόσιο κύρος των εγγράφων αποστολής και των εγγράφων εξουσιοδότησης που φέρει ο μεταφορέας.

Εάν το φορτίο ανοιχθεί από τις τελωνειακές αρχές, το άνοιγμα θα πρέπει να πραγματοποιηθεί εκτός του οπτικού πεδίου μη εξουσιοδοτημένων προσώπων και, κατά το δυνατόν, παρουσία του μεταφορέα. Ο μεταφορέας ζητεί να επανασυσκευασθεί το φορτίο και ζητεί από τις αρχές που διενεργούν τον έλεγχο να επανασφραγίσουν το φορτίο και να επιβεβαιώσουν εγγράφως ότι το φορτίο ανοίχθηκε από αυτές.

5. Η ιδιόχειρη μεταφορά, από προσωπικό του δικαιούχου, πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET σε τρίτη χώρα ή σε διεθνή οργανισμό υπόκειται στις διατάξεις της συμφωνίας για την ασφάλεια των πληροφοριών ή του διοικητικού διακανονισμού που έχει συναφθεί μεταξύ της Ένωσης ή της Επιτροπής και της εν λόγω τρίτης χώρας ή του εν λόγω διεθνούς οργανισμού, αντίστοιχα.

ΚΕΦΑΛΑΙΟ 6

ΣΧΕΔΙΑΣΜΟΣ ΣΥΝΕΧΙΣΗΣ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

Άρθρο 16

Σχέδια έκτακτης ανάγκης και επανορθωτικά μέτρα

Η χορηγούσα αρχή διασφαλίζει ότι η διαβαθμισμένη συμφωνία επιδότησης επιβάλλει στους δικαιούχους την υποχρέωση να εκπονήσουν επιχειρησιακά σχέδια έκτακτης ανάγκης (BCP) για την προστασία των ΔΠΕΕ που αποτελούν αντικείμενο χειρισμού στο πλαίσιο της διαβαθμισμένης συμφωνίας επιδότησης σε καταστάσεις έκτακτης ανάγκης, καθώς και να θεσπίσει, στο πλαίσιο του σχεδιασμού συνέχισης των δραστηριοτήτων, προληπτικά και επανορθωτικά μέτρα με σκοπό την ελαχιστοποίηση του αντίκτυπου ενδεχόμενων συμβάντων στον χειρισμό και την αποθήκευση ΔΠΕΕ. Οι δικαιούχοι διαβεβαιώνουν τη χορηγούσα αρχή ότι διαθέτουν τα οικεία επιχειρησιακά σχέδια έκτακτης ανάγκης.

Άρθρο 17

Έναρξη ισχύος

Η παρούσα απόφαση αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Βρυξέλλες, 10 Φεβρουαρίου 2021.

Για την Επιτροπή,
Εξ ονόματος του Προέδρου
Johannes HAHN
Μέλος της Επιτροπής

ΠΑΡΑΡΤΗΜΑ Ι

ΤΥΠΟΠΟΙΗΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΣΤΗΝ ΠΡΟΣΚΛΗΣΗ ΥΠΟΒΟΛΗΣ ΠΡΟΤΑΣΕΩΝ

(πρέπει να προσαρμόζεται στην εκάστοτε χρησιμοποιούμενη πρόσκληση)

Ασφάλεια

Τα έργα που περιλαμβάνουν διαβαθμισμένες πληροφορίες της ΕΕ πρέπει να υποβάλλονται σε έλεγχο ασφαλείας προκειμένου να εγκριθεί η χρηματοδότησή τους και μπορεί να προβλέπονται για αυτά ειδικοί κανόνες ασφαλείας [οι οποίοι αναλύονται σε έγγραφο θεμάτων ασφαλείας (ΕΘΑ) το οποίο επισυνάπτεται στη συμφωνία επιδότησης].

Οι κανόνες αυτοί (οι οποίοι διέπονται από την απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής ([1]) και/ή από εθνικούς κανόνες) προβλέπουν, για παράδειγμα, τα εξής:

— **δεν** επιτρέπεται η χρηματοδότηση έργων που περιλαμβάνουν πληροφορίες με διαβάθμιση TRES SECRET UE/EU TOP SECRET (ή ισοδύναμη)·

— οι διαβαθμισμένες πληροφορίες πρέπει να επισημαίνονται σύμφωνα με τις εφαρμοστέες οδηγίες ασφαλείας που περιλαμβάνονται στο έγγραφο θεμάτων ασφαλείας·

— πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή ανώτερη (και RESTREINT UE/EU RESTRICTED εάν απαιτείται από τους εθνικούς κανόνες) μπορεί:

  — να παράγονται ή να χορηγείται πρόσβαση σε αυτές μόνο σε εγκαταστάσεις που έχουν λάβει εξουσιοδότηση ασφαλείας φορέα από την αρμόδια εθνική αρχή ασφαλείας (ΕΑΑ), σύμφωνα με τους εθνικούς κανόνες·

  — να αποτελούν αντικείμενο χειρισμού μόνο σε χώρο ασφαλείας πιστοποιημένο από την αρμόδια ΕΑΑ·

  — να χορηγείται πρόσβαση σε αυτές και να αποτελούν αντικείμενο χειρισμού μόνο από πρόσωπα με έγκυρη εξουσιοδότηση ασφαλείας προσωπικού (ΕΑΠ) και ανάγκη γνώσης·

— με το πέρας της επιδότησης, οι διαβαθμισμένες πληροφορίες πρέπει είτε να επιστρέφονται ή να συνεχίσουν να προστατεύονται σύμφωνα με τους εφαρμοστέους κανόνες·

— καθήκοντα δράσης που περιλαμβάνουν διαβαθμισμένες πληροφορίες της ΕΕ (ΔΠΕΕ) μπορούν να ανατίθενται υπεργολαβικά μόνο με προηγούμενη έγγραφη συναίνεση της χορηγούσας αρχής και μόνο σε οντότητες που έχουν την έδρα τους σε κράτος μέλος της ΕΕ ή τρίτη χώρα που έχει συνάψει συμφωνία για την ασφάλεια των πληροφοριών με την ΕΕ (ή διοικητικό διακανονισμό με την Επιτροπή)·

— για την κοινοποίηση ΔΠΕΕ σε τρίτους απαιτείται προηγούμενη έγγραφη συναίνεση της χορηγούσας αρχής.

Επισημαίνεται ότι, ανάλογα με το είδος της δραστηριότητας, η εξουσιοδότηση ασφαλείας φορέα ενδέχεται να πρέπει να χορηγηθεί πριν από την υπογραφή της συμφωνίας επιδότησης. Η χορηγούσα αρχή θα αξιολογεί τις ανάγκες για εξουσιοδοτήσεις σε κάθε περίπτωση και θα καθορίζει την ημερομηνία έκδοσής τους στο στάδιο προετοιμασίας της επιδότησης. Επισημαίνεται ότι σε **καμία περίπτωση** δεν είναι δυνατή η υπογραφή συμφωνίας επιδότησης εάν τουλάχιστον ένας από τους δικαιούχους κοινοπραξίας δεν διαθέτει εξουσιοδότηση ασφαλείας φορέα.

Στη συμφωνία επιδότησης μπορούν να προστεθούν περαιτέρω συστάσεις για την ασφάλεια με τη μορφή παραδοτέων για την ασφάλεια (*π.χ. δημιουργία συμβουλευτικής ομάδας για την ασφάλεια, περιορισμένο επίπεδο λεπτομέρειας, χρήση υποθετικών σεναρίων, απαγόρευση χρήσης διαβαθμισμένων πληροφοριών* κ.λπ.).

Οι δικαιούχοι πρέπει να διασφαλίζουν ότι τα έργα τους δεν υπόκεινται σε προδιαγραφές ασφαλείας κράτους μέλους / τρίτης χώρας που θα μπορούσαν να επηρεάσουν την εκτέλεσή τους ή να αμφισβητήσουν τη χορήγηση της επιδότησης (*π.χ. τεχνολογικοί περιορισμοί, εθνική διαβάθμιση ασφαλείας* κ.λπ.). Η χορηγούσα αρχή πρέπει να ενημερώνεται αμέσως για κάθε πιθανό ζήτημα ασφαλείας.

[πρόσθετη ΕΠΙΛΟΓΗ για τις εταιρικές σχέσεις-πλαίσια: Για τις εταιρικές σχέσεις-πλαίσια, τόσο οι αιτήσεις για τις εταιρικές σχέσεις-πλαίσια όσο και οι αιτήσεις για επιδότηση ενδέχεται να πρέπει να υποβάλλονται σε έλεγχο ασφαλείας.]

([1]) Βλ. απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 72 της 17.3.2015, σ. 53).

ΠΑΡΑΡΤΗΜΑ II

ΤΥΠΟΠΟΙΗΜΕΝΕΣ ΡΗΤΡΕΣ ΣΥΜΦΩΝΙΑΣ ΕΠΙΔΟΤΗΣΗΣ

(πρέπει να προσαρμόζεται στην εκάστοτε χρησιμοποιούμενη συμφωνία επιδότησης)

13.2 Ασφάλεια – Διαβαθμισμένες πληροφορίες

Τα μέρη πρέπει να χειρίζονται τις διαβαθμισμένες πληροφορίες (της ΕΕ ή εθνικές) σύμφωνα με το εφαρμοστέο ενωσιακό ή εθνικό δίκαιο για τις διαβαθμισμένες πληροφορίες [ειδικότερα την απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής ([1]) και τους κανόνες εφαρμογής της].

Ειδικοί κανόνες για την ασφάλεια (εάν υπάρχουν) παρατίθενται στο παράρτημα 5.

ΠΑΡΑΡΤΗΜΑ 5

Ασφάλεια – Διαβαθμισμένες πληροφορίες της ΕΕ

[ΕΠΙΛΟΓΗ για δράσεις με διαβαθμισμένες πληροφορίες της ΕΕ (τυποποιημένη): Εάν η δράση συνεπάγεται τη χρήση ή την παραγωγή διαβαθμισμένων πληροφοριών της ΕΕ, οι πληροφορίες αυτές πρέπει να αντιμετωπίζονται σύμφωνα με τον οδηγό διαβάθμισης ασφαλείας (ΟΔΑ) και το έγγραφο θεμάτων ασφαλείας (ΕΘΑ) όπως ορίζεται στο παράρτημα 1, καθώς και με την απόφαση (ΕΕ, Ευρατόμ) 2015/444 και τους κανόνες εφαρμογής της, έως ότου αποχαρακτηριστούν.

Παραδοτέα που περιέχουν διαβαθμισμένες πληροφορίες της ΕΕ πρέπει να υποβάλλονται σύμφωνα με τις ειδικές διαδικασίες που έχουν συμφωνηθεί με τη χορηγούσα αρχή.

Καθήκοντα δράσης που περιλαμβάνουν διαβαθμισμένες πληροφορίες της ΕΕ μπορούν να ανατίθενται υπεργολαβικά μόνο με προηγούμενη ρητή έγγραφη συναίνεση της χορηγούσας αρχής και μόνο σε οντότητες που έχουν την έδρα τους σε κράτος μέλος της ΕΕ ή τρίτη χώρα που έχει συνάψει συμφωνία για την ασφάλεια των πληροφοριών με την ΕΕ (ή διοικητικό διακανονισμό με την Επιτροπή).

Διαβαθμισμένες πληροφορίες της ΕΕ δεν πρέπει να κοινοποιούνται σε τρίτους (συμπεριλαμβανομένων των συμμετεχόντων στην υλοποίηση της δράσης) χωρίς την προηγούμενη ρητή έγγραφη συναίνεση της χορηγούσας αρχής.]

([1]) Απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 72 της 17.3.2015, σ. 53).

ΠΑΡΑΡΤΗΜΑ III

[Παράρτημα IV (της ……)]

ΕΓΓΡΑΦΟ ΘΕΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ (ΕΘΑ) ([1])

[Υπόδειγμα]

([1]) Το παρόν υπόδειγμα ΕΘΑ αφορά τις περιπτώσεις στις οποίες η Επιτροπή θεωρείται φορέας προέλευσης των διαβαθμισμένων πληροφοριών που παράγονται ή αποτελούν αντικείμενο χειρισμού για την εκτέλεση της συμφωνίας επιδότησης. Στις περιπτώσεις στις οποίες ο φορέας προέλευσης των διαβαθμισμένων πληροφοριών που παράγονται ή αποτελούν αντικείμενο χειρισμού για την εκτέλεση της συμφωνίας επιδότησης δεν είναι η Επιτροπή, και εφόσον έχει δημιουργηθεί ειδικό πλαίσιο ασφαλείας από τα κράτη μέλη που συμμετέχουν στη συμφωνία επιδότησης, μπορούν να χρησιμοποιούνται άλλα υποδείγματα ΕΘΑ.

Προσάρτημα Α

ΠΡΟΔΙΑΓΡΑΦΕΣ ΑΣΦΑΛΕΙΑΣ

Η χορηγούσα αρχή πρέπει να συμπεριλάβει τις ακόλουθες προδιαγραφές ασφαλείας στο έγγραφο θεμάτων ασφαλείας (ΕΘΑ). Ορισμένες ρήτρες ενδέχεται να μην αρμόζουν στη συμφωνία επιδότησης. Οι εν λόγω ρήτρες παρουσιάζονται σε αγκύλες.

Ο κατάλογος των ρητρών δεν είναι εξαντλητικός. Μπορούν να προστεθούν και άλλες ρήτρες, ανάλογα με τη φύση της διαβαθμισμένης συμφωνίας επιδότησης.

ΓΕΝΙΚΟΙ ΟΡΟΙ [*Σημ.: ισχύουν για όλες τις διαβαθμισμένες συμφωνίες επιδότησης*]

1. Το παρόν έγγραφο θεμάτων ασφαλείας (ΕΘΑ) αποτελεί αναπόσπαστο μέρος της διαβαθμισμένης συμφωνίας επιδότησης [ή σύμβασης υπεργολαβίας] και περιγράφει τις σχετιζόμενες με τη συμφωνία επιδότησης προδιαγραφές ασφαλείας. Μη τήρηση των εν λόγω προδιαγραφών μπορεί να συνιστά επαρκή λόγο καταγγελίας της συμφωνίας επιδότησης.

2. Οι δικαιούχοι της επιδότησης υπόκεινται σε όλες τις υποχρεώσεις που καθορίζονται στην απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής ([2]) (στο εξής: απόφαση 2015/444) και στους κανόνες εφαρμογής της ([3]). Εάν ο δικαιούχος της επιδότησης αντιμετωπίζει πρόβλημα σε σχέση με την εφαρμογή του εφαρμοστέου νομικού πλαισίου σε ένα κράτος μέλος, πρέπει να το αναφέρει στην Αρχή Ασφαλείας της Επιτροπής και στην εθνική αρχή ασφαλείας (ΕΑΑ) ή την καθορισμένη αρχή ασφαλείας (ΚΑΑ).

3. Οι διαβαθμισμένες πληροφορίες που παράγονται κατά την εκτέλεση της συμφωνίας επιδότησης πρέπει να επισημαίνονται ως διαβαθμισμένες πληροφορίες της ΕΕ (ΔΠΕΕ) σε επίπεδο διαβάθμισης ασφαλείας, όπως καθορίζεται στον οδηγό διαβάθμισης ασφαλείας (ΟΔΑ) του προσαρτήματος Β του παρόντος εγγράφου. Απόκλιση από το επίπεδο διαβάθμισης ασφαλείας που καθορίζεται από τον οδηγό διαβάθμισης ασφαλείας επιτρέπεται μόνο με την έγγραφη συναίνεση της χορηγούσας αρχής.

4. Τα δικαιώματα του φορέα προέλευσης οποιωνδήποτε ΔΠΕΕ δημιουργηθούν και αποτελέσουν αντικείμενο χειρισμού για την εκτέλεση της διαβαθμισμένης συμφωνίας επιδότησης ασκούνται από την Επιτροπή, ως χορηγούσα αρχή.

5. Χωρίς την έγγραφη συναίνεση της χορηγούσας αρχής, ο δικαιούχος ή υπεργολάβος δεν πρέπει να κάνει χρήση οποιασδήποτε πληροφορίας ή υλικού που παρασχέθηκε από τη χορηγούσα αρχή ή που παρήχθη για λογαριασμό της χορηγούσας αρχής για οποιονδήποτε σκοπό πέραν αυτών της συμφωνίας επιδότησης.

6. Στην περίπτωση που απαιτείται εξουσιοδότηση ασφαλείας φορέα (FSC) για την εκτέλεση της συμφωνίας επιδότησης, ο δικαιούχος πρέπει να ζητήσει από τη χορηγούσα αρχή να διεκπεραιώσει την αίτηση για FSC.

7. Ο δικαιούχος πρέπει να διερευνά όλες τις παραβιάσεις ασφαλείας που σχετίζονται με ΔΠΕΕ και να τις αναφέρει στη χορηγούσα αρχή το συντομότερο πρακτικά δυνατόν. Ο δικαιούχος ή υπεργολάβος πρέπει να γνωστοποιεί αμέσως στην αρμόδια ΕΑΑ ή ΚΑΑ, και, εφόσον το επιτρέπουν οι εθνικές νομοθετικές και κανονιστικές διατάξεις, στην Αρχή Ασφαλείας της Επιτροπής, όλες τις περιπτώσεις για τις οποίες είναι γνωστό ή υπάρχουν εύλογες υπόνοιες ότι ΔΠΕΕ που παρασχέθηκαν ή παρήχθησαν σύμφωνα με τη συμφωνία επιδότησης απωλέσθηκαν ή κοινοποιήθηκαν σε μη εξουσιοδοτημένα πρόσωπα.

([2]) Απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 72 της 17.3.2015, σ. 53).

([3]) Η χορηγούσα αρχή θα πρέπει να εισαγάγει τις παραπομπές αφού εκδοθούν οι κανόνες εφαρμογής.

8. Μετά τη λύση της συμφωνίας επιδότησης, ο δικαιούχος ή υπεργολάβος πρέπει να επιστρέψει το συντομότερο δυνατόν στη χορηγούσα αρχή τις ΔΠΕΕ που έχει στην κατοχή του. Εάν είναι εφικτό, ο δικαιούχος ή υπεργολάβος μπορεί να καταστρέψει τις ΔΠΕΕ αντί να τις επιστρέψει. Η εν λόγω καταστροφή πρέπει να πραγματοποιηθεί σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις της χώρας στην οποία έχει την έδρα του ο δικαιούχος, με την προηγούμενη συναίνεση της Αρχής Ασφαλείας της Επιτροπής και υπό την καθοδήγηση αυτής. Οι ΔΠΕΕ πρέπει να καταστρέφονται κατά τρόπο ώστε να μην μπορούν να ανασυσταθούν, εν όλω ή εν μέρει.

9. Εάν ο δικαιούχος ή υπεργολάβος έχει λάβει άδεια διατήρησης ΔΠΕΕ μετά τη λύση ή την ολοκλήρωση της συμφωνίας επιδότησης, οι ΔΠΕΕ πρέπει να εξακολουθήσουν να προστατεύονται σύμφωνα με την απόφαση 2015/444 και με τους κανόνες εφαρμογής της ([4]).

10. Κάθε ηλεκτρονικός χειρισμός, επεξεργασία και διαβίβαση ΔΠΕΕ πρέπει να πραγματοποιείται σε συμμόρφωση προς τις διατάξεις των κεφαλαίων 5 και 6 της απόφασης 2015/444. Σε αυτές περιλαμβάνονται, μεταξύ άλλων, η υποχρέωση πιστοποίησης των συστημάτων επικοινωνίας και πληροφοριών που ανήκουν στον δικαιούχο και χρησιμοποιούνται για τον χειρισμό ΔΠΕΕ για τους σκοπούς της συμφωνίας επιδότησης (στο εξής: CIS του δικαιούχου) ([5])· ο όρος ότι κάθε ηλεκτρονική διαβίβαση ΔΠΕΕ πρέπει να προστατεύεται με κρυπτογραφικά προϊόντα που έχουν εγκριθεί σύμφωνα με το άρθρο 36 παράγραφος 4 της απόφασης 2015/444 και ο όρος ότι πρέπει να εφαρμόζονται μέτρα ασφαλείας TEMPEST σύμφωνα με το άρθρο 36 παράγραφος 6 της απόφασης 2015/444.

11. Ο δικαιούχος ή υπεργολάβος διαθέτει επιχειρησιακά σχέδια έκτακτης ανάγκης (BCP) για την προστασία των ΔΠΕΕ που αποτελούν αντικείμενο χειρισμού στο πλαίσιο της εκτέλεσης της διαβαθμισμένης συμφωνίας επιδότησης σε καταστάσεις έκτακτης ανάγκης, και θεσπίζει προληπτικά και επανορθωτικά μέτρα με σκοπό την ελαχιστοποίηση του αντίκτυπου ενδεχόμενων συμβάντων στον χειρισμό και την αποθήκευση ΔΠΕΕ. Ο δικαιούχος ή υπεργολάβος πρέπει να ενημερώσει τη χορηγούσα αρχή για τα εν λόγω επιχειρησιακά σχέδιά του.

ΣΥΜΦΩΝΙΕΣ ΕΠΙΔΟΤΗΣΗΣ ΠΟΥ ΑΠΑΙΤΟΥΝ ΠΡΟΣΒΑΣΗ ΣΕ ΠΛΗΡΟΦΟΡΙΕΣ ΜΕ ΔΙΑΒΑΘΜΙΣΗ RESTREINT UE/EU RESTRICTED

12. Καταρχήν, δεν απαιτείται εξουσιοδότηση ασφαλείας προσωπικού (ΕΑΠ) για να υπάρχει συμμόρφωση με τη συμφωνία επιδότησης ([6]). Ωστόσο, πρόσβαση σε πληροφορίες ή υλικό με διαβάθμιση RESTREINT UE/EU RESTRICTED πρέπει να παρέχεται μόνο σε προσωπικό του δικαιούχου που χρειάζεται τις εν λόγω πληροφορίες για την εκτέλεση της συμφωνίας επιδότησης (*αρχή της ανάγκης για γνώση*) και το οποίο έχει ενημερωθεί από τον υπεύθυνο ασφαλείας του δικαιούχου για τις ευθύνες του και τις συνέπειες τυχόν θέσης σε κίνδυνο ή παραβίασης της ασφάλειας των εν λόγω πληροφοριών, και το οποίο έχει αναγνωρίσει εγγράφως ότι έχει λάβει γνώση των συνεπειών της μη προστασίας των ΔΠΕΕ.

13. Εκτός εάν η χορηγούσα αρχή έχει παράσχει την έγγραφη συναίνεσή της, ο δικαιούχος ή υπεργολάβος δεν πρέπει να παρέχει πρόσβαση σε πληροφορίες ή υλικό με διαβάθμιση RESTREINT UE/EU RESTRICTED σε οποιαδήποτε οντότητα ή πρόσωπο πέραν των μελών του προσωπικού του που έχουν ανάγκη γνώσης.

14. Ο δικαιούχος ή υπεργολάβος πρέπει να διατηρεί τις σημάνσεις διαβάθμισης ασφαλείας των διαβαθμισμένων πληροφοριών που παράγονται από ή παρέχονται κατά την εκτέλεση της συμφωνίας επιδότησης, και δεν πρέπει να αποχαρακτηρίζει πληροφορίες χωρίς την έγγραφη συναίνεση της χορηγούσας αρχής.

15. Πληροφορίες ή υλικό με διαβάθμιση RESTREINT UE/EU RESTRICTED πρέπει, όταν δεν χρησιμοποιούνται, να αποθηκεύονται σε κλειδωμένα έπιπλα γραφείου. Κατά τη μεταφορά τους, τα έγγραφα πρέπει να μεταφέρονται εντός αδιαφανούς φακέλου. Τα έγγραφα πρέπει να παραμένουν συνεχώς στην κατοχή του κομιστή τους και δεν πρέπει να ανοίγονται καθ' οδόν.

([4]) Η χορηγούσα αρχή θα πρέπει να εισαγάγει τις παραπομπές αφού εκδοθούν οι κανόνες εφαρμογής.

([5]) Το μέρος που αναλαμβάνει την πιστοποίηση θα πρέπει να υποβάλει στη χορηγούσα αρχή δήλωση συμμόρφωσης, μέσω της Αρχής Ασφαλείας της Επιτροπής και σε συντονισμό με την αρμόδια εθνική αρχή πιστοποίησης της ασφάλειας (ΑΠΑ).

([6]) Στην περίπτωση που οι δικαιούχοι προέρχονται από κράτη μέλη που απαιτούν ΕΑΠ και/ή FSC για επιδοτήσεις με διαβάθμιση RESTREINT UE/EU RESTRICTED, η χορηγούσα αρχή απαριθμεί στο ΕΘΑ τις απαιτήσεις για ΕΑΠ και FSC για τους εν λόγω δικαιούχους.

16. Ο δικαιούχος ή υπεργολάβος μπορεί να διαβιβάζει στη χορηγούσα αρχή έγγραφα με διαβάθμιση RESTREINT UE/EU RESTRICTED μέσω εμπορικών εταιρειών ταχυμεταφορών, ταχυδρομικών υπηρεσιών, ιδιοχείρως ή με ηλεκτρονικά μέσα. Προς τον σκοπό αυτόν, ο δικαιούχος ή υπεργολάβος πρέπει να ακολουθεί τις εντολές ασφαλείας προγράμματος (ή έργου) (PSI) που έχει εκδώσει η Επιτροπή και/ή τους κανόνες εφαρμογής της Επιτροπής για τη βιομηχανική ασφάλεια όσον αφορά τις διαβαθμισμένες συμφωνίες επιδότησης ([7]).

17. Όταν δεν χρειάζονται πλέον, τα έγγραφα με διαβάθμιση RESTREINT UE/EU RESTRICTED πρέπει να καταστρέφονται κατά τρόπο ώστε να μην μπορούν να ανασυσταθούν, εν όλω ή εν μέρει.

18. Η πιστοποίηση ασφαλείας των CIS του δικαιούχου που χειρίζονται ΔΠΕΕ επιπέδου RESTREINT UE/EU RESTRICTED και κάθε τυχόν διασύνδεσής τους μπορεί να ανατίθεται στον υπεύθυνο ασφαλείας του δικαιούχου, εάν αυτό επιτρέπεται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις. Σε περίπτωση ανάθεσης της πιστοποίησης κατά τα παραπάνω, οι αρμόδιες ΕΑΑ, ΚΑΑ ή αρχές πιστοποίησης της ασφάλειας (ΑΠΑ) διατηρούν την ευθύνη για την προστασία των πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED τις οποίες χειρίζεται ο δικαιούχος, καθώς και το δικαίωμα να επιθεωρούν τα μέτρα ασφαλείας που εφαρμόζει ο δικαιούχος. Επιπροσθέτως, ο δικαιούχος υποβάλλει στη χορηγούσα αρχή και, εάν απαιτείται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις, στην αρμόδια εθνική ΑΠΑ δήλωση συμμόρφωσης με την οποία βεβαιώνεται ότι τα CIS του δικαιούχου και οι σχετικές διασυνδέσεις έχουν πιστοποιηθεί για τον χειρισμό ΔΠΕΕ επιπέδου RESTREINT UE/EU RESTRICTED.

ΧΕΙΡΙΣΜΟΣ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕ ΔΙΑΒΑΘΜΙΣΗ RESTREINT UE/EU RESTRICTED ΣΕ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ (CIS)

19. Οι ελάχιστες προδιαγραφές για τα CIS που χειρίζονται πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED καθορίζονται στο προσάρτημα Ε του παρόντος εγγράφου θεμάτων ασφαλείας.

ΟΡΟΙ ΥΠΟ ΤΟΥΣ ΟΠΟΙΟΥΣ Ο ΔΙΚΑΙΟΥΧΟΣ ΜΠΟΡΕΙ ΝΑ ΣΥΝΑΠΤΕΙ ΣΥΜΒΑΣΕΙΣ ΥΠΕΡΓΟΛΑΒΙΑΣ

20. Ο δικαιούχος πρέπει να εξασφαλίσει άδεια από τη χορηγούσα αρχή προτού αναθέσει υπεργολαβικά οποιοδήποτε μέρος διαβαθμισμένης συμφωνίας επιδότησης.

21. Δεν επιτρέπεται η ανάθεση υπεργολαβίας σε οντότητα με έδρα σε τρίτη χώρα ή σε οντότητα που ανήκει σε διεθνή οργανισμό, εάν η εν λόγω τρίτη χώρα ή ο εν λόγω διεθνής οργανισμός δεν έχει συνάψει συμφωνία για την ασφάλεια των πληροφοριών με την ΕΕ ή διοικητικό διακανονισμό με την Επιτροπή.

22. Εάν ο δικαιούχος προβεί σε ανάθεση υπεργολαβίας, οι διατάξεις της συμφωνίας επιδότησης για την ασφάλεια εφαρμόζονται αναλογικά στον/στους υπεργολάβο/-ους και στο προσωπικό του/τους. Στην περίπτωση αυτή, αποτελεί ευθύνη του δικαιούχου να διασφαλίζει ότι όλοι οι υπεργολάβοι εφαρμόζουν τις εν λόγω αρχές στις συμβάσεις υπεργολαβίας που συνάπτουν οι ίδιοι. Προκειμένου να διασφαλίζεται η δέουσα εποπτεία των ζητημάτων ασφάλειας, οι ΕΑΑ και/ή ΚΑΑ του δικαιούχου και του υπεργολάβου ενημερώνονται από την Αρχή Ασφαλείας της Επιτροπής για τη σύναψη κάθε σχετικής διαβαθμισμένης σύμβασης υπεργολαβίας επιπέδου CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET. Κατά περίπτωση, υποβάλλεται στις ΕΑΑ και/ή ΚΑΑ του δικαιούχου και του υπεργολάβου αντίγραφο των διατάξεων για την ασφάλεια που σχετίζονται με τη σύμβαση υπεργολαβίας. Οι ΕΑΑ και ΚΑΑ που απαιτούν κοινοποίηση σχετικά με τις διατάξεις για την ασφάλεια των διαβαθμισμένων συμφωνιών επιδότησης επιπέδου RESTREINT UE/EU RESTRICTED παρατίθενται στο παράρτημα των κανόνων εφαρμογής της Επιτροπής για τη βιομηχανική ασφάλεια όσον αφορά τις διαβαθμισμένες συμφωνίες επιδότησης ([8]).

23. Ο δικαιούχος δεν επιτρέπεται να κοινοποιήσει οποιεσδήποτε ΔΠΕΕ σε υπεργολάβο χωρίς την προηγούμενη έγγραφη συναίνεση της χορηγούσας αρχής. Εάν πρόκειται να αποστέλλονται ΔΠΕΕ σε υπεργολάβους συχνά ή κατά τρόπο συστηματικό, η χορηγούσα αρχή μπορεί να παράσχει τη συναίνεσή της για συγκεκριμένο χρονικό διάστημα (π.χ. 12 μήνες) ή για τη διάρκεια της σύμβασης υπεργολαβίας.

([7]) Η χορηγούσα αρχή θα πρέπει να εισαγάγει τις παραπομπές αφού εκδοθούν οι κανόνες εφαρμογής.
([8]) Η χορηγούσα αρχή θα πρέπει να εισαγάγει τις παραπομπές αφού εκδοθούν οι κανόνες εφαρμογής.

ΕΠΙΣΚΕΨΕΙΣ

Εάν πρόκειται να εφαρμόζεται η συνήθης διαδικασία αίτησης επίσκεψης (RFV) για τις επισκέψεις που αφορούν πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, η χορηγούσα αρχή πρέπει να συμπεριλάβει τα σημεία 24, 25 και 26 και να διαγράψει το σημείο 27. Εάν οι επισκέψεις που αφορούν πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET διοργανώνονται απευθείας μεταξύ των εγκαταστάσεων αποστολής και προορισμού, η χορηγούσα αρχή πρέπει να διαγράψει τα σημεία 25 και 26 και να συμπεριλάβει μόνο το σημείο 27.

24. Οι επισκέψεις που συνεπάγονται πρόσβαση ή πιθανή πρόσβαση σε πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED διοργανώνονται απευθείας μεταξύ των εγκαταστάσεων αποστολής και προορισμού, χωρίς να χρειάζεται να τηρηθούν οι διαδικασίες των παρακάτω σημείων 25 έως 27.

[25. Οι επισκέψεις που συνεπάγονται πρόσβαση ή πιθανή πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET υπόκεινται στην ακόλουθη διαδικασία:

α) ο υπεύθυνος ασφαλείας της εγκατάστασης αποστολής του επισκέπτη συμπληρώνει όλα τα σχετικά σημεία του εντύπου αίτησης επίσκεψης (προσάρτημα Γ) και υποβάλλει την αίτηση στην ΕΑΑ ή ΚΑΑ της εγκατάστασης·

β) η ΕΑΑ ή ΚΑΑ της εγκατάστασης αποστολής πρέπει να επιβεβαιώσει την εξουσιοδότηση ασφαλείας προσωπικού του επισκέπτη προτού υποβάλει την αίτηση επίσκεψης στην ΕΑΑ ή ΚΑΑ της εγκατάστασης υποδοχής (ή στην Αρχή Ασφαλείας της Επιτροπής, εάν η επίσκεψη πρόκειται να πραγματοποιηθεί σε εγκαταστάσεις της χορηγούσας αρχής)·

γ) στη συνέχεια, ο υπεύθυνος ασφαλείας της εγκατάστασης αποστολής λαμβάνει από την οικεία ΕΑΑ ή ΚΑΑ την απάντηση της ΕΑΑ ή ΚΑΑ της εγκατάστασης υποδοχής (ή της Αρχής Ασφαλείας της Επιτροπής), με την οποία η αίτηση επίσκεψης είτε γίνεται δεκτή είτε απορρίπτεται·

δ) η αίτηση επίσκεψης θεωρείται ότι έχει γίνει δεκτή εάν δεν διατυπωθούν αντιρρήσεις έως πέντε εργάσιμες ημέρες πριν από την ημερομηνία της επίσκεψης.]

[26. Πριν παράσχει στον/στους επισκέπτη/-ες πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, η εγκατάσταση υποδοχής πρέπει να έχει λάβει άδεια από την οικεία ΕΑΑ ή ΚΑΑ.]

[27. Οι επισκέψεις που συνεπάγονται πρόσβαση ή πιθανή πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET διοργανώνονται απευθείας μεταξύ των εγκαταστάσεων αποστολής και προορισμού (παράδειγμα εντύπου που μπορεί να χρησιμοποιηθεί για τον σκοπό αυτόν παρέχεται στο προσάρτημα Γ).]

28. Οι επισκέπτες πρέπει να αποδεικνύουν την ταυτότητά τους κατά την άφιξή τους στην εγκατάσταση υποδοχής, με την επίδειξη ισχύοντος δελτίου ταυτότητας ή διαβατηρίου.

29. Η εγκατάσταση υποδοχής της επίσκεψης πρέπει να διασφαλίζει ότι τηρούνται αρχεία για όλους τους επισκέπτες. Στα εν λόγω αρχεία πρέπει να καταγράφονται για κάθε επισκέπτη το όνομά του, ο οργανισμός τον οποίο εκπροσωπεί, η ημερομηνία λήξης της εξουσιοδότησης ασφαλείας προσωπικού του (κατά περίπτωση), η ημερομηνία της επίσκεψης και το/τα όνομα/ονόματα του/των προσώπου/-ων που επισκέφθηκε. Με την επιφύλαξη των ευρωπαϊκών κανόνων για την προστασία των δεδομένων, τα εν λόγω αρχεία πρέπει να τηρούνται για διάστημα τουλάχιστον πέντε ετών ή για το διάστημα που ορίζουν οι εθνικές νομοθετικές και κανονιστικές διατάξεις, ανάλογα με την περίπτωση.

ΕΠΙΣΚΕΨΕΙΣ ΑΞΙΟΛΟΓΗΣΗΣ

30. Η Αρχή Ασφαλείας της Επιτροπής μπορεί, σε συνεργασία με τις αρμόδιες ΕΑΑ ή ΚΑΑ, να πραγματοποιεί επισκέψεις σε εγκαταστάσεις δικαιούχων ή υπεργολάβων, προκειμένου να ελέγχει την τήρηση των προδιαγραφών ασφαλείας για τον χειρισμό ΔΠΕΕ.

ΟΔΗΓΟΣ ΔΙΑΒΑΘΜΙΣΗΣ ΑΣΦΑΛΕΙΑΣ

31. Στον οδηγό διαβάθμισης ασφαλείας (ΟΔΑ) περιλαμβάνεται κατάλογος όλων των στοιχείων της συμφωνίας επιδότησης που είναι διαβαθμισμένα ή πρόκειται να διαβαθμιστούν κατά την εκτέλεση της συμφωνίας επιδότησης, οι κανόνες για την εν λόγω διαβάθμιση και ο καθορισμός των εφαρμοστέων επιπέδων διαβάθμισης ασφάλειας. Ο οδηγός διαβάθμισης ασφαλείας αποτελεί αναπόσπαστο μέρος της παρούσας συμφωνίας επιδότησης και περιλαμβάνεται στο προσάρτημα Β του παρόντος παραρτήματος.

Προσάρτημα Β

ΟΔΗΓΟΣ ΔΙΑΒΑΘΜΙΣΗΣ ΑΣΦΑΛΕΙΑΣ

[το συγκεκριμένο κείμενο πρέπει να προσαρμόζεται ανάλογα με το αντικείμενο της συμφωνίας επιδότησης]

Προσάρτημα Γ

ΑΙΤΗΣΗ ΕΠΙΣΚΕΨΗΣ (ΥΠΟΔΕΙΓΜΑ)

ΑΝΑΛΥΤΙΚΕΣ ΟΔΗΓΙΕΣ ΓΙΑ ΤΗ ΣΥΜΠΛΗΡΩΣΗ ΤΗΣ ΑΙΤΗΣΗΣ ΕΠΙΣΚΕΨΗΣ

(Η αίτηση πρέπει να υποβληθεί στην αγγλική γλώσσα μόνο)

HEADING	Συμπληρώστε τα τετραγωνίδια που αφορούν το είδος της επίσκεψης, το είδος των πληροφοριών και σημειώστε τον αριθμό των χώρων στους οποίους πρόκειται να πραγματοποιηθεί επίσκεψη και τον αριθμό των επισκεπτών.
4. **ADMINISTRATIVE DATA**	Συμπληρώνεται από την αιτούσα εθνική αρχή ασφαλείας (ΕΑΑ)/καθορισμένη αρχή ασφαλείας (ΚΑΑ).
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**	Αναγράψτε την πλήρη ονομασία και ταχυδρομική διεύθυνση. Συμπεριλάβετε την πόλη, τη χώρα και τον ταχυδρομικό κώδικα, κατά περίπτωση.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Αναγράψτε την πλήρη ονομασία και ταχυδρομική διεύθυνση. Συμπεριλάβετε την πόλη, τη χώρα, τον ταχυδρομικό κώδικα, τον αριθμό τέλεξ ή φαξ (αν συντρέχει περίπτωση), τον αριθμό τηλεφώνου και τη διεύθυνση ηλεκτρονικού ταχυδρομείου. Αναγράψτε το όνομα, τον αριθμό τηλεφώνου/φαξ και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του κύριου σημείου επαφής σας ή του προσώπου με το οποίο συνεννοηθήκατε για την πραγματοποίηση της επίσκεψης. Παρατηρήσεις: 1) Η αναγραφή του ορθού ταχυδρομικού κώδικα είναι σημαντική διότι μια εταιρεία μπορεί να έχει διάφορες εγκαταστάσεις. 2) Όταν η αίτηση συμπληρώνεται χειρόγραφα, το παράρτημα 1 μπορεί να χρησιμοποιηθεί όταν πρέπει να πραγματοποιηθούν επισκέψεις σε δύο ή περισσότερες εγκαταστάσεις σε σχέση με το ίδιο θέμα. Όταν χρησιμοποιείται παράρτημα, στο σημείο 3 πρέπει να αναγράφεται: «ΒΛ. ΠΑΡΑΡΤΗΜΑ 1, ΑΡΙΘ. ΕΓΚΑΤ. » (δηλώστε τον αριθμό των εγκαταστάσεων).
7. **DATES OF VISIT**	Αναγράψτε τη συγκεκριμένη ημερομηνία ή περίοδο (ημερομηνία έως ημερομηνία) της επίσκεψης υπό τη μορφή «ημέρα – μήνας – έτος». Αν συντρέχει περίπτωση, αναγράψτε εναλλακτική ημερομηνία ή περίοδο εντός παρενθέσεων.
8. **TYPE OF INITIATIVE**	Διευκρινίστε αν η επίσκεψη πραγματοποιείται με πρωτοβουλία του οργανισμού ή της εγκατάστασης που υποβάλλει την αίτηση ή κατόπιν πρόσκλησης της εγκατάστασης στην οποία πρόκειται να πραγματοποιηθεί η επίσκεψη.
9. **THE VISIT RELATES TO:**	Αναγράψτε την πλήρη ονομασία του έργου, της σύμβασης ή της πρόσκλησης υποβολής προσφορών, αποφεύγοντας τη χρήση συντομογραφιών που δεν χρησιμοποιούνται ευρέως.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Περιγράψτε συνοπτικά τον/τους λόγο/-ους της επίσκεψης. Μη χρησιμοποιείτε συντομογραφίες που δεν επεξηγούνται. Παρατηρήσεις: Στην περίπτωση επαναλαμβανόμενων επισκέψεων, στο σημείο αυτό θα πρέπει να αναγραφεί η φράση «Επαναλαμβανόμενες επισκέψεις» στην αρχή του στοιχείου δεδομένων (π.χ. Επαναλαμβανόμενες επισκέψεις για να συζητηθεί ___)
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Αναγράψτε SECRET EU/EU SECRET (S-EU/EU-S) ή CONFIDENTIEL EU/EU CONFIDENTIAL (C-EU/EU-C), ανάλογα με την περίπτωση.

12. **PARTICULARS OF VISITOR**	Παρατήρηση: Όταν στην επίσκεψη συμμετέχουν περισσότεροι από δύο επισκέπτες, θα πρέπει να χρησιμοποιείται το παράρτημα 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Στο σημείο αυτό πρέπει να αναγραφεί το όνομα, ο αριθμός τηλεφώνου, ο αριθμός φαξ και η διεύθυνση ηλεκτρονικού ταχυδρομείου του υπευθύνου ασφαλείας της αιτούσας εγκατάστασης.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Το πεδίο αυτό συμπληρώνεται από την αρχή πιστοποίησης. Σημειώσεις για την αρχή πιστοποίησης: α. Αναγράψτε το όνομα, τη διεύθυνση, τον αριθμό τηλεφώνου, τον αριθμό φαξ και τη διεύθυνση ηλεκτρονικού ταχυδρομείου (μπορούν να προεκτυπώνονται). β. Το παρόν σημείο θα πρέπει να φέρει υπογραφή και σφραγίδα (κατά περίπτωση).
15. **REQUESTING SECURITY AUTHORITY**	Το πεδίο αυτό συμπληρώνεται από την ΕΑΑ/ΚΑΑ. Σημειώσεις για την ΕΑΑ/ΚΑΑ: α. Αναγράψτε το όνομα, τη διεύθυνση, τον αριθμό τηλεφώνου, τον αριθμό φαξ και τη διεύθυνση ηλεκτρονικού ταχυδρομείου (μπορούν να προεκτυπώνονται). β. Το παρόν σημείο θα πρέπει να φέρει υπογραφή και σφραγίδα (κατά περίπτωση).

Όλα τα πεδία πρέπει να συμπληρωθούν και το έντυπο πρέπει να υποβληθεί μέσω διακυβερνητικών διαύλων (9).

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**	
Requester: To:	NSA/DSA RFV Reference No_____ Date *(dd/mm/yyyy)*: _____/_____/_____

(9) Εάν έχει συμφωνηθεί ότι οι επισκέψεις που συνεπάγονται πρόσβαση ή πιθανή πρόσβαση σε ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET μπορούν να διοργανώνονται απευθείας, το συμπληρωμένο έντυπο μπορεί να υποβληθεί απευθείας στον υπεύθυνο ασφαλείας της εγκατάστασης στην οποία πρόκειται να πραγματοποιηθεί η επίσκεψη.

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED *(Annex 1 to be completed)***

7. **DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____**

8. **TYPE OF INITIATIVE:**

□ Initiated by requesting organisation or facility

□ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):**

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S) *(Annex 2 to be completed)***

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

DATE *(dd/mm/yyyy)*:
_____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE:

DATE *(dd/mm/yyyy)*:
_____/_____/_____

16. **REMARKS *(Mandatory justification required in the case of an emergency visit)*:**

<Θέση κειμένου για παραπομπή στην εφαρμοστέα νομοθεσία περί δεδομένων προσωπικού χαρακτήρα και σύνδεσμο προς τις πληροφορίες που πρέπει υποχρεωτικά να παρέχονται στο υποκείμενο των δεδομένων, π.χ. με ποιον τρόπο εφαρμόζεται το άρθρο 13 του Γενικού Κανονισμού για την Προστασία Δεδομένων ([10]).>

([10]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

ΠΑΡΑΡΤΗΜΑ 1 του ΕΝΤΥΠΟΥ ΑΙΤΗΣΗΣ ΕΠΙΣΚΕΨΗΣ

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

<Θέση κειμένου για παραπομπή στην εφαρμοστέα νομοθεσία περί δεδομένων προσωπικού χαρακτήρα και σύνδεσμο προς τις πληροφορίες που πρέπει υποχρεωτικά να παρέχονται στο υποκείμενο των δεδομένων, π.χ. με ποιον τρόπο εφαρμόζεται το άρθρο 13 του Γενικού Κανονισμού για την Προστασία Δεδομένων ([11]).>

([11]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

ΠΑΡΑΡΤΗΜΑ 2 του ΕΝΤΥΠΟΥ ΑΙΤΗΣΗΣ ΕΠΙΣΚΕΨΗΣ

PARTICULARS OF VISITOR(S)
1. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
2. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION: ***(Continue as required)***

<Θέση κειμένου για παραπομπή στην εφαρμοστέα νομοθεσία περί δεδομένων προσωπικού χαρακτήρα και σύνδεσμο προς τις πληροφορίες που πρέπει υποχρεωτικά να παρέχονται στο υποκείμενο των δεδομένων, π.χ. με ποιον τρόπο εφαρμόζεται το άρθρο 13 του Γενικού Κανονισμού για την Προστασία Δεδομένων ([12]).>

([12]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

Προσάρτημα Δ

ΔΕΛΤΙΟ ΠΛΗΡΟΦΟΡΙΩΝ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΦΟΡΕΑ (FSCIS) (ΥΠΟΔΕΙΓΜΑ)

1. **ΕΙΣΑΓΩΓΗ**

1.1. Συνημμένα παρατίθεται υπόδειγμα δελτίου πληροφοριών εξουσιοδότησης ασφαλείας φορέα (FSCIS), το οποίο εξυπηρετεί την ταχεία ανταλλαγή πληροφοριών μεταξύ της εθνικής αρχής ασφαλείας (ΕΑΑ) ή της καθορισμένης αρχής ασφαλείας (ΚΑΑ), άλλων αρμόδιων εθνικών αρχών ασφαλείας και της Αρχής Ασφαλείας της Επιτροπής (η οποία ενεργεί εξ ονόματος των χορηγουσών αρχών) όσον αφορά την εξουσιοδότηση ασφαλείας φορέα (FSC) που συμμετέχει σε διαδικασίες υποβολής αιτήσεων για διαβαθμισμένες συμφωνίες επιδότησης ή συμβάσεις υπεργολαβίας ή στην εκτέλεση αυτών.

1.2. Το FSCIS είναι έγκυρο μόνο εάν φέρει τη σφραγίδα της αρμόδιας ΕΑΑ, ΚΑΑ ή άλλης αρμόδιας αρχής.

1.3. Το FSCIS διαιρείται στο τμήμα αίτησης και στο τμήμα απάντησης, και μπορεί να χρησιμοποιηθεί για τους σκοπούς που αναφέρονται ανωτέρω ή για οποιουσδήποτε άλλους σκοπούς για τους οποίους απαιτείται το καθεστώς FSC συγκεκριμένου φορέα. Ο λόγος της έρευνας πρέπει να επισημανθεί από την αιτούσα ΕΑΑ ή ΚΑΑ στο πεδίο 7 του τμήματος αίτησης.

1.4. Κατά κανόνα, τα στοιχεία που περιέχονται στο FSCIS δεν είναι διαβαθμισμένα· επομένως, όταν πρέπει να αποσταλεί FSCIS μεταξύ των οικείων ΕΑΑ/ΚΑΑ/Επιτροπής, η αποστολή θα πρέπει κατά προτίμηση να γίνεται με ηλεκτρονικά μέσα.

1.5. Οι ΕΑΑ/ΚΑΑ θα πρέπει να καταβάλλουν κάθε δυνατή προσπάθεια για να ανταποκρίνονται στις αιτήσεις FSCIS εντός δέκα εργάσιμων ημερών.

1.6. Εάν διαβιβαστούν διαβαθμισμένες πληροφορίες ή συναφθεί συμφωνία επιδότησης ή σύμβαση υπεργολαβίας σε συνάρτηση με την παρούσα διαβεβαίωση, πρέπει να ενημερωθεί η ΕΑΑ ή ΚΑΑ που την εξέδωσε.

Διαδικασίες και οδηγίες για τη χρήση του δελτίου πληροφοριών εξουσιοδότησης ασφαλείας φορέα (FSCIS)

Οι παρούσες αναλυτικές οδηγίες απευθύνονται στην ΕΑΑ ή ΚΑΑ ή στη χορηγούσα αρχή και στην Αρχή Ασφαλείας της Επιτροπής που συμπληρώνει το FSCIS. Κατά προτίμηση, η αίτηση θα πρέπει να δακτυλογραφηθεί με κεφαλαία γράμματα.

ΕΠΙΚΕΦΑΛΙΔΑ	Ο αιτών αναγράφει το πλήρες όνομα της ΕΑΑ/ΚΑΑ και της χώρας.
1. **ΕΙΔΟΣ ΑΙΤΗΣΗΣ**	Η αιτούσα χορηγούσα αρχή επιλέγει το κατάλληλο τετραγωνίδιο για το είδος της αίτησης FSCIS. Συμπεριλάβετε το επίπεδο της εξουσιοδότησης ασφαλείας που ζητείται. Θα πρέπει να χρησιμοποιηθούν οι ακόλουθες συντομογραφίες: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = Συστήματα επικοινωνίας και πληροφοριών για την επεξεργασία διαβαθμισμένων πληροφοριών.
2. **ΣΤΟΙΧΕΙΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ**	Τα πεδία 1 έως 6 είναι προφανή. Στο πεδίο 4 θα πρέπει να αναγραφεί ο συνήθης διψήφιος κωδικός χώρας. Το πεδίο 5 είναι προαιρετικό.
3. **ΛΟΓΟΣ ΤΗΣ ΑΙΤΗΣΗΣ**	Αναγράψτε τον συγκεκριμένο λόγο για τον οποίο υποβάλλεται η αίτηση και συμπεριλάβετε τους δείκτες του έργου και τον αριθμό της πρόσκλησης υποβολής προτάσεων ή της επιδότησης. Προσδιορίστε τις ανάγκες σε ικανότητα αποθήκευσης, το επίπεδο διαβάθμισης των CIS κ.λπ. Θα πρέπει να αναφερθούν τυχόν προθεσμίες/ημερομηνίες λήξης/κατακύρωσης που μπορεί να έχουν σημασία για την ολοκλήρωση της FSC.

4. **ΑΙΤΟΥΣΑ ΕΑΑ/ΚΑΑ**	Αναγράψτε το όνομα του φυσικού προσώπου που υποβάλλει την αίτηση (εξ ονόματος της ΕΑΑ/ΚΑΑ) και την ημερομηνία της αίτησης με αριθμούς (ηη/μμ/εεεε).
5. **ΤΜΗΜΑ ΑΠΑΝΤΗΣΗΣ**	Πεδία 1-5: επιλέξτε τα κατάλληλα πεδία. Πεδίο 2: εάν FSC βρίσκεται υπό επεξεργασία, συνιστάται να γνωστοποιηθεί στον αιτούντα ο απαιτούμενος χρόνος επεξεργασίας (εφόσον είναι γνωστός). Πεδίο 6: α) Μολονότι η έγκριση διαφέρει ανά χώρα ή ακόμη και ανά φορέα, συνιστάται να αναγράφεται η ημερομηνία λήξης της ισχύος της FSC. β) Στις περιπτώσεις που η διάρκεια της διαβεβαίωσης της FSC είναι αόριστη, το πεδίο αυτό μπορεί να διαγραφεί. γ) Σύμφωνα με τις αντίστοιχες εθνικές νομοθετικές και κανονιστικές διατάξεις, ο αιτών ή είτε ο δικαιούχος είτε ο υπεργολάβος είναι υπεύθυνος για την υποβολή αίτησης ανανέωσης της FSC.
6. **ΠΑΡΑΤΗΡΗΣΕΙΣ**	Το εν λόγω πεδίο μπορεί να χρησιμοποιηθεί για να παρασχεθούν συμπληρωματικές πληροφορίες σχετικά με την FSC, τον φορέα ή τα παραπάνω σημεία.
7. **ΕΑΑ/ΚΑΑ ΕΚΔΟΣΗΣ**	Αναγράψτε το όνομα της αρχής που παρέχει τις πληροφορίες (εξ ονόματος της ΕΑΑ/ΚΑΑ) και την ημερομηνία της απάντησης με αριθμούς (ηη/μμ/εεεε).

ΔΕΛΤΙΟ ΠΛΗΡΟΦΟΡΙΩΝ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΦΟΡΕΑ (FSCIS) (ΥΠΟΔΕΙΓΜΑ)

Όλα τα πεδία πρέπει να συμπληρωθούν και το έντυπο πρέπει να διαβιβαστεί μέσω διακυβερνητικών διαύλων ή μέσω διαύλων μεταξύ κυβέρνησης και διεθνούς οργανισμού.

ΑΙΤΗΣΗ ΓΙΑ ΔΙΑΒΕΒΑΙΩΣΗ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΦΟΡΕΑ

ΠΡΟΣ: _____

(Όνομα χώρας ΕΑΑ/ΚΑΑ)

Συμπληρώστε τα τετραγωνίδια απάντησης, κατά περίπτωση:

[ ] Παράσχετε διαβεβαίωση εξουσιοδότησης ασφαλείας φορέα (FSC) επιπέδου: [ ] S-UE/EU-S [ ] C-UE/EU-C

για τον παρακάτω φορέα

[ ] Συμπεριλαμβανομένης της διαφύλαξης διαβαθμισμένου υλικού/πληροφοριών

[ ] Συμπεριλαμβανομένων συστημάτων επικοινωνίας και πληροφοριών (CIS) για την επεξεργασία διαβαθμισμένων πληροφοριών

[ ] Κινήστε, απευθείας ή κατόπιν αντίστοιχου αιτήματος δικαιούχου ή υπεργολάβου, τη διαδικασία λήψης FSC έως και το επίπεδο ..... με επίπεδο διαφύλαξης ..... και επίπεδο CIS ....., εάν ο φορέας δεν διαθέτει επί του παρόντος τα εν λόγω επίπεδα ικανοτήτων.

Επιβεβαιώστε την ακρίβεια των στοιχείων του παρακάτω φορέα και αναφέρετε τις τυχόν αναγκαίες διορθώσεις/προσθήκες.

1. Πλήρες όνομα φορέα: Διορθώσεις/Προσθήκες:

....

2. Πλήρης διεύθυνση φορέα:

....

3. Ταχυδρομική διεύθυνση (εάν διαφέρει από τη διεύθυνση του σημείου 2):

....

4. Ταχυδρομικός κώδικας/πόλη/χώρα:

....

5. Όνομα του υπευθύνου ασφαλείας:

.....
.....

6. Τηλέφωνο/φαξ/διεύθυνση ηλεκτρονικού ταχυδρομείου του υπευθύνου ασφαλείας:

....

7. Η παρούσα αίτηση υποβάλλεται για τον/τους ακόλουθο/-ους λόγο/-ους: [παράσχετε λεπτομέρειες για το προσυμβατικό στάδιο (επιλογής προτάσεων), την επιδότηση ή σύμβαση υπεργολαβίας, το πρόγραμμα/έργο κ.λπ.]

.....

Αιτούσα ΕΑΑ/ΚΑΑ/χορηγούσα αρχή: Όνομα: ..... Ημερομηνία: (ηη/μμ/εεεε) .....

ΑΠΑΝΤΗΣΗ (εντός 10 εργάσιμων ημερών)

Με την παρούσα διαβεβαιώνεται ότι:

1. [ ] ο παραπάνω φορέας διαθέτει FSC επιπέδου έως και [ ] S-UE/EU-S

   [ ] C-UE/EU-C.

2. Ο παραπάνω φορέας έχει την ικανότητα να διαφυλάσσει διαβαθμισμένες πληροφορίες/υλικό:

   [ ] ναι, επιπέδου: ..... [ ] όχι.

3. Ο παραπάνω φορέας διαθέτει πιστοποιημένα/εγκεκριμένα CIS:

   [ ] ναι, επιπέδου: ..... [ ] όχι.

4. [ ] σε σχέση με την παραπάνω αίτηση, η διαδικασία FSC έχει κινηθεί. Θα ενημερωθείτε όταν η FSC παρασχεθεί ή απορριφθεί.

5. [ ] ο παραπάνω φορέας δεν διαθέτει FSC.

6. Η παρούσα διαβεβαίωση FSC λήγει στις: ..... (*ηη/μμ/εεεε*) ή όπως τυχόν άλλως κοινοποιήσει η ΕΑΑ/ΚΑΑ. Σε περίπτωση πρόωρης ακύρωσης ή οποιασδήποτε αλλαγής στα παραπάνω στοιχεία, θα ενημερωθείτε.

7. Παρατηρήσεις:
   .....

ΕΑΑ/ΚΑΑ έκδοσης Όνομα: ..... *Ημερομηνία (ηη/μμ/εεεε)* .....

<Θέση κειμένου για παραπομπή στην εφαρμοστέα νομοθεσία περί δεδομένων προσωπικού χαρακτήρα και σύνδεσμο προς τις πληροφορίες που πρέπει υποχρεωτικά να παρέχονται στο υποκείμενο των δεδομένων, π.χ. με ποιον τρόπο εφαρμόζεται το άρθρο 13 του Γενικού Κανονισμού για την Προστασία Δεδομένων ([13]).>

([13]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

Προσάρτημα Ε

Ελάχιστες προδιαγραφές για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΔΠΕΕ) σε ηλεκτρονική μορφή επιπέδου RESTREINT UE/EU RESTRICTED που αποτελούν αντικείμενο χειρισμού στα CIS του δικαιούχου

Γενικά

1. Ο δικαιούχος πρέπει να υποχρεώνεται να διασφαλίζει ότι η προστασία των πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED πληροί τις ελάχιστες προδιαγραφές ασφαλείας που ορίζονται στην παρούσα ρήτρα για την ασφάλεια, καθώς και τις τυχόν πρόσθετες προδιαγραφές της χορηγούσας αρχής ή, κατά περίπτωση, της εθνικής αρχής ασφαλείας (ΕΑΑ) ή της καθορισμένης αρχής ασφαλείας (ΚΑΑ).

2. Αποτελεί ευθύνη του δικαιούχου να εφαρμόζει τις προδιαγραφές ασφαλείας που προσδιορίζονται στο παρόν έγγραφο.

3. Για τους σκοπούς του παρόντος εγγράφου, η έννοια του συστήματος επικοινωνίας και πληροφοριών (CIS) καλύπτει το σύνολο του εξοπλισμού που χρησιμοποιείται για τον χειρισμό, την αποθήκευση και τη διαβίβαση ΔΠΕΕ, συμπεριλαμβανομένων των σταθμών εργασίας, των εκτυπωτών, των φωτοτυπικών, των συσκευών φαξ, των εξυπηρετητών, των συστημάτων διαχείρισης δικτύου, των ελεγκτών δικτύου και των ελεγκτών επικοινωνίας, των φορητών υπολογιστών τύπου laptop ή notebook, των υπολογιστών-ταμπλετών, των έξυπνων τηλεφώνων και των αφαιρούμενων συσκευών αποθήκευσης, όπως είναι τα κλειδιά USB, τα CD, οι κάρτες SD κ.λπ.

4. Ο ειδικός εξοπλισμός, όπως τα κρυπτογραφικά προϊόντα, πρέπει να προστατεύεται σύμφωνα με τις ειδικές του λειτουργικές διαδικασίες ασφαλείας (SecOPs).

5. Ο δικαιούχος πρέπει να δημιουργήσει δομή η οποία θα είναι υπεύθυνη για τη διαχείριση της ασφάλειας των CIS που χειρίζονται πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED και να διορίσει υπεύθυνο ασφαλείας που θα είναι υπεύθυνος για τον οικείο φορέα.

6. Δεν επιτρέπεται η χρήση λύσεων ΤΠ (υλισμικού, λογισμικού ή υπηρεσιών) που ανήκουν προσωπικά σε υπαλλήλους του δικαιούχου για την αποθήκευση ή την επεξεργασία πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED.

7. Η πιστοποίηση των CIS του δικαιούχου που χειρίζονται πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED πρέπει να έχει εγκριθεί από την αρχή πιστοποίησης της ασφάλειας (ΑΠΑ) του οικείου κράτους μέλους ή να έχει ανατεθεί στον υπεύθυνο ασφαλείας του δικαιούχου, εάν και υπό τους όρους που επιτρέπεται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις.

8. Στο πλαίσιο της συμφωνίας επιδότησης, πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED μπορούν να αποτελούν αντικείμενο χειρισμού, να αποθηκεύονται ή να διαβιβάζονται (με ενσύρματα ή ασύρματα μέσα) όπως οποιαδήποτε άλλη μη διαβαθμισμένη πληροφορία, μόνον εάν είναι κρυπτογραφημένες με τη χρήση εγκεκριμένων κρυπτογραφικών προϊόντων. Τα εν λόγω κρυπτογραφικά προϊόντα πρέπει να έχουν εγκριθεί από την ΕΕ ή από κράτος μέλος.

9. Οι εξωτερικοί φορείς που συμμετέχουν σε εργασίες συντήρησης/επισκευής πρέπει να υποχρεώνονται συμβατικά να συμμορφώνονται με τις εφαρμοστέες διατάξεις για τον χειρισμό πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED, όπως ορίζεται στο παρόν έγγραφο.

10. Κατόπιν αιτήματος της χορηγούσας αρχής ή της οικείας ΕΑΑ, ΚΑΑ ή ΑΠΑ, ο δικαιούχος πρέπει να αποδεικνύει τη συμμόρφωσή του με τη ρήτρα της συμφωνίας επιδότησης που αφορά την ασφάλεια. Εάν ζητείται επίσης έλεγχος και επιθεώρηση των διαδικασιών και των εγκαταστάσεων του δικαιούχου προκειμένου να διασφαλιστεί η συμμόρφωση με τις εν λόγω προδιαγραφές, ο δικαιούχος επιτρέπει στους εκπροσώπους της χορηγούσας αρχής, της ΕΑΑ, της ΚΑΑ και/ή της ΑΠΑ, ή της οικείας αρχής ασφαλείας της ΕΕ να διενεργήσουν τον εν λόγω έλεγχο και επιθεώρηση.

Φυσική ασφάλεια

11. Οι χώροι στους οποίους χρησιμοποιούνται CIS για την προβολή, την αποθήκευση, την επεξεργασία ή τη διαβίβαση πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED και οι χώροι που στεγάζουν εξυπηρετητές, συστήματα διαχείρισης δικτύου, ελεγκτές δικτύου και ελεγκτές επικοινωνίας για τα εν λόγω CIS θα πρέπει να προσδιορίζονται ως χωριστοί και ελεγχόμενοι χώροι με κατάλληλο σύστημα ελέγχου της πρόσβασης. Η πρόσβαση στους εν λόγω χωριστούς και ελεγχόμενους χώρους θα πρέπει να περιορίζεται σε άτομα με ειδική άδεια. Με την επιφύλαξη του σημείου 8, ο εξοπλισμός που περιγράφεται στο σημείο 3 πρέπει να αποθηκεύεται σε τέτοιους χωριστούς και ελεγχόμενους χώρους.

12. Πρέπει να εφαρμόζονται μηχανισμοί και/ή διαδικασίες ασφαλείας για τη ρύθμιση της προσθήκης ή της σύνδεσης αφαιρούμενων ηλεκτρονικών μέσων αποθήκευσης (όπως κλειδιών USB, συσκευών μαζικής αποθήκευσης ή CD-RW) σε στοιχεία των CIS.

Πρόσβαση στα CIS

13. Η πρόσβαση στα CIS του δικαιούχου που χειρίζονται ΔΠΕΕ περιορίζεται αυστηρά στο προσωπικό που έχει ανάγκη γνώσης και σχετική εξουσιοδότηση.

14. Όλα τα CIS πρέπει να διαθέτουν επικαιροποιημένους καταλόγους εξουσιοδοτημένων χρηστών. Όλοι οι χρήστες πρέπει να πιστοποιούνται κατά την έναρξη κάθε συνεδρίας επεξεργασίας.

15. Οι κωδικοί πρόσβασης, που αποτελούν μέρος των περισσότερων μέτρων εξακρίβωσης της ταυτότητας και πιστοποίησης, πρέπει να είναι μήκους τουλάχιστον εννέα χαρακτήρων και πρέπει να περιλαμβάνουν αριθμητικούς και «ειδικούς» χαρακτήρες (εάν επιτρέπεται από το σύστημα), καθώς και αλφαβητικούς χαρακτήρες. Οι κωδικοί πρόσβασης πρέπει να αλλάζουν το αργότερο κάθε 180 ημέρες. Πρέπει να αλλάζουν το συντομότερο δυνατόν εάν έχουν διαρρεύσει ή αποκαλυφθεί σε μη εξουσιοδοτημένο πρόσωπο, ή εάν υπάρχει υπόνοια τέτοιας διαρροής ή αποκάλυψής τους.

16. Όλα τα CIS πρέπει να διαθέτουν εσωτερικούς ελέγχους πρόσβασης ώστε να εμποδίζουν τους μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση ή να τροποποιήσουν πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED, ή να τροποποιήσουν ρυθμίσεις του συστήματος ή ελέγχους ασφαλείας. Οι χρήστες πρέπει να αποσυνδέονται αυτόματα από τα CIS εάν οι τερματικοί σταθμοί τους παραμένουν αδρανείς για προκαθορισμένο χρονικό διάστημα ή τα CIS πρέπει να ενεργοποιούν προστατευόμενη με κωδικό πρόσβασης προφύλαξη οθόνης ύστερα από 15 λεπτά αδράνειας.

17. Σε κάθε χρήστη των CIS απονέμεται μοναδικός λογαριασμός χρήστη και μοναδικό αναγνωριστικό. Οι λογαριασμοί χρήστη πρέπει να κλειδώνονται αυτόματα όταν έχουν γίνει τουλάχιστον πέντε διαδοχικές εσφαλμένες απόπειρες σύνδεσης.

18. Όλοι οι χρήστες των CIS πρέπει να ενημερώνονται για τις ευθύνες τους και τις διαδικασίες που πρέπει να ακολουθούνται για την προστασία των πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED στα CIS. Οι ευθύνες και οι διαδικασίες που πρέπει να ακολουθούνται πρέπει να είναι καταγεγραμμένες και οι χρήστες πρέπει να δηλώνουν εγγράφως ότι έχουν λάβει γνώση τους.

19. Πρέπει να υπάρχουν λειτουργικές διαδικασίες ασφαλείας (SecOPs) για τους χρήστες και τους διαχειριστές, αυτές δε πρέπει να περιλαμβάνουν περιγραφές των ρόλων ασφαλείας και σχετικούς καταλόγους καθηκόντων, εντολών και σχεδίων.

Τήρηση αρχείων, έλεγχος και αντιμετώπιση περιστατικών

20. Κάθε πρόσβαση στα CIS πρέπει να καταγράφεται.

21. Τα ακόλουθα περιστατικά πρέπει να καταγράφονται:

    α) κάθε προσπάθεια σύνδεσης, είτε είναι επιτυχής είτε ανεπιτυχής·

    β) κάθε αποσύνδεση (συμπεριλαμβανομένων, κατά περίπτωση, των αποσυνδέσεων που οφείλονται σε συμπλήρωση του χρόνου λήξης της σύνδεσης)·

    γ) η δημιουργία, διαγραφή ή τροποποίηση δικαιωμάτων και προνομίων πρόσβασης·

    δ) η δημιουργία, διαγραφή ή τροποποίηση κωδικών πρόσβασης.

22. Για όλα τα προαναφερόμενα περιστατικά, πρέπει να κοινοποιούνται τουλάχιστον οι ακόλουθες πληροφορίες:

    α) το είδος του περιστατικού·

    β) το μοναδικό αναγνωριστικό του χρήστη·

    γ) η ημερομηνία και η ώρα·

    δ) το μοναδικό αναγνωριστικό της συσκευής.

23. Τα τηρούμενα αρχεία θα πρέπει να διευκολύνουν τον υπεύθυνο ασφαλείας στην εξέταση των πιθανών περιστατικών ασφαλείας. Μπορούν επίσης να χρησιμοποιούνται στο πλαίσιο τυχόν νομικών ερευνών σε περίπτωση περιστατικού ασφαλείας. Όλα τα αρχεία ασφαλείας θα πρέπει να ελέγχονται τακτικά για τον εντοπισμό πιθανών περιστατικών ασφαλείας. Τα τηρούμενα αρχεία πρέπει να προστατεύονται από μη εξουσιοδοτημένη διαγραφή ή τροποποίηση.

24. Ο δικαιούχος πρέπει να διαθέτει καθορισμένη στρατηγική απόκρισης για την αντιμετώπιση περιστατικών ασφαλείας. Οι χρήστες και οι διαχειριστές πρέπει να έχουν λάβει εντολές σχετικά με τον τρόπο αντιμετώπισης περιστατικών, τον τρόπο αναφοράς τους και το τι πρέπει να πράξουν σε περίπτωση έκτακτης ανάγκης.

25. Για κάθε διαρροή ή υπόνοια διαρροής πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED πρέπει να υποβάλλεται αναφορά στη χορηγούσα αρχή. Η αναφορά πρέπει να περιέχει περιγραφή των σχετικών πληροφοριών και των περιστάσεων της διαρροής ή της εικαζόμενης διαρροής. Όλοι οι χρήστες των CIS πρέπει να έχουν ενημερωθεί για τον δέοντα τρόπο αναφοράς των διαπιστωμένων ή εικαζόμενων περιστατικών ασφαλείας στον υπεύθυνο ασφαλείας.

Δικτύωση και διασύνδεση

26. Σε περίπτωση κατά την οποία CIS του δικαιούχου τα οποία χειρίζονται πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED διασυνδέονται με CIS τα οποία δεν είναι πιστοποιημένα, υφίσταται σημαντικά αυξημένη απειλή τόσο για την ασφάλεια των CIS όσο και για την ασφάλεια των πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED τις οποίες χειρίζονται τα εν λόγω CIS. Αυτό περιλαμβάνει το διαδίκτυο και άλλα δημόσια ή ιδιωτικά CIS, όπως άλλα CIS που ανήκουν στον δικαιούχο ή σε υπεργολάβο. Στην περίπτωση αυτήν, ο δικαιούχος πρέπει να διενεργήσει εκτίμηση επικινδυνότητας για να προσδιορίσει τις πρόσθετες προδιαγραφές ασφαλείας που πρέπει να εφαρμοστούν στο πλαίσιο της διαδικασίας πιστοποίησης της ασφάλειας. Ο δικαιούχος υποβάλλει στη χορηγούσα αρχή και, εάν απαιτείται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις, στην αρμόδια αρχή πιστοποίησης της ασφάλειας (ΑΠΑ) δήλωση συμμόρφωσης με την οποία βεβαιώνεται ότι τα CIS του δικαιούχου και οι σχετικές διασυνδέσεις έχουν πιστοποιηθεί για τον χειρισμό ΔΠΕΕ επιπέδου RESTREINT UE/EU RESTRICTED.

27. Η εξ αποστάσεως πρόσβαση από άλλα συστήματα σε υπηρεσίες LAN (π.χ. η εξ αποστάσεως πρόσβαση σε ηλεκτρονικό ταχυδρομείο και η εξ αποστάσεως τεχνική υποστήριξη συστημάτων) απαγορεύεται, εκτός εάν εφαρμόζονται ειδικά μέτρα ασφαλείας που έχουν εγκριθεί από τη χορηγούσα αρχή και, εφόσον απαιτείται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις, από την αρμόδια ΑΠΑ.

Διαχείριση διαμόρφωσης

28. Πρέπει να υφίσταται και να συντηρείται τακτικά λεπτομερής διαμόρφωση υλισμικού και λογισμικού, όπως αποτυπώνεται στην τεκμηρίωση της πιστοποίησης/έγκρισης (συμπεριλαμβανομένων διαγραμμάτων του συστήματος και του δικτύου).

29. Ο υπεύθυνος ασφαλείας του δικαιούχου πρέπει να διενεργεί ελέγχους διαμόρφωσης του υλισμικού και του λογισμικού ώστε να διασφαλίζει ότι δεν έχει προστεθεί μη εγκεκριμένο υλισμικό ή λογισμικό.

30. Οι αλλαγές στη διαμόρφωση των CIS του δικαιούχου πρέπει να αξιολογούνται όσον αφορά τις επιπτώσεις τους στην ασφάλεια και πρέπει να εγκρίνονται από τον υπεύθυνο ασφαλείας και, εφόσον απαιτείται από τις εθνικές νομοθετικές και κανονιστικές διατάξεις, την ΑΠΑ.

31. Το σύστημα πρέπει να σαρώνεται για ενδεχόμενα τρωτά σημεία ασφαλείας τουλάχιστον μία φορά το τρίμηνο. Πρέπει να υπάρχει εγκατεστημένο και να ενημερώνεται τακτικά λογισμικό για την ανίχνευση κακόβουλου λογισμικού. Εάν είναι δυνατόν, το εν λόγω λογισμικό θα πρέπει να έχει εθνική ή αναγνωρισμένη διεθνή έγκριση, διαφορετικά θα πρέπει να αποτελεί ευρέως αποδεκτό πρότυπο για τον τομέα.

32. Ο δικαιούχος πρέπει να εκπονήσει σχέδιο συνέχισης των δραστηριοτήτων. Πρέπει να θεσπιστούν διαδικασίες εφεδρείας για τη ρύθμιση των ακόλουθων ζητημάτων:

    α) συχνότητα δημιουργίας εφεδρικών αντιγράφων·

    β) απαιτήσεις αποθήκευσης επιτόπου (πυρίμαχοι περιέκτες) ή εκτός της εγκατάστασης·

    γ) έλεγχος της εξουσιοδοτημένης πρόσβασης στα εφεδρικά αντίγραφα.

Καθαρισμός και καταστροφή

33. Τα CIS ή τα μέσα αποθήκευσης δεδομένων τα οποία σε οποιαδήποτε στιγμή περιλάμβαναν πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED πρέπει να υποβάλλονται στην ακόλουθη διαδικασία καθαρισμού ολόκληρου του συστήματος ή του μέσου αποθήκευσης πριν από την απόρριψή τους:

    α) οι μνήμες flash (π.χ. τα κλειδιά USB, οι κάρτες SD, οι δίσκοι στερεάς κατάστασης, οι υβριδικοί σκληροί δίσκοι) πρέπει να επεγγράφονται τουλάχιστον τρεις φορές και στη συνέχεια να επαληθεύεται ότι το αρχικό περιεχόμενο δεν μπορεί να ανακτηθεί, ή να καθαρίζονται με τη χρήση εγκεκριμένου λογισμικού διαγραφής δεδομένων·

    β) τα μαγνητικά μέσα (π.χ. οι σκληροί δίσκοι) πρέπει να επεγγράφονται ή να απομαγνητίζονται·

    γ) τα οπτικά μέσα (π.χ. τα CD και τα DVD) πρέπει να κατατεμαχίζονται ή να θρυμματίζονται·

    δ) ως προς τα λοιπά μέσα αποθήκευσης, πρέπει να ζητείται η γνώμη της χορηγούσας αρχής ή, κατά περίπτωση, της ΕΑΑ, ΚΑΑ ή ΑΠΑ σχετικά με τις προδιαγραφές ασφαλείας που πρέπει να πληρούνται.

34. Κάθε μέσο αποθήκευσης δεδομένων πρέπει να καθαρίζεται από κάθε πληροφορία με διαβάθμιση RESTREINT UE/EU RESTRICTED προτού δοθεί σε οποιαδήποτε οντότητα η οποία δεν έχει εξουσιοδότηση πρόσβασης σε πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED (π.χ. για εργασίες συντήρησης).

ΠΑΡΑΡΤΗΜΑ IV

Εξουσιοδότηση ασφαλείας φορέα και προσωπικού (FSC και ΕΑΠ) για τους δικαιούχους ή υπεργολάβους που έρχονται σε επαφή με πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED και εθνικές αρχές ασφαλείας ή καθορισμένες αρχές ασφαλείας (ΕΑΑ/ΚΑΑ) που απαιτούν κοινοποίηση των διαβαθμισμένων συμφωνιών επιδότησης επιπέδου RESTREINT UE/EU RESTRICTED [1]

Κράτος μέλος	FSC		Κοινοποίηση των συμφωνιών επιδότησης ή συμβάσεων υπεργολαβίας που συνεπάγονται επαφή με πληροφορίες με διαβάθμιση R-UE/EU-R στην ΕΑΑ και/ή την ΚΑΑ		ΕΑΠ	
	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΟΧΙ
Βέλγιο		**X**		**X**		**X**
Βουλγαρία		**X**		**X**		**X**
Τσεχία		**X**		**X**		**X**
Δανία	**X**		**X**		**X**	
Γερμανία		**X**		**X**		**X**
Εσθονία	**X**		**X**			**X**
Ιρλανδία		**X**		**X**		**X**
Ελλάδα	**X**			**X**	**X**	
Ισπανία		**X**	**X**			**X**
Γαλλία		**X**		**X**		**X**
Κροατία		**X**	**X**			**X**
Ιταλία		**X**	**X**			**X**
Κύπρος		**X**	**X**			**X**
Λετονία		**X**		**X**		**X**
Λιθουανία	**X**		**X**			**X**
Λουξεμβούργο	**X**		**X**		**X**	
Ουγγαρία		**X**		**X**		**X**
Μάλτα		**X**		**X**		**X**
Κάτω Χώρες	**X** (μόνο για τις συμφωνίες επιδότησης και τις συμβάσεις υπεργολαβίας που συνδέονται με τον τομέα της άμυνας)		**X** (μόνο για τις συμφωνίες επιδότησης και τις συμβάσεις υπεργολαβίας που συνδέονται με τον τομέα της άμυνας)			**X**
Αυστρία		**X**		**X**		**X**
Πολωνία		**X**		**X**		**X**

[1] Οι εν λόγω εθνικές απαιτήσεις για FSC/ΕΑΠ και κοινοποίηση για τις συμφωνίες επιδότησης που συνεπάγονται επαφή με πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED δεν πρέπει να επιβάλλουν πρόσθετες υποχρεώσεις σε άλλα κράτη μέλη ή δικαιούχους και υπεργολάβους υπό τη δικαιοδοσία τους.
Σημείωση: η κοινοποίηση των συμφωνιών επιδότησης που συνεπάγονται επαφή με πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET είναι υποχρεωτική.

Πορτογαλία		**X**		**X**		**X**
Ρουμανία		**X**		**X**		**X**
Σλοβενία	**X**		**X**			**X**
Σλοβακία	**X**		**X**			**X**
Φινλανδία		**X**		**X**		**X**
Σουηδία		**X**		**X**		**X**

ΠΑΡΑΡΤΗΜΑ V

ΚΑΤΑΛΟΓΟΣ ΤΩΝ ΕΘΝΙΚΩΝ ΑΡΧΩΝ ΑΣΦΑΛΕΙΑΣ / ΚΑΘΟΡΙΣΜΕΝΩΝ ΑΡΧΩΝ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΕΙΝΑΙ ΑΡΜΟΔΙΕΣ ΓΙΑ ΤΟΝ ΧΕΙΡΙΣΜΟ ΔΙΑΔΙΚΑΣΙΩΝ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗ ΒΙΟΜΗΧΑΝΙΚΗ ΑΣΦΑΛΕΙΑ

ΒΕΛΓΙΟ

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels

Τηλ. +32 25014542 (Γραμματεία)

Φαξ +32 25014596

Email: nvo-ans@diplobel.fed.be

ΒΟΥΛΓΑΡΙΑ

1. State Commission on Information Security — National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Τηλ. +359 29835775
   Φαξ +359 29873750
   Email: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Τηλ. +359 29227002
   Φαξ +359 29885211
   Email: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Τηλ. +359 29813221
   Φαξ +359 29862706
   Email: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Τηλ. +359 29824971
   Φαξ +359 29461339
   Email: dato@dato.bg

[Οι αρμόδιες αρχές που αναφέρονται παραπάνω διεξάγουν τις διαδικασίες ελέγχου για τη χορήγηση εξουσιοδότησης ασφαλείας φορέα (FSC) σε νομικά πρόσωπα που υποβάλλουν αίτηση για τη σύναψη διαβαθμισμένης σύμβασης και εξουσιοδότηση ασφαλείας προσωπικού (ΕΑΠ) σε φυσικά πρόσωπα που εκτελούν διαβαθμισμένη σύμβαση για τις ανάγκες των εν λόγω αρχών.]

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.

   1407 Sofia

   Τηλ. +359 28147109

   Φαξ +359 29632188, +359 28147441

   Email: dans@dans.bg

(Η παραπάνω υπηρεσία ασφαλείας διεξάγει τις διαδικασίες ελέγχου για τη χορήγηση FSC και ΕΑΠ σε όλες τις άλλες νομικές οντότητες και φυσικά πρόσωπα στη χώρα που υποβάλλουν αίτηση σύναψης διαβαθμισμένης σύμβασης ή διαβαθμισμένης συμφωνίας επιδότησης ή εκτελούν διαβαθμισμένη σύμβαση ή διαβαθμισμένη συμφωνία επιδότησης).

ΤΣΕΧΙΑ

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56

Τηλ. +420 257283129

Email: sbr@nbu.cz

ΔΑΝΙΑ

1. Politiets Efterretningstjeneste
   (Danish Security Intelligence Service)

   Klausdalsbrovej 1

   2860 Søborg

   Τηλ. +45 33148888

   Φαξ +45 33430190

2. Forsvarets Efterretningstjeneste
   (Danish Defence Intelligence Service)
   Kastellet 30
   2100 Copenhagen Ø

   Τηλ. +45 33325566

   Φαξ +45 33931320

ΓΕΡΜΑΝΙΑ

1. Για θέματα που αφορούν την πολιτική για τη βιομηχανική ασφάλεια, εξουσιοδοτήσεις ασφαλείας (FSC), σχέδια μεταφοράς [πλην για κρυπτογραφικό υλικό/ελεγχόμενο κρυπτογραφικό στοιχείο (CCI)]:
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division - RS3

   Villemombler Str. 76

   53123 Bonn

   Τηλ. +49 228996154028

   Φαξ +49 228996152676

   Email: dsagermany-rs3@bmwi.bund.de (υπηρεσιακή διεύθυνση ηλεκτρονικού ταχυδρομείου)

2. Για συνήθεις αιτήσεις επίσκεψης από/προς γερμανικές εταιρείες:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS2
Villemombler Str. 76
53123 Bonn

Τηλ. +49 228996152401

Φαξ +49 228996152603

Email: rs2-international@bmwi.bund.de (υπηρεσιακή διεύθυνση ηλεκτρονικού ταχυδρομείου)

3. Σχέδια μεταφοράς για κρυπτογραφικό υλικό:

Federal Office for Information Security (BSI)
National Distribution Agency / NDA-EU DEU
Mainzer Str. 84
53179 Bonn

Τηλ. +49 2289995826052

Φαξ +49 228991095826052

Email: NDAEU@bsi.bund.de

ΕΣΘΟΝΙΑ

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn

Τηλ. +372 6939211

Φαξ +372 6935001

Email: nsa@fis.gov.ee

ΙΡΛΑΝΔΙΑ

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45

Τηλ. +353 14082724

Email: nsa@dfa.ie

ΕΛΛΑΔΑ

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens

Τηλ. +30 2106572022, +30 2106572178

Φαξ +30 2106527612

Email: daa.industrial@hndgs.mil.gr

ΙΣΠΑΝΙΑ

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Τηλ. +34 912832583, +34 912832752, +34 913725928

Φαξ +34 913725808

Email: nsa-sp@areatec.com

Για πληροφορίες σχετικά με διαβαθμισμένα προγράμματα: programas.ons@areatec.com

Για υποθέσεις που αφορούν εξουσιοδοτήσεις ασφαλείας προσωπικού: hps.ons@areatec.com

Για σχέδια μεταφοράς και διεθνείς επισκέψεις: sp-ivtco@areatec.com

ΓΑΛΛΙΑ

National Security Authority (NSA) (για θέματα πολιτικής και εφαρμογής σε τομείς εκτός της αμυντικής βιομηχανίας)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Τηλ. +33 171758193

Φαξ +33 171758200

Email: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (για θέματα εφαρμογής στην αμυντική βιομηχανία)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15

Τηλ. +33 988670421

Email: για έντυπα και εξερχόμενες αιτήσεις επισκέψεων: dga-ssdi.ai.fct@intradef.gouv.fr

για εισερχόμενες αιτήσεις επισκέψεων: dga-ssdi.visit.fct@intradef.gouv.fr

ΚΡΟΑΤΙΑ

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb

Τηλ. +385 14681222

Φαξ +385 14686049

Email: NSACroatia@uvns.hr

ΙΤΑΛΙΑ

Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna 15
00187 Roma

Τηλ. +39 0661174266

Φαξ +39 064885273

ΚΥΠΡΟΣ

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

Email: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia

Τηλ. +357 22807569, +357 22807764

Φαξ +357 22302351

Email: cynsa@mod.gov.cy

ΛΕΤΟΝΙΑ

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001

Τηλ. +371 67025418, +371 67025463

Φαξ +371 67025454

Email: ndi@sab.gov.lv, ndi@zd.gov.lv

ΛΙΘΟΥΑΝΙΑ

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Pilaitės pr. 19
LT-06264 Vilnius

Τηλ. +370 70666128

Email: nsa@vsd.lt

ΛΟΥΞΕΜΒΟΥΡΓΟ

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg

Τηλ. +352 24782210

Email: ans@me.etat.lu

ΟΥΓΓΑΡΙΑ

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Τηλ. +36 13911862

Φαξ +36 13911889

Email: nbf@nbf.hu

ΜΑΛΤΑ

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010

Τηλ. +356 23952000

Φαξ +356 21242406

Email: certification@mccaa.org.mt

ΚΑΤΩ ΧΩΡΕΣ

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague

Τηλ. +31 703204400

Φαξ +31 703200733

Email: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague

Τηλ. +31 704419407

Φαξ +31 703459189

Email: indussec@mindef.nl

ΑΥΣΤΡΙΑ

1. Federal Chancellery of Austria
Department I/10, Federal Office for Information Security

Ballhausplatz 2
10104 Vienna

Τηλ. +43 153115202594

Email: isk@bka.gv.at

2. ΚΑΑ στον τομέα της άμυνας:
BMLV/Abwehramt

Postfach 2000
1030 Vienna

Email: abwa@bmlvs.gv.at

ΠΟΛΩΝΙΑ

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw

Τηλ. +48 225857944

Φαξ +48 225857443

Email: nsa@abw.gov.pl

ΠΟΡΤΟΓΑΛΙΑ

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon

Τηλ. +351 213031710

Φαξ +351 213031711

Email: sind@gns.gov.pt, franco@gns.gov.pt

ΡΟΥΜΑΝΙΑ

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
Romanian NSA - ORNISS - National Registry Office for Classified Information
4th Mures Street
012275 Bucharest

Τηλ. +40 212075115

Φαξ +40 212245830

Email: relatii.publice@orniss.ro, nsa.romania@nsa.ro

ΣΛΟΒΕΝΙΑ

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Τηλ. +386 14781390

Φαξ +386 14781399

Email: gp.uvtp@gov.si

ΣΛΟΒΑΚΙΑ

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava

Τηλ. +421 268691111

Φαξ +421 268691700

Email: podatelna@nbu.gov.sk

ΦΙΝΛΑΝΔΙΑ

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Email: NSA@formin.fi

ΣΟΥΗΔΙΑ

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK / NSA
   SE-103 39 Stockholm
   Τηλ. +46 84051000
   Φαξ +46 87231176
   Email: ud-nsa@gov.se

2. ΚΑΑ
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Τηλ. +46 87824000
   Φαξ +46 87826900
   Email: security@fmv.se