1.4.2014 EL Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης C 96/1

II

(Ανακοινώσεις)

ΑΝΑΚΟΙΝΩΣΕΙΣ ΤΩΝ ΘΕΣΜΙΚΩΝ ΚΑΙ ΛΟΙΠΩΝ ΟΡΓΑΝΩΝ ΚΑΙ ΤΩΝ ΟΡΓΑΝΙΣΜΩΝ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ

ΑΠΟΦΑΣΗ ΤΟΥ ΠΡΟΕΔΡΕΙΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ

της 15ης Απριλίου 2013

σχετικά με τους κανόνες που διέπουν την επεξεργασία των εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο

(2014/C 96/01)

ΤΟ ΠΡΟΕΔΡΕΙΟ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ,

Έχοντας υπόψη το άρθρο 23 παράγραφος 12 του Κανονισμού του Ευρωπαϊκού Κοινοβουλίου,

Εκτιμώντας τα εξής:

(1) Δεδομένων της συμφωνίας-πλαισίου για τις σχέσεις μεταξύ του Ευρωπαϊκού Κοινοβουλίου και της Ευρωπαϊκής Επιτροπής ([1]) που υπεγράφη στις 20 Οκτωβρίου 2010 («συμφωνία-πλαίσιο») και της διοργανικής συμφωνίας μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη διαβίβαση προς το Ευρωπαϊκό Κοινοβούλιο και τον χειρισμό από αυτό διαβαθμισμένων πληροφοριών του Συμβουλίου πλην εκείνων του τομέα της κοινής εξωτερικής πολιτικής και της πολιτικής ασφάλειας ([2]) που υπεγράφη στις 12 Μαρτίου 2014, («διοργανική συμφωνία») είναι αναγκαίο να καθοριστούν ειδικοί κανόνες σχετικά με την επεξεργασία των εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο.

(2) Η Συνθήκη της Λισαβόνας αναθέτει νέα καθήκοντα στο Ευρωπαϊκό Κοινοβούλιο και, προκειμένου να αναπτυχθούν πρωτοβουλίες του Κοινοβουλίου στους τομείς εκείνους που απαιτούν ένα βαθμό εμπιστευτικότητας, είναι απαραίτητο να θεσπιστούν βασικές αρχές, ελάχιστα πρότυπα ασφάλειας και κατάλληλες διαδικασίες για την επεξεργασία εμπιστευτικών αλλά και διαβαθμισμένων πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο.

(3) Οι κανόνες που ορίζονται στην απόφαση αυτή έχουν ως στόχο να διασφαλίσουν ισοδύναμα πρότυπα προστασίας και συμβατότητα με τους κανόνες που έχουν θεσπίσει άλλα όργανα, οργανισμοί, γραφεία και υπηρεσίες που έχουν ιδρυθεί βάσει των Συνθηκών ή από τα κράτη μέλη, προκειμένου να καταστεί δυνατή η εύρυθμη λειτουργία της διαδικασίας λήψης αποφάσεων στην Ευρωπαϊκή Ένωση.

(4) Οι διατάξεις της απόφασης αυτής δεν θίγουν τους υφιστάμενους και τους μελλοντικούς κανόνες σχετικά με την πρόσβαση σε έγγραφα, που θεσπίζονται σύμφωνα με το άρθρο 15 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).

([1]) ΕΕ L 304, 20.11.2010, σ. 47.
([2]) ΕΕ C 95, 1.4.2014, σ. 1.

(5) Οι διατάξεις της απόφασης αυτής δεν θίγουν τους υφιστάμενους και τους μελλοντικούς κανόνες σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα, που θεσπίζονται σύμφωνα με το άρθρο 16 ΣΛΕΕ,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Σκοπός

Η παρούσα απόφαση διέπει τη διαχείριση και το χειρισμό εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο, συμπεριλαμβανομένων της δημιουργίας, παραλαβής, διαβίβασης και αποθήκευσης τέτοιων πληροφοριών με στόχο την ενδεδειγμένη προστασία του εμπιστευτικού τους χαρακτήρα. Εφαρμόζει τη διοργανική συμφωνία και τη συμφωνία πλαίσιο, ιδίως το Παράρτημα ΙΙ αυτής.

Άρθρο 2

Ορισμοί

Για τους σκοπούς της παρούσας απόφασης:

α) ως «πληροφορία» νοείται κάθε προφορική ή γραπτή πληροφόρηση, ανεξάρτητα από το μέσο στο οποίο διατίθεται ή τον συντάκτη της·

β) ως «εμπιστευτική πληροφορία» νοείται η «διαβαθμισμένη πληροφορία» και η μη διαβαθμισμένη «άλλη εμπιστευτική πληροφορία»·

γ) ως «διαβαθμισμένη πληροφορία» νοείται η «διαβαθμισμένη πληροφορία ΕΕ» και η «ισοδύναμη διαβαθμισμένη πληροφορία»·

δ) ως «διαβαθμισμένη πληροφορία ΕΕ» (ΔΠΕΕ) νοείται κάθε πληροφορία και υλικό που έχει διαβαθμιστεί ως «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET», «CONFIDENTIEL UE/EU CONFIDENTIAL» ή «RESTREINT UE/EU RESTRICTED», των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σε ποικίλο βαθμό τα συμφέροντα της Ένωσης, ή ενός ή περισσότερων κρατών μελών της, είτε η πληροφορία αυτή προέρχεται από όργανα, οργανισμούς, γραφεία ή υπηρεσίες που έχουν συσταθεί από ή με βάση τις Συνθήκες είτε όχι. Στο πλαίσιο αυτό, πληροφορίες και υλικό που διαβαθμίζονται σε επίπεδο:

— «TRÈS SECRET UE/EU TOP SECRET» για πληροφορίες και υλικό, η άνευ αδείας κοινολόγηση των οποίων θα μπορούσε να βλάψει σοβαρότατα τα ζωτικά συμφέροντα της Ένωσης ή ενός ή περισσοτέρων κρατών μελών της·

— «SECRET UE/EU SECRET» για πληροφορίες και υλικό, η άνευ αδείας κοινολόγηση των οποίων θα μπορούσε να βλάψει σοβαρά τα ζωτικά συμφέροντα της Ένωσης ή ενός ή περισσοτέρων κρατών μελών της·

— «CONFIDENTIEL UE/EU CONFIDENTIAL» για πληροφορίες και υλικό, η άνευ αδείας κοινολόγηση των οποίων θα μπορούσε να βλάψει τα ζωτικά συμφέροντα της Ένωσης ή ενός ή περισσοτέρων κρατών μελών της·

— «RESTREINT UE/EU RESTRICTED» για πληροφορίες και υλικό, η άνευ αδείας κοινολόγηση των οποίων θα μπορούσε να είναι αντίθετη προς τα συμφέροντα της Ένωσης ή ενός ή περισσοτέρων κρατών μελών της·

ε) ως «ισοδύναμη διαβαθμισμένη πληροφορία» νοείται η διαβαθμισμένη πληροφορία που προέρχεται από κράτη μέλη, τρίτα κράτη ή διεθνείς οργανισμούς, φέρει σήμανση διαβάθμισης ασφαλείας ισοδύναμη προς μία από τις χρησιμοποιούμενες σημάνσεις διαβάθμισης ασφαλείας για τις ΔΠΕΕ και έχει διαβιβαστεί στο Ευρωπαϊκό Κοινοβούλιο από το Συμβούλιο ή την Επιτροπή·

στ) ως «άλλη εμπιστευτική πληροφορία» νοείται οποιαδήποτε άλλη μη διαβαθμισμένη εμπιστευτική πληροφορία, συμπεριλαμβανομένων των πληροφοριών που καλύπτονται από κανόνες περί προστασίας δεδομένων ή από υποχρέωση επαγγελματικής εχεμύθειας, που έχει δημιουργηθεί στο Ευρωπαϊκό Κοινοβούλιο ή έχει διαβιβασθεί στο Ευρωπαϊκό Κοινοβούλιο από άλλα όργανα, οργανισμούς, γραφεία και αρχές που έχουν συσταθεί από ή με βάση τις Συνθήκες ή από τα κράτη μέλη·

ζ) ως «έγγραφο» νοείται κάθε καταγεγραμμένη πληροφορία ανεξαρτήτως της φυσικής της μορφής ή των χαρακτηριστικών γνωρισμάτων της·

η) ως «υλικό» νοείται κάθε έγγραφο ή αντικείμενο ή μηχανή ή εξοπλισμός που είτε έχει κατασκευασθεί ή βρίσκεται σε διαδικασία κατασκευής·

θ) ως «ανάγκη γνώσης» νοείται η ανάγκη ενός προσώπου να αποκτήσει πρόσβαση σε εμπιστευτική πληροφορία προκειμένου να μπορεί να ασκεί ένα επίσημο καθήκον ή μία εργασία·

ι) ως «άδεια» νοείται μία απόφαση που εκδίδει ο Πρόεδρος, προκειμένου για μέλη του Ευρωπαϊκού Κοινοβουλίου, ή ο Γενικός Γραμματέας, προκειμένου για υπαλλήλους του Ευρωπαϊκού Κοινοβουλίου και λοιπό προσωπικό του Ευρωπαϊκού Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, με την οποία χορηγείται ατομική πρόσβαση σε διαβαθμισμένες πληροφορίες έως ένα συγκεκριμένο επίπεδο, βάσει του θετικού αποτελέσματος ενός ελέγχου ασφάλειας που διενεργείται από εθνική αρχή στο πλαίσιο του εθνικού δικαίου και βάσει των διατάξεων που θεσπίζονται στο Παράρτημα Ι Μέρος 2·

ια) ως «υποχαρακτηρισμός» νοείται η μείωση του βαθμού ασφάλειας·

ιβ) ως «αποχαρακτηρισμός» νοείται η άρση οποιασδήποτε διαβάθμισης·

ιγ) ως «σήμανση» νοείται διακριτικό γνώρισμα που τίθεται σε «άλλες εμπιστευτικές πληροφορίες» προκειμένου να προσδιοριστούν προκαθορισμένες ειδικές οδηγίες σχετικά με τον χειρισμό των πληροφοριών αυτών ή το πεδίο που καλύπτεται από συγκεκριμένο έγγραφο. Μπορεί επίσης να τεθεί σε διαβαθμισμένες πληροφορίες προκειμένου να επιβληθούν πρόσθετες απαιτήσεις όσον αφορά το χειρισμό τους·

ιδ) ως «αφαίρεση της σήμανσης» νοείται η άρση οποιασδήποτε σήμανσης·

ιε) ως «αρχικός συντάκτης» νοείται ο δεόντως εξουσιοδοτημένος συντάκτης εμπιστευτικής πληροφορίας·

ιστ) ως «κοινοποιήσεις ασφάλειας» νοούνται τα μέτρα εφαρμογής που θεσπίζονται στο Παράρτημα ΙΙ·

ιζ) ως «οδηγίες χειρισμού» νοούνται οι τεχνικές οδηγίες που εκδίδονται προς τις υπηρεσίες του Ευρωπαϊκού Κοινοβουλίου σχετικά με τη διαχείριση εμπιστευτικών πληροφοριών.

Άρθρο 3

Βασικές αρχές και ελάχιστα πρότυπα

1. Η επεξεργασία εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο ακολουθεί τις βασικές αρχές και τους ελάχιστους κανόνες που θεσπίζονται στο Παράρτημα Ι Μέρος 1.

2. Το Ευρωπαϊκό Κοινοβούλιο συγκροτεί ένα σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ΣΔΑΠ) σύμφωνα με τις βασικές αυτές αρχές και τα ελάχιστα αυτά πρότυπα. Το ΣΔΑΠ αποτελείται από τις κοινοποιήσεις ασφάλειας, τις οδηγίες χειρισμού και τον οικείο Κανονισμό. Το ΣΔΑΠ αποσκοπεί στο να διευκολύνει το κοινοβουλευτικό και διοικητικό έργο, διασφαλίζοντας συγχρόνως την προστασία κάθε εμπιστευτικής πληροφορίας που επεξεργάζεται το Ευρωπαϊκό Κοινοβούλιο, σεβόμενο πλήρως τους κανόνες που έχει θεσπίσει ο αρχικός συντάκτης των πληροφοριών αυτών, όπως καθορίζονται στις κοινοποιήσεις ασφάλειας.

Η επεξεργασία εμπιστευτικών πληροφοριών μέσω ενός αυτόματου συστήματος επικοινωνιών και πληροφοριών (ΣΕΠ) του Ευρωπαϊκού Κοινοβουλίου διεξάγεται σύμφωνα με το σύστημα ασφάλειας των πληροφοριών (ΑΠ), όπως ορίζεται στην κοινοποίηση ασφάλειας 3.

3. Τα μέλη του Ευρωπαϊκού Κοινοβουλίου μπορούν να συμβουλεύονται διαβαθμισμένες πληροφορίες μέχρι και το επίπεδο «RESTREINT UE/EU RESTRICTED» χωρίς έλεγχο ασφάλειας.

4. Όταν οι σχετικές πληροφορίες έχουν διαβαθμιστεί σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή σε ισοδύναμό του, διατίθενται μόνο στα μέλη του Ευρωπαϊκού Κοινοβουλίου που έχουν εξουσιοδοτηθεί από τον Πρόεδρο σύμφωνα με την παράγραφο 5 ή έχουν υπογράψει επίσημη δήλωση μη κοινολόγησης του περιεχομένου των πληροφοριών αυτών σε τρίτους, τήρησης της υποχρέωσης προστασίας των πληροφοριών διαβαθμισμένων σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL και αποδοχής των συνεπειών σε περίπτωση μη συμμόρφωσης.

5. Όταν οι πληροφορίες έχουν διαβαθμισθεί σε επίπεδο SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του, διατίθενται μόνο στα μέλη του Ευρωπαϊκού Κοινοβουλίου που έχουν εξουσιοδοτηθεί από τον Πρόεδρο εφόσον:

α) έχουν ελεγχθεί από απόψεως ασφαλείας σύμφωνα με το Παράρτημα Ι Μέρος 2 της παρούσας απόφασης, ή

β) έχει γίνει κοινοποίηση από αρμόδια εθνική αρχή ότι τα εν λόγω μέλη είναι δεόντως εξουσιοδοτημένα δυνάμει των καθηκόντων τους σύμφωνα με το εθνικό δίκαιο.

6. Προ της χορήγησης πρόσβασης σε διαβαθμισμένες πληροφορίες, τα μέλη του Ευρωπαϊκού Κοινοβουλίου ενημερώνονται και δηλώνουν ότι έχουν κατανοήσει σαφώς την ευθύνη τους να προστατεύουν τις πληροφορίες αυτές σύμφωνα με το Παράρτημα Ι. Ενημερώνονται επίσης σχετικά με τα μέσα για τη διασφάλιση της προστασίας αυτής.

7. Οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες μπορούν να συμβουλεύονται εμπιστευτικές πληροφορίες εφόσον έχουν διαπιστωμένη «ανάγκη γνώσης» και μπορούν να συμβουλεύονται διαβαθμισμένες πληροφορίες πάνω από το επίπεδο RESTREINT UE/EU RESTRICTED, εφόσον διαθέτουν το κατάλληλο επίπεδο ελέγχου ασφάλειας. Πρόσβαση σε διαβαθμισμένες πληροφορίες χορηγείται μόνο εφόσον έχουν ενημερωθεί και έχουν λάβει γραπτές οδηγίες ως προς τις ευθύνες τους για την προστασία των εν λόγω πληροφοριών καθώς και σχετικά με τα μέσα διασφάλισης της προστασίας αυτής, και εφόσον έχουν υπογράψει δήλωση με την οποία αναγνωρίζουν την παραλαβή των οδηγιών αυτών και δεσμεύονται ότι θα τις τηρήσουν σύμφωνα με τους υφιστάμενους κανόνες.

Άρθρο 4

Δημιουργία εμπιστευτικών πληροφοριών και διοικητική διαχείριση από το Ευρωπαϊκό Κοινοβούλιο

1. Ο Πρόεδρος του Ευρωπαϊκού Κοινοβουλίου, οι πρόεδροι των αρμόδιων κοινοβουλευτικών επιτροπών και ο Γενικός Γραμματέας ή/και κάθε πρόσωπο δεόντως εξουσιοδοτημένο από αυτόν εγγράφως μπορούν να αποτελούν τον αρχικό συντάκτη εμπιστευτικών πληροφοριών ή/και να διαβαθμίζουν πληροφορίες, όπως ορίζεται στις κοινοποιήσεις ασφάλειας.

2. Κατά τη δημιουργία διαβαθμισμένης πληροφορίας, ο αρχικός συντάκτης εφαρμόζει το ενδεδειγμένο επίπεδο διαβάθμισης σύμφωνα με τα διεθνή πρότυπα και τους ορισμούς που εκτίθενται στο Παράρτημα Ι. Κατά κανόνα, ο αρχικός συντάκτης καθορίζει επίσης τους αποδέκτες που εξουσιοδοτούνται να συμβουλεύονται τις πληροφορίες που αντιστοιχούν στο επίπεδο διαβάθμισης. Οι πληροφορίες αυτές κοινοποιούνται στη Μονάδα Διαβαθμισμένων Πληροφοριών (CIU) όταν το έγγραφο κατατίθεται σε αυτήν.

3. «Άλλες εμπιστευτικές πληροφορίες» που καλύπτονται από επαγγελματικό απόρρητο εξετάζονται σύμφωνα με τα Παραρτήματα Ι και ΙΙ και τις οδηγίες χειρισμού.

Άρθρο 5

Παραλαβή εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο

1. Οι εμπιστευτικές πληροφορίες που παραλαμβάνει το Ευρωπαϊκό Κοινοβούλιο γνωστοποιούνται όπως ακολούθως:

α) πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλη εμπιστευτική πληροφορία» στη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου που υπέβαλε τη σχετική αίτηση ή απευθείας στην CIU·

β) πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του: στην CIU.

2. Η καταχώριση, αποθήκευση και ανιχνευσιμότητα εμπιστευτικών πληροφοριών διασφαλίζεται, κατά περίπτωση, είτε από τη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου που παρέλαβε την πληροφορία είτε από την CIU.

3. Οι συμφωνηθείσες ρυθμίσεις που θεσπίζονται με κοινή συμφωνία με σκοπό τη διαφύλαξη της εμπιστευτικότητας των πληροφοριών, σε περίπτωση γνωστοποίησης εμπιστευτικών πληροφοριών από την Επιτροπή σύμφωνα με το σημείο 3.2 του Παραρτήματος ΙΙ της συμφωνίας-πλαίσιο ή στην περίπτωση διαβίβασης διαβαθμισμένων πληροφοριών από το Συμβούλιο σύμφωνα με το άρθρο 5 παράγραφος 4 της διοργανικής συμφωνίας, κατατίθενται μαζί με τις εμπιστευτικές πληροφορίες στη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου ή στην CIU, κατά περίπτωση.

4. Οι ρυθμίσεις της παραγράφου 3 μπορούν επίσης να εφαρμοστούν τηρουμένων των αναλογιών για τη γνωστοποίηση εμπιστευτικών πληροφοριών από άλλα όργανα, οργανισμούς, γραφεία και υπηρεσίες που έχουν συσταθεί από ή με βάση τις Συνθήκες ή από τα κράτη μέλη.

5. Προκειμένου να διασφαλιστεί επίπεδο προστασίας αντίστοιχο με το επίπεδο διαβάθμισης TRÈS SECRET UE/EU TOP SECRET ή με ισοδύναμό του, η Διάσκεψη των Προέδρων συγκροτεί επιτροπή εποπτείας. Οι πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του γνωστοποιούνται στο Ευρωπαϊκό Κοινοβούλιο με επιφύλαξη περαιτέρω ρυθμίσεων που θα συμφωνηθούν μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του οργάνου της Ένωσης από το οποίο προέρχονται οι πληροφορίες.

Άρθρο 6

Γνωστοποίηση διαβαθμισμένων πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο σε τρίτους

Το Ευρωπαϊκό Κοινοβούλιο μπορεί, με τη προηγούμενη γραπτή συγκατάθεση του αρχικού συντάκτη ή του θεσμικού οργάνου της Ένωσης που γνωστοποίησε τις διαβαθμισμένες πληροφορίες στο Ευρωπαϊκό Κοινοβούλιο, κατά περίπτωση, να διαβιβάσει τις εν λόγω διαβαθμισμένες πληροφορίες σε τρίτους, υπό την προϋπόθεση ότι διασφαλίζουν ότι, κατά την επεξεργασία των πληροφοριών αυτών, τηρούνται στις υπηρεσίες και τις εγκαταστάσεις τους κανόνες ισοδύναμοι προς τους κανόνες που ορίζονται στην παρούσα απόφαση.

Άρθρο 7

Ασφαλείς εγκαταστάσεις

1. Για τους σκοπούς της διαχείρισης των εμπιστευτικών πληροφοριών το Ευρωπαϊκό Κοινοβούλιο δημιουργεί έναν ασφαλή χώρο και ασφαλείς αίθουσες ανάγνωσης.

2. Ο ασφαλής χώρος παρέχει διευκολύνσεις για την καταχώριση, αναζήτηση στοιχείων, αρχειοθέτηση, διαβίβαση και επεξεργασία διαβαθμισμένων πληροφοριών. Περιλαμβάνει, μεταξύ άλλων, αίθουσα ανάγνωσης και αίθουσα συνεδριάσεων προκειμένου τα εξουσιοδοτημένα άτομα να συμβουλεύονται διαβαθμισμένες πληροφορίες και τη διαχείρισή του έχει η CIU.

3. Εκτός του ασφαλούς χώρου, μπορούν να δημιουργηθούν ασφαλείς αίθουσες ανάγνωσης, ώστε να μπορούν τα εξουσιοδοτημένα άτομα να συμβουλεύονται πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του, και «άλλες εμπιστευτικές πληροφορίες». Αυτές οι ασφαλείς αίθουσες ανάγνωσης διευθύνονται από τις αρμόδιες υπηρεσίες της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου ή από την CIU, κατά περίπτωση. Δεν περιέχουν φωτοαντιγραφικά μηχανήματα, τηλέφωνα, τηλεομοιοτυπικά μηχανήματα (fax), σαρωτές (scanners) ή άλλα τεχνικά μέσα αναπαραγωγής ή διαβίβασης εγγράφων.

Άρθρο 8

Καταχώριση, χειρισμός και αποθήκευση εμπιστευτικών πληροφοριών

1. Πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλες εμπιστευτικές πληροφορίες» καταχωρίζονται και αποθηκεύονται από τις αρμόδιες υπηρεσίες της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου ή από την CIU, ανάλογα με το ποιος έλαβε τις πληροφορίες.

2. Οι ακόλουθοι όροι ισχύουν όσον αφορά το χειρισμό των πληροφοριών που έχουν διαβαθμιστεί σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλων εμπιστευτικών πληροφοριών»:

α) τα έγγραφα παραδίδονται προσωπικά στον προϊστάμενο της γραμματείας, ο οποίος τα καταχωρεί και εκδίδει απόδειξη παραλαβής·

β) τα έγγραφα αυτά, εφόσον δεν χρησιμοποιούνται, τηρούνται σε χώρο στον οποίο απαγορεύεται η πρόσβαση, υπό την ευθύνη της γραμματείας·

γ) σε καμία περίπτωση δεν μπορούν οι πληροφορίες να αποθηκευθούν σε άλλο μέσο, ή να διαβιβαστούν σε οποιοδήποτε πρόσωπο. Τα έγγραφα αυτά μπορούν να αναπαραχθούν μέσω δεόντως εγκεκριμένου εξοπλισμού όπως ορίζεται στις κοινοποιήσεις ασφάλειας·

δ) η πρόσβαση στα έγγραφα αυτά περιορίζεται σε όσους ορίζονται από τον αρχικό συντάκτη ή από το θεσμικό όργανο της Ένωσης που γνωστοποίησε την πληροφορία στο Ευρωπαϊκό Κοινοβούλιο, σύμφωνα με τις ρυθμίσεις που αναφέρονται στο άρθρο 4 παράγραφος 2 ή στο άρθρο 5 παράγραφοι 3, 4 και 5·

ε) η γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου τηρεί μητρώο των προσώπων που εξέτασαν τις πληροφορίες, και της ημερομηνίας και του χρόνου της εξέτασης αυτής, και διαβιβάζει το μητρώο στην CIU κατά τη στιγμή της κατάθεσης των πληροφοριών στην CIU.

3. Οι πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του καταχωρίζονται, τυγχάνουν επεξεργασίας και αποθηκεύονται από την CIU στον Ασφαλή Χώρο, σύμφωνα με το εκάστοτε επίπεδο διαβάθμισης και όπως ορίζεται στις κοινοποιήσεις ασφάλειας.

4. Σε περίπτωση παραβίασης των κανόνων που καθορίζονται στις παραγράφους 1 έως 3, ο αρμόδιος υπάλληλος της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου ή της CIU, κατά περίπτωση, ενημερώνει σχετικώς τον Γενικό Γραμματέα, ο οποίος παραπέμπει το θέμα στον Πρόεδρο σε περίπτωση που ενέχεται βουλευτής του Ευρωπαϊκού Κοινοβουλίου.

Άρθρο 9

Πρόσβαση στις εγκαταστάσεις ασφαλείας

1. Στον Ασφαλή Χώρο έχουν πρόσβαση μόνο τα ακόλουθα πρόσωπα:

α) πρόσωπα εξουσιοδοτημένα, σύμφωνα με το άρθρο 3 παράγραφοι 4 έως 7, να συμβουλεύονται τις πληροφορίες που τηρούνται στο χώρο αυτό και τα οποία έχουν υποβάλει αίτηση σύμφωνα με το άρθρο 10 παράγραφος 1·

β) πρόσωπα εξουσιοδοτημένα, σύμφωνα με το άρθρο 4 παράγραφος 1, να δημιουργούν διαβαθμισμένες πληροφορίες και τα οποία έχουν υποβάλει αίτηση σύμφωνα με το άρθρο 10 παράγραφος 1·

γ) οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου που εργάζονται στην CIU·

δ) οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου που ασκούν διαχειριστικά καθήκοντα στην ΥΕΠ·

ε) οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου που είναι αρμόδιοι για την ασφάλεια και την πυροπροστασία, όταν παρίσταται ανάγκη·

στ) το προσωπικό καθαρισμού μόνο παρουσία και υπό τη στενή επιτήρηση υπαλλήλου της CIU·

2. Η CIU δύναται να αρνηθεί την πρόσβαση στον ασφαλή χώρο σε κάθε μη εξουσιοδοτημένο πρόσωπο. Οιαδήποτε ένσταση κατά της άρνησης για πρόσβαση υποβάλλεται στον Πρόεδρο στην περίπτωση αίτησης πρόσβασης βουλευτών του Ευρωπαϊκού Κοινοβουλίου και στον Γενικό Γραμματέα στις άλλες περιπτώσεις.

3. Ο Γενικός Γραμματέας μπορεί να εγκρίνει τη διεξαγωγή συνεδρίασης περιορισμένου αριθμού ατόμων στην αίθουσα συνεδριάσεων στον ασφαλή χώρο.

4. Σε ασφαλή αίθουσα ανάγνωσης έχουν πρόσβαση μόνο τα ακόλουθα πρόσωπα:

α) οι βουλευτές του Ευρωπαϊκού Κοινοβουλίου, οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Ευρωπαϊκού Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, που ταυτοποιούνται δεόντως για τους σκοπούς της εξέτασης ή της δημιουργίας εμπιστευτικών πληροφοριών·

β) οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου που ασκούν διαχειριστικά καθήκοντα στο ΣΕΠ, οι υπάλληλοι της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου που έλαβαν τις πληροφορίες και οι υπάλληλοι της CIU·

γ) εφόσον απαιτείται, οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου που είναι αρμόδιοι για την ασφάλεια και την πυροπροστασία·

δ) το προσωπικό καθαρισμού μόνο παρουσία και υπό τη στενή επιτήρηση υπαλλήλου που εργάζεται στη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου ή στην CIU, κατά περίπτωση.

5. Η αρμόδια γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου ή η CIU, ανάλογα με την περίπτωση, δύναται να αρνηθεί την πρόσβαση σε ασφαλή αίθουσα ανάγνωσης σε κάθε μη εξουσιοδοτημένο πρόσωπο. Οιαδήποτε ένσταση κατά αυτής της άρνησης για πρόσβαση υποβάλλεται στον Πρόεδρο στην περίπτωση αίτησης πρόσβασης βουλευτών του Ευρωπαϊκού Κοινοβουλίου και στον Γενικό Γραμματέα στις άλλες περιπτώσεις.

Άρθρο 10

Εξέταση ή δημιουργία εμπιστευτικών πληροφοριών σε ασφαλείς εγκαταστάσεις

1. Κάθε πρόσωπο που επιθυμεί να εξετάσει ή να δημιουργήσει εμπιστευτικές πληροφορίες στον ασφαλή χώρο γνωστοποιεί εκ των προτέρων το όνομά του στην CIU. Η CIU ελέγχει την ταυτότητα κάθε προσώπου και εξακριβώνει εάν το πρόσωπο αυτό έχει σχετική άδεια προκειμένου να εξετάσει ή να δημιουργήσει εμπιστευτικές πληροφορίες, σύμφωνα με το άρθρο 3 παράγραφοι 3 έως 7, το άρθρο 4 παράγραφος 1 ή το άρθρο 5 παράγραφοι 3, 4 και 5·

2. Κάθε πρόσωπο που επιθυμεί, σύμφωνα με το άρθρο 3 παράγραφοι 3 και 7, να εξετάσει εμπιστευτικές πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του ή «άλλες εμπιστευτικές πληροφορίες» σε ασφαλή αίθουσα ανάγνωσης, γνωστοποιεί εκ των προτέρων το όνομά του στις αρμόδιες υπηρεσίες της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου ή στην CIU.

3. Με την επιφύλαξη εξαιρετικών συνθηκών (π.χ. όταν πολυάριθμες αιτήσεις εξέτασης υποβάλλονται σε βραχύ χρονικό διάστημα), μόνο ένα πρόσωπο κάθε φορά λαμβάνει άδεια για να εξετάσει εμπιστευτική πληροφορία σε ασφαλή εγκατάσταση, παρουσία ενός υπαλλήλου της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου ή της CIU.

4. Κατά τη διαδικασία ανάγνωσης, οι εξωτερικές επαφές (συμπεριλαμβανομένης της χρήσης τηλεφώνων ή άλλων τεχνολογικών συσκευών), η λήψη σημειώσεων και η φωτοαντιγραφική αναπαραγωγή ή φωτογράφηση των εμπιστευτικών πληροφοριών απαγορεύονται.

5. Πριν επιτρέψει σε ένα πρόσωπο να εγκαταλείψει την ασφαλή εγκατάσταση, ο υπάλληλος της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου ή της CIU ελέγχει ότι τα εμπιστευτικά έγγραφα που εξετάσθηκαν είναι ακόμη παρόντα, άθικτα και πλήρη.

6. Σε περίπτωση παραβίασης των ανωτέρω κανόνων, ο υπάλληλος της γραμματείας του κοινοβουλευτικού οργάνου/αξιωματούχου ή της CIU ενημερώνει σχετικώς τον Γενικό Γραμματέα, ο οποίος παραπέμπει το θέμα στον Πρόεδρο σε περίπτωση που ενέχεται βουλευτής του Ευρωπαϊκού Κοινοβουλίου.

Άρθρο 11

Ελάχιστα πρότυπα για την εξέταση εμπιστευτικών πληροφοριών σε κεκλεισμένων των θυρών συνεδρίαση εκτός των ασφαλών εγκαταστάσεων

1. Πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλες εμπιστευτικές πληροφορίες» μπορούν να εξετάζονται από μέλη κοινοβουλευτικών επιτροπών ή άλλων πολιτικών και διοικητικών οργάνων του Ευρωπαϊκού Κοινοβουλίου σε κεκλεισμένων των θυρών συνεδρίαση εκτός των ασφαλών εγκαταστάσεων.

2. Στις περιπτώσεις που προβλέπονται στην παράγραφο 1, η γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου που έχει αρμοδιότητα για τη συνεδρίαση διασφαλίζει ότι τηρούνται οι ακόλουθοι όροι:

α) μόνο τα πρόσωπα που ορίζονται από τον πρόεδρο της αρμόδιας επιτροπής ή οργάνου να συμμετάσχουν στη συνεδρίαση μπορούν να εισέλθουν στην αίθουσα συνεδρίασης·

β) όλα τα έγγραφα αριθμούνται, διανέμονται κατά την έναρξη της συνεδρίασης και συλλέγονται και πάλι μετά το πέρας της και δεν λαμβάνονται σημειώσεις, φωτοτυπίες ή φωτογραφίες των εγγράφων αυτών·

γ) τα πρακτικά της συνεδρίασης δεν κάνουν καμία αναφορά στο περιεχόμενο της συζήτησης για τις πληροφορίες που εξετάστηκαν. Μόνο η απόφαση, εφόσον υπάρξει, μπορεί να αναγράφεται στα πρακτικά·

δ) οι εμπιστευτικές πληροφορίες που παρέχονται προφορικά σε αποδέκτες στο Ευρωπαϊκό Κοινοβούλιο υποβάλλονται στον ισοδύναμο βαθμό προστασίας με αυτόν που εφαρμόζεται για τις εμπιστευτικές πληροφορίες που παρέχονται σε γραπτή μορφή·

ε) δεν διατηρείται κανένα συμπληρωματικό απόθεμα εγγράφων στις αίθουσες συνεδριάσεων·

στ) μόνο ο απαιτούμενος αριθμός αντιγράφων των εγγράφων διανέμεται στους συμμετέχοντες και στους διερμηνείς κατά την έναρξη της συνεδρίασης·

ζ) η κατηγορία διαβάθμισης/σήμανσης των εγγράφων προσδιορίζεται από τον πρόεδρο της συνεδρίασης κατά την έναρξη της συνεδρίασης·

η) οι συμμετέχοντες δεν αφαιρούν έγγραφα από την αίθουσα συνεδρίασης·

θ) όλα τα αντίγραφα των εγγράφων συλλέγονται και καταμετρώνται κατά τη λήξη της συνεδρίασης από τη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου· και

ι) απαγορεύεται η εισαγωγή συσκευών ηλεκτρονικής επικοινωνίας ή άλλων ηλεκτρονικών συσκευών στην αίθουσα συνεδριάσεων όπου εξετάζονται ή συζητούνται οι εν λόγω εμπιστευτικές πληροφορίες.

3. Στις περιπτώσεις κατά τις οποίες, σύμφωνα με τις εξαιρέσεις που καθορίζονται στο σημείο 3.2.2 του Παραρτήματος ΙΙ της συμφωνίας-πλαισίου και στο άρθρο 6 παράγραφος 5 της διοργανικής συμφωνίας, πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή σε ισοδύναμό του συζητούνται σε συνεδρίαση κεκλεισμένων των θυρών, η γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου που έχει αρμοδιότητα για τη συνεδρίαση διασφαλίζει, επιπλέον των διατάξεων που προβλέπονται στην παράγραφο 2, ότι τα πρόσωπα που ορίζονται να συμμετάσχουν στη συνεδρίαση συμμορφώνονται με τις απαιτήσεις του άρθρου 3 παράγραφοι 4 και 7.

4. Στην περίπτωση που προβλέπεται στην παράγραφο 3, η CIU παρέχει στη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου που έχει αρμοδιότητα για τη συνεδρίαση κεκλεισμένων των θυρών ο απαιτούμενος αριθμός αντιγράφων των εγγράφων που πρόκειται να συζητηθούν, τα οποία επιστρέφονται στην CIU μετά τη συνεδρίαση.

Άρθρο 12

Αρχειοθέτηση εμπιστευτικών πληροφοριών

1. Δυνατότητες ασφαλούς αρχειοθέτησης παρέχονται εντός του Ασφαλούς Χώρου. Η CIU είναι αρμόδια για τη διαχείριση του ασφαλούς αρχείου, σύμφωνα με καθιερωμένα κριτήρια αρχειοθέτησης.

2. Διαβαθμισμένες πληροφορίες που κατατίθενται οριστικά στην CIU και πληροφορίες που έχουν διαβαθμιστεί σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του που κατατίθενται στη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου μεταφέρονται στο ασφαλές αρχείο στον ασφαλή χώρο έξι μήνες μετά την τελευταία εξέτασή τους και, το αργότερο, ένα έτος μετά την κατάθεσή τους. Οι «άλλες εμπιστευτικές πληροφορίες» αρχειοθετούνται, εκτός εάν έχουν κατατεθεί στην CIU, από τη γραμματεία του οικείου κοινοβουλευτικού οργάνου/αξιωματούχου, σύμφωνα με τους γενικούς κανόνες διαχείρισης των εγγράφων.

3. Οι εμπιστευτικές πληροφορίες που τηρούνται στο ασφαλές αρχείο μπορούν να εξετασθούν σύμφωνα με τους ακόλουθους κανόνες:

α) μόνον τα πρόσωπα των οποίων η ταυτότητα προσδιορίζεται ονομαστικώς με τη θέση ή την ιδιότητά τους στο συνοδευτικό δελτίο που συμπληρώνεται κατά την κατάθεση της εμπιστευτικής πληροφορίας έχουν άδεια να εξετάσουν την πληροφορία αυτή·

β) η αίτηση εξέτασης εμπιστευτικών πληροφοριών υποβάλλεται στην CIU, η οποία διασφαλίζει τη μεταφορά του εν λόγω εγγράφου από το αρχείο στην ασφαλή αίθουσα ανάγνωσης· και

γ) εφαρμόζονται οι διαδικασίες και οι κανόνες που ισχύουν για την εξέταση των εμπιστευτικών πληροφοριών οι οποίοι καθορίζονται στο άρθρο 10.

Άρθρο 13

Υποχαρακτηρισμός, αποχαρακτηρισμός και αφαίρεση σήμανσης εμπιστευτικών πληροφοριών.

1. Οι εμπιστευτικές πληροφορίες μπορούν να υποχαρακτηρίζονται, να αποχαρακτηρίζονται ή να αφαιρείται η σήμανσή τους μόνο κατόπιν προηγούμενης συναίνεσης του αρχικού συντάκτη, και, εφόσον απαιτείται, αφού ζητηθεί η γνώμη των λοιπών ενδιαφερομένων.

2. Ο υποχαρακτηρισμός ή αποχαρακτηρισμός επιβεβαιώνεται γραπτώς. Ο αρχικός συντάκτης ενημερώνει τους παραλήπτες του εγγράφου για τη μεταβολή της διαβάθμισης, οι δε παραλήπτες ενημερώνουν τους διαδοχικούς παραλήπτες στους οποίους έχουν διαβιβάσει το πρωτότυπο ή αντίγραφο του εγγράφου για τη μεταβολή. Ει δυνατόν, οι αρχικοί συντάκτες αναγράφουν επί των διαβαθμισμένων εγγράφων την ημερομηνία, την προθεσμία ή το γεγονός μετά τα οποία τα περιεχόμενά τους μπορούν να υποχαρακτηρίζονται ή αποχαρακτηρίζονται. Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι η αρχική διαβάθμιση εξακολουθεί να είναι αναγκαία.

3. Οι εμπιστευτικές πληροφορίες που τηρούνται σε ασφαλή αρχεία εξετάζονται σε εύθετο χρόνο, και το αργότερο κατά το 25ο έτος από την ημερομηνία δημιουργίας τους, προκειμένου να καθορισθεί εάν θα αποχαρακτηριστούν, υποχαρακτηριστούν ή θα στερηθούν της σήμανσης. Η εξέταση και δημοσίευση των πληροφοριών αυτών λαμβάνει χώρα σύμφωνα με τις διατάξεις του κανονισμού (ΕΟΚ, Ευρατόμ) αριθ. 354/83 του Συμβουλίου της 1ης Φεβρουαρίου 1983 για το άνοιγμα στο κοινό των ιστορικών αρχείων της Ευρωπαϊκής Οικονομικής Κοινότητας και της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας ([1]). Ο αποχαρακτηρισμός πραγματοποιείται από τον αρχικό συντάκτη του διαβαθμισμένου εγγράφου ή από την αρμόδια υπηρεσία σύμφωνα με το Παράρτημα Ι Μέρος 1 Τμήμα 10.

4. Μετά τον αποχαρακτηρισμό, τα πρώην διαβαθμισμένα έγγραφα που τηρούνται στο ασφαλές αρχείο μεταφέρονται στα ιστορικά αρχεία του Ευρωπαϊκού Κοινοβουλίου για μόνιμη φύλαξη και περαιτέρω επεξεργασία σύμφωνα με τους ισχύοντες κανόνες.

5. Μετά την αφαίρεση της σήμανσης, τα πρώην «άλλα εμπιστευτικά έγγραφα» υπόκεινται στους κανόνες του Ευρωπαϊκού Κοινοβουλίου σχετικά με τη διαχείριση εγγράφων.

Άρθρο 14

Παραβίαση της ασφάλειας, απώλεια ή διαρροή εμπιστευτικών πληροφοριών

1. Η παραβίαση της εμπιστευτικότητας εν γένει και της παρούσας απόφασης ειδικότερα επιφέρει στην περίπτωση των βουλευτών του Ευρωπαϊκού Κοινοβουλίου την εφαρμογή των σχετικών περί κυρώσεων διατάξεων που θεσπίζονται στον Κανονισμό του Ευρωπαϊκού Κοινοβουλίου.

2. Η παραβίαση που διαπράττει μέλος του προσωπικού του Ευρωπαϊκού Κοινοβουλίου επιφέρει την εφαρμογή των διαδικασιών και των κυρώσεων που προβλέπονται, αντίστοιχα, στον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων και στο καθεστώς που εφαρμόζεται στο λοιπό προσωπικό της Ευρωπαϊκής Ένωσης, όπως ορίζονται στον κανονισμό (ΕΟΚ, Ευρατόμ, ΕΚΑΧ) αριθ. 259/68 ([2]) (ο «κανονισμός υπηρεσιακής κατάστασης»).

([1]) ΕΕ L 43, 15.2.1983, σ. 1.
([2]) ΕΕ L 56, 4.3.1968, σ. 1.

3. Ο Πρόεδρος και ο Γενικός Γραμματέας, κατά περίπτωση, οργανώνουν τυχόν απαραίτητες έρευνες σε περίπτωση παραβίασης όπως ορίζεται στην κοινοποίηση ασφάλειας 6.

4. Εάν η εμπιστευτική πληροφορία γνωστοποιήθηκε στο Ευρωπαϊκό Κοινοβούλιο από θεσμικό όργανο της Ένωσης ή από κράτος μέλος, ο Πρόεδρος και/ή ο Γενικός Γραμματέας, κατά περίπτωση, ενημερώνουν το ενεχόμενο θεσμικό όργανο της Ένωσης ή το κράτος μέλος σχετικά με κάθε αποδεδειγμένη ή εικαζόμενη απώλεια ή διαρροή διαβαθμισμένων πληροφοριών, τα αποτελέσματα της έρευνας και τα μέτρα που ελήφθησαν για την αποφυγή επανάληψης των ιδίων περιστατικών.

Άρθρο 15

Προσαρμογή της παρούσας απόφασης και των κανόνων εφαρμογής και υποβολή ετήσιας έκθεσης σχετικά με την εφαρμογή της παρούσας απόφασης

1. Ο Γενικός Γραμματέας προτείνει κάθε απαραίτητη προσαρμογή της παρούσας απόφασης και των παραρτημάτων εφαρμογής της και διαβιβάζει τις προτάσεις αυτές στο Προεδρείο με σκοπό τη λήψη απόφασης.

2. Ο Γενικός Γραμματέας είναι υπεύθυνος για την εφαρμογή της παρούσας απόφασης από τις υπηρεσίες του Ευρωπαϊκού Κοινοβουλίου και εκδίδει τις οδηγίες χειρισμού για θέματα που καλύπτονται από το ΣΔΑΠ σύμφωνα με τις αρχές που καθορίζονται στην παρούσα απόφαση.

3. Ο Γενικός Γραμματέας υποβάλλει ετήσια έκθεση στο Προεδρείο σχετικά με την εφαρμογή της παρούσας απόφασης.

Άρθρο 16

Τελικές και μεταβατικές διατάξεις

1. Οι μη διαβαθμισμένες πληροφορίες που υπάρχουν στην CIU ή σε οποιοδήποτε άλλο αρχείο του Ευρωπαϊκού Κοινοβουλίου που θεωρείται εμπιστευτικό και χρονολογείται πριν από τις 1 Απριλίου 2014 θεωρούνται, για τους σκοπούς της παρούσας απόφασης, «άλλες εμπιστευτικές πληροφορίες». Ο αρχικός συντάκτης τους μπορεί οποτεδήποτε να επαναπροσδιορίσει το επίπεδο εμπιστευτικότητας.

2. Κατά παρέκκλιση από το στοιχείο α) του άρθρου 5 παράγραφος 1 και από το άρθρο 8 παράγραφος 1 της παρούσας απόφασης, για περίοδο δώδεκα μηνών από τις 1 Απριλίου 2014, οι πληροφορίες που παρέχονται από το Συμβούλιο δυνάμει της διοργανικής συμφωνίας και διαβαθμίζονται σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του κατατίθενται, καταχωρίζονται και αποθηκεύονται στην CIU. Οι εν λόγω πληροφορίες μπορούν να εξετάζονται σύμφωνα με το άρθρο 4 παράγραφος 2 στοιχεία α) και γ) και το άρθρο 5 παράγραφος 4 της διοργανικής συμφωνίας.

3. Η απόφαση του Προεδρείου της 6ης Ιουνίου 2011 σχετικά με τους κανόνες που διέπουν την επεξεργασία των εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο καταργείται.

Άρθρο 17

Έναρξη ισχύος

Η παρούσα απόφαση τίθεται σε ισχύ την ημέρα δημοσίευσής της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

ΠΑΡΑΡΤΗΜΑ I

Μέρος 1ο

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΕΛΑΧΙΣΤΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

1. **ΕΙΣΑΓΩΓΗ**

Οι παρούσες διατάξεις θεσπίζουν τις βασικές αρχές και τα ελάχιστα πρότυπα ασφάλειας για την προστασία των εμπιστευτικών πληροφοριών που πρέπει να σέβεται ή/και να τηρεί το Ευρωπαϊκό Κοινοβούλιο, σε όλους τους τόπους δραστηριοτήτων του, καθώς και όλοι οι αποδέκτες διαβαθμισμένων πληροφοριών και «άλλων εμπιστευτικών πληροφοριών» έτσι ώστε να περιφρουρείται η ασφάλεια και όλα τα εμπλεκόμενα πρόσωπα να βεβαιούνται ότι έχουν θεσπισθεί κοινά πρότυπα προστασίας. Οι διατάξεις αυτές συμπληρώνονται από τις κοινοποιήσεις ασφάλειας που περιέχονται στο Παράρτημα II και από άλλες διατάξεις που διέπουν την επεξεργασία εμπιστευτικών πληροφοριών από κοινοβουλευτικές επιτροπές και άλλα όργανα/αξιωματούχους του Κοινοβουλίου.

2. **ΒΑΣΙΚΕΣ ΑΡΧΕΣ**

Η πολιτική του Ευρωπαϊκού Κοινοβουλίου για την ασφάλεια αποτελεί αναπόσπαστο τμήμα της γενικής πολιτικής του για την εσωτερική διαχείριση και, κατά συνέπεια, βασίζεται στις αρχές που διέπουν τη γενική πολιτική αυτή. Οι εν λόγω αρχές περιλαμβάνουν τη νομιμότητα, τη διαφάνεια, τη λογοδοσία, την επικουρικότητα και την αναλογικότητα.

Η νομιμότητα συνεπάγεται την ανάγκη της παραμονής αυστηρά εντός του νομικού πλαισίου κατά την άσκηση των λειτουργιών ασφάλειας, καθώς και της τήρησης των εφαρμοστέων νομικών απαιτήσεων. Επίσης, οι αρμοδιότητες στον τομέα της ασφάλειας πρέπει να βασίζονται στις κατάλληλες νομικές διατάξεις. Οι διατάξεις του κανονισμού υπηρεσιακής κατάστασης, ιδίως το άρθρο 17, σχετικά με την υποχρέωση του προσωπικού να απέχει από την χωρίς άδεια κοινολόγηση των πληροφοριών που περιέρχονται στην αντίληψή του εξαιτίας των καθηκόντων του, καθώς και ο τίτλος VI σχετικά με τα πειθαρχικά μέτρα, εφαρμόζονται πλήρως. Τέλος, οι παραβιάσεις της ασφάλειας εντός της αρμοδιότητας του Ευρωπαϊκού Κοινοβουλίου αντιμετωπίζονται κατά τρόπο συνεπή με τον Κανονισμό του και την πολιτική του σχετικά με τη λήψη πειθαρχικών μέτρων.

Η διαφάνεια συνεπάγεται την ανάγκη για σαφήνεια όσον αφορά όλους τους κανόνες και τις διατάξεις ασφάλειας, για να επιτευχθεί εξισορρόπηση μεταξύ των διαφόρων υπηρεσιών και των διαφόρων τομέων (φυσική ασφάλεια σε σύγκριση με την προστασία των πληροφοριών, κλπ) και την ανάγκη για μια συνεκτική και διαρθρωμένη πολιτική ευαισθητοποίησης σχετικά με την ασφάλεια. Επιπλέον, είναι αναγκαίες σαφείς γραπτές γενικές κατευθύνσεις για την εφαρμογή μέτρων ασφάλειας.

Η λογοδοσία σημαίνει ότι πρέπει να καθορίζονται σαφώς οι αρμοδιότητες στον τομέα της ασφάλειας. Επιπλέον, συνεπάγεται την ανάγκη να ελέγχεται τακτικά εάν οι εν λόγω αρμοδιότητες έχουν εκτελεσθεί ορθά.

Η επικουρικότητα σημαίνει ότι η ασφάλεια πρέπει να οργανώνεται στο χαμηλότερο δυνατό επίπεδο και όσο το δυνατόν στενότερα σε συνεργασία με τις Γενικές Διευθύνσεις και τις υπηρεσίες του Ευρωπαϊκού Κοινοβουλίου.

Η αναλογικότητα σημαίνει ότι οι δραστηριότητες ασφάλειας πρέπει να περιορίζονται αυστηρά στο απολύτως αναγκαίο και ότι τα μέτρα ασφάλειας πρέπει να είναι ανάλογα των συμφερόντων που πρέπει να προστατευθούν και της πραγματικής ή δυνητικής απειλής για τα εν λόγω συμφέροντα, ούτως ώστε να είναι δυνατή η προστασία των συμφερόντων αυτών με τρόπο που διασφαλίζει τις ελάχιστες δυνατές διαταραχές.

3. **ΘΕΜΕΛΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

Η ορθή διαχείριση της ασφάλειας των πληροφοριών θεμελιώνεται στα εξής στοιχεία:

α) σε κατάλληλα συστήματα επικοινωνίας και πληροφοριών (ΣΕΠ). Τα εν λόγω συστήματα είναι υπό την ευθύνη της αρχής ασφάλειας του Ευρωπαϊκού Κοινοβουλίου (όπως ορίζεται στην κοινοποίηση ασφαλείας 1)·

β) εντός του Ευρωπαϊκού Κοινοβουλίου, στην αρχή ασφάλειας των πληροφοριών (όπως ορίζεται στην κοινοποίηση ασφάλειας 1), υπεύθυνη για τη συνεργασία με την οικεία αρχή ασφάλειας προκειμένου να παρέχει πληροφορίες και συμβουλές σχετικά με τις απειλές τεχνικής φύσεως στα ΣΕΠ και τα μέσα για την προστασία από τις απειλές αυτές·

γ) στη στενή συνεργασία μεταξύ των αρμοδίων υπηρεσιών του Ευρωπαϊκού Κοινοβουλίου και των υπηρεσιών ασφάλειας των άλλων οργάνων της Ένωσης.

4. **ΑΡΧΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

4.1. ***Στόχοι***

Οι κύριοι στόχοι της ασφάλειας των πληροφοριών είναι οι εξής:

α) η προστασία των εμπιστευτικών πληροφοριών από κατασκοπεία, διαρροή ή κοινοποίηση άνευ αδείας·

β) η προστασία των διαβαθμισμένων πληροφοριών που διακινούνται στα συστήματα και στα δίκτυα επικοινωνιών και πληροφορικής από κάθε απειλή για την εμπιστευτικότητα, την αξιοπιστία και τη διαθεσιμότητά τους·

γ) η προστασία των εγκαταστάσεων του Ευρωπαϊκού Κοινοβουλίου στις οποίες αποθηκεύονται διαβαθμισμένες πληροφορίες από το ενδεχόμενο δολιοφθοράς και κακόβουλης εκ προθέσεως φθοράς·

δ) σε περίπτωση αποτυχίας της ασφάλειας, η εκτίμηση της ζημίας, ο περιορισμός των συνεπειών της, η διενέργεια ερευνών ασφάλειας και η λήψη των τυχόν αναγκαίων επανορθωτικών μέτρων.

4.2. ***Διαβάθμιση***

4.2.1. Όσον αφορά την εμπιστευτικότητα, απαιτείται μέριμνα και πείρα κατά την επιλογή των πληροφοριών και του υλικού που πρέπει να προστατεύονται καθώς και κατά την εκτίμηση του αναγκαίου βαθμού προστασίας. Είναι θεμελιώδες ο βαθμός προστασίας να ανταποκρίνεται στο βαθμό ευαισθησίας, ως προς την ασφάλεια, των συγκεκριμένων προστατευτέων πληροφοριακών στοιχείων ή υλικών. Για να διασφαλιστεί η ομαλή ροή των πληροφοριών, τόσο η υπερβολική όσο και η ανεπαρκής διαβάθμιση αποφεύγονται.

4.2.2. Το σύστημα διαβάθμισης αποτελεί το μέσο για την υλοποίηση των αρχών που ορίζονται στο τμήμα αυτό. Παρόμοιο σύστημα διαβάθμισης εφαρμόζεται και κατά τον προγραμματισμό και την οργάνωση τρόπων αντιμετώπισης της κατασκοπείας, των δολιοφθορών, της τρομοκρατίας και άλλων απειλών, προκειμένου να διασφαλίζεται ο μέγιστος βαθμός προστασίας στους κυριότερους χώρους εντός των οποίων αποθηκεύονται διαβαθμισμένες πληροφορίες καθώς και στα πλέον ευαίσθητα σημεία των χώρων αυτών.

4.2.3. Την ευθύνη για τη διαβάθμιση των πληροφοριών έχει αποκλειστικά ο αρχικός συντάκτης των εν λόγω πληροφοριών.

4.2.4. Το επίπεδο διαβάθμισης μπορεί να βασίζεται αποκλειστικά στο περιεχόμενο των σχετικών πληροφοριών.

4.2.5. Σε περίπτωση πλειόνων πληροφοριακών στοιχείων που αποτελούν μια ενότητα, η διαβάθμισή τους είναι τουλάχιστον ίση με το υψηλότερο επίπεδο διαβάθμισης που παρέχεται σε ένα από τα επιμέρους στοιχεία της ενότητας. Ωστόσο, μια συλλογή πληροφοριών δύναται να έχει υψηλότερη διαβάθμιση σε σχέση με τα επιμέρους στοιχεία της.

4.2.6. Οι διαβαθμίσεις καθορίζονται μόνον εφόσον είναι απαραίτητο και για τον απαιτούμενο χρόνο.

4.3. ***Στόχοι των μέτρων ασφάλειας***

Τα μέτρα ασφάλειας:

α) καλύπτουν όλα τα πρόσωπα που έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες, τα μέσα που φέρουν διαβαθμισμένες πληροφορίες και «άλλες εμπιστευτικές πληροφορίες», καθώς και όλους τους χώρους όπου υπάρχουν τέτοιες πληροφορίες και τις σημαντικές εγκαταστάσεις·

β) σχεδιάζονται κατά τρόπο που να επισημαίνονται τα πρόσωπα των οποίων η θέση (από την άποψη της πρόσβασης, των σχέσεων και άλλων στοιχείων) ενδέχεται να διακινδυνεύσει την ασφάλεια των πληροφοριών αυτών και των σημαντικών εγκαταστάσεων στις οποίες αποθηκεύονται και να παρέχεται η δυνατότητα αποκλεισμού ή απομάκρυνσής τους·

γ) εμποδίζουν κάθε μη εξουσιοδοτημένο πρόσωπο να έχει πρόσβαση στις πληροφορίες αυτές ή στις εγκαταστάσεις όπου αποθηκεύονται·

δ) εξασφαλίζουν ότι οι πληροφορίες αυτές διανέμονται μόνο με βάση την αρχή της «ανάγκης γνώσης», αρχή θεμελιώδους σημασίας για όλες τις πτυχές της ασφάλειας·

ε) εξασφαλίζουν την αξιοπιστία (εμποδίζοντας την αλλοίωση, την άνευ αδείας τροποποίηση ή διαγραφή στοιχείων) και τη διαθεσιμότητα (στα πρόσωπα που απαιτείται να έχουν γνώση αυτών και διαθέτουν σχετική άδεια) των εμπιστευτικών πληροφοριών και όταν αποτελούν αντικείμενο αποθήκευσης, επεξεργασίας ή διαβίβασης με ηλεκτρομαγνητικά μέσα.

5. **ΚΟΙΝΑ ΕΛΑΧΙΣΤΑ ΠΡΟΤΥΠΑ**

Το Ευρωπαϊκό Κοινοβούλιο διασφαλίζει την τήρηση των κοινών ελάχιστων προτύπων ασφάλειας από όλους τους αποδέκτες των διαβαθμισμένων πληροφοριών, τόσο μέσα στο θεσμικό όργανο όσο και στο πλαίσιο της ευθύνης του, συγκεκριμένα από όλες τις υπηρεσίες και τους συμβαλλόμενους, έτσι ώστε να είναι δυνατόν οι πληροφορίες αυτές να διαβιβάζονται με τη βεβαιότητα ότι θα αντιμετωπιστούν με την αντίστοιχη προσοχή. Τα εν λόγω ελάχιστα πρότυπα περιλαμβάνουν κριτήρια για τον έλεγχο των υπαλλήλων του Ευρωπαϊκού Κοινοβουλίου και του λοιπού προσωπικού του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, και διαδικασίες για την προστασία των εμπιστευτικών πληροφοριών.

Το Ευρωπαϊκό Κοινοβούλιο επιτρέπει σε τρίτους την πρόσβαση στις πληροφορίες αυτές μόνο όταν οι εν λόγω τρίτοι διασφαλίζουν ότι κατά τον χειρισμό των πληροφοριών αυτών τηρούνται διατάξεις που είναι τουλάχιστον αυστηρά ισοδύναμες με αυτά τα κοινά ελάχιστα πρότυπα.

Τα εν λόγω κοινά ελάχιστα πρότυπα εφαρμόζονται επίσης όταν το Ευρωπαϊκό Κοινοβούλιο, με βάση σύμβαση ή συμφωνία επιχορήγησης, μεταβιβάζει σε βιομηχανικές επιχειρήσεις ή άλλους φορείς καθήκοντα που αφορούν εμπιστευτικές πληροφορίες.

6. **ΑΣΦΑΛΕΙΑ ΟΣΟΝ ΑΦΟΡΑ ΤΟΥΣ ΥΠΑΛΛΗΛΟΥΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟ ΛΟΙΠΟ ΠΡΟΣΩΠΙΚΟ ΤΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΠΟΥ ΕΡΓΑΖΕΤΑΙ ΓΙΑ ΤΙΣ ΠΟΛΙΤΙΚΕΣ ΟΜΑΔΕΣ**

6.1. ***Κοινοποιήσεις ασφάλειας όσον αφορά τους υπαλλήλους του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες***

Οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες που απασχολούνται σε θέσεις που επιτρέπουν την πρόσβαση σε διαβαθμισμένες πληροφορίες λαμβάνουν λεπτομερείς οδηγίες τόσο κατά την ανάληψη των καθηκόντων τους όσο και σε τακτικά διαστήματα στη συνέχεια για την ανάγκη ασφάλειας καθώς και για τις σχετικές διαδικασίες. Τα πρόσωπα αυτά καλούνται να επιβεβαιώσουν εγγράφως ότι έχουν διαβάσει και κατανοήσει πλήρως τις εφαρμοστέες διατάξεις ασφάλειας.

6.2. ***Ευθύνες της διεύθυνσης***

Μέρος των καθηκόντων των διευθυντικών στελεχών πρέπει να είναι το να γνωρίζουν ποιοι από το προσωπικό τους εργάζονται σε επαφή με διαβαθμισμένες πληροφορίες ή έχουν πρόσβαση σε ασφαλή συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών, καθώς και να καταγράφουν και να αναφέρουν όλα τα περιστατικά ή τα εμφανή τρωτά σημεία τα οποία ενδέχεται να έχουν επιπτώσεις στην ασφάλεια.

6.3. ***Καθεστώς ασφάλειας για τους υπαλλήλους του Ευρωπαϊκού Κοινοβουλίου και του λοιπού προσωπικού του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες***

Θεσμοθετούνται διαδικασίες που εξασφαλίζουν ότι, όταν υπάρχουν αρνητικές πληροφορίες για κάποιον υπάλληλο του Ευρωπαϊκού Κοινοβουλίου ή λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, πραγματοποιούνται ενέργειες για να εξετασθεί εάν το πρόσωπο αυτό εργάζεται σε επαφή με διαβαθμισμένες πληροφορίες ή έχει πρόσβαση σε ασφαλή συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών και ενημερώνεται η αρμόδια υπηρεσία του Ευρωπαϊκού Κοινοβουλίου. Εάν η αρμόδια εθνική αρχή ασφάλειας αναφέρει ότι το πρόσωπο αυτό αποτελεί κίνδυνο για την ασφάλεια, τότε του απαγορεύεται η πρόσβαση ή απομακρύνεται από θέσεις στις οποίες θα μπορούσε να δημιουργήσει κίνδυνο για την ασφάλεια.

7. **ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ**

Ως «φυσική ασφάλεια» νοείται η εφαρμογή φυσικών και τεχνικών προστατευτικών μέτρων που παρεμποδίζουν την μη εξουσιοδοτημένη πρόσβαση σε διαβαθμισμένες πληροφορίες.

7.1. ***Ανάγκη προστασίας***

Η αυστηρότητα των μέτρων φυσικής ασφάλειας που εφαρμόζονται για την προστασία των διαβαθμισμένων πληροφοριών είναι ανάλογη με τη διαβάθμιση και τον όγκο των πληροφοριών και του υλικού και την υφισταμένη απειλή. Όλοι οι κάτοχοι διαβαθμισμένων πληροφοριών ακολουθούν ομοιόμορφες διαδικασίες όσον αφορά τη διαβάθμιση των πληροφοριών αυτών και οφείλουν να εφαρμόζουν κοινές προδιαγραφές ασφάλειας σχετικά με τη φύλαξη, τη διαβίβαση και τη διάθεση πληροφοριών και υλικού που απαιτούν προστασία.

7.2. ***Έλεγχος***

Προτού εγκαταλείψουν αφύλακτους τους χώρους όπου αποθηκεύονται διαβαθμισμένες πληροφορίες, τα πρόσωπα που είναι επιφορτισμένα με τη φύλαξή τους βεβαιώνονται ότι αυτές είναι ασφαλώς αποθηκευμένες και ότι έχουν ενεργοποιηθεί όλοι οι μηχανισμοί ασφάλειας (κλειδαριές, συναγερμοί, κ.λπ.). Διεξάγονται περαιτέρω ανεξάρτητοι έλεγχοι μετά το πέρας των ωρών εργασίας.

7.3. ***Ασφάλεια των κτιρίων***

Τα κτίρια όπου στεγάζονται διαβαθμισμένες πληροφορίες ή ασφαλή συστήματα επικοινωνιών και πληροφοριών προστατεύονται από το ενδεχόμενο εισόδου μη εξουσιοδοτημένων προσώπων.

Η φύση της προστασίας των διαβαθμισμένων πληροφοριών, π.χ. κάγκελα στα παράθυρα, κλειδαριές στις πόρτες, φύλακες στις εισόδους, αυτόματα συστήματα ελέγχου των εισερχομένων, έλεγχοι ασφάλειας και περίπολοι, συστήματα συναγερμού, συστήματα ανίχνευσης εισβολών και σκύλοι-φύλακες, εξαρτάται από:

α) τη διαβάθμιση, τον όγκο και τη θέση εντός του κτιρίου των προστατευτέων πληροφοριών και υλικού·

β) την ποιότητα των φωριαμών ασφάλειας όπου φυλάσσονται αυτές οι πληροφορίες και το υλικό· και

γ) τη φύση της κατασκευής και τη θέση του κτιρίου.

Η φύση της προστασίας των συστημάτων επικοινωνιών και πληροφοριών εξαρτάται και αυτή από την εκτίμηση της αξίας των συγκεκριμένων περιουσιακών στοιχείων, από το μέγεθος της ενδεχόμενης ζημίας σε περίπτωση παραβίασης της ασφάλειας, από τη φύση της κατασκευής και τη θέση του κτιρίου στο οποίο στεγάζεται το σύστημα και από τη θέση του συστήματος αυτού εντός του κτιρίου.

7.4. ***Σχέδια έκτακτης ανάγκης***

Υπάρχουν εκ των προτέρων αναλυτικά σχέδια για τη διασφάλιση της προστασίας των διαβαθμισμένων πληροφοριών για τις περιπτώσεις έκτακτης ανάγκης.

8. **ΕΝΔΕΙΞΕΙΣ ΑΣΦΑΛΕΙΑΣ, ΣΗΜΑΝΣΕΙΣ, ΘΕΣΕΙΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΔΙΑΒΑΘΜΙΣΗΣ**

8.1. ***Ενδείξεις ασφάλειας***

Δεν επιτρέπονται άλλες διαβαθμίσεις εκτός από εκείνες που ορίζονται στο άρθρο 2 στοιχείο δ) της παρούσας απόφασης.

Μπορεί να χρησιμοποιείται μια συμφωνημένη ένδειξη ασφάλειας για τον περιορισμό της ισχύος της διαβάθμισης (που σημαίνει για τις διαβαθμισμένες πληροφορίες αυτόματο υποχαρακτηρισμό ή αποχαρακτηρισμό).

Οι ενδείξεις ασφάλειας χρησιμοποιούνται μόνο σε συνδυασμό με μια διαβάθμιση.

Οι ενδείξεις ασφάλειας ρυθμίζονται περαιτέρω στην κοινοποίηση ασφάλειας 2 και καθορίζονται στις οδηγίες χειρισμού.

8.2. ***Σημάνσεις***

Μία σήμανση χρησιμοποιείται προκειμένου να προσδιοριστούν προκαθορισμένες ειδικές οδηγίες σχετικά με τον χειρισμό των εμπιστευτικών πληροφοριών. Οι σημάνσεις μπορεί επίσης να υποδεικνύουν τον τομέα που καλύπτεται από ένα συγκεκριμένο έγγραφο, ορισμένη διανομή του με βάση την ανάγκη γνώσης ή (για τις μη διαβαθμισμένες πληροφορίες) για να δηλώνεται η λήξη της απαγόρευσης κυκλοφορίας.

Μια σήμανση δεν αποτελεί διαβάθμιση και δεν χρησιμοποιείται στη θέση αυτής.

Οι σημάνσεις ρυθμίζονται περαιτέρω στην κοινοποίηση ασφάλειας 2 και καθορίζονται στις οδηγίες χειρισμού.

8.3. ***Θέση της διαβάθμισης και των ενδείξεων ασφαλείας***

Η θέση διαβαθμίσεων και ενδείξεων ασφαλείας και σημάνσεων πραγματοποιείται σύμφωνα με την κοινοποίηση ασφάλειας 2, τμήμα Ε, και τις οδηγίες χειρισμού.

8.4. ***Διαχείριση της διαβάθμισης***

8.4.1 *Γενικά*

Οι πληροφορίες διαβαθμίζονται μόνον εφόσον αυτό είναι απαραίτητο. Η διαβάθμιση επισημαίνεται σαφώς και καταλλήλως και διατηρείται μόνο για όσο χρονικό διάστημα οι συγκεκριμένες πληροφορίες απαιτείται να προστατευθούν.

Αποκλειστικός υπεύθυνος για τη διαβάθμιση των πληροφοριών και για τον τυχόν μεταγενέστερο υποχαρακτηρισμό ή αποχαρακτηρισμό τους είναι ο αρχικός συντάκτης του εγγράφου.

Οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου διαβαθμίζουν, υποχαρακτηρίζουν ή αποχαρακτηρίζουν πληροφορίες κατόπιν εντολής του Γενικού Γραμματέα ή κατόπιν εξουσιοδοτήσεως από αυτόν.

Οι αναλυτικές ρυθμίσεις για τον χειρισμό των διαβαθμισμένων εγγράφων εκπονούνται κατά τρόπο που να εξασφαλίζει ότι τυγχάνουν προστασίας ανάλογα με τις πληροφορίες που περιέχουν.

Ο αριθμός των προσώπων που επιτρέπεται να παράγουν πληροφορίες που διαβαθμίζονται σε επίπεδο TRÈS SECRET UE/EU TOP SECRET περιορίζεται στο ελάχιστο, τα δε ονόματά τους καταγράφονται σε κατάλογο που καταρτίζεται από την CIU.

8.4.2 *Εφαρμογή των διαβαθμίσεων*

Η διαβάθμιση ενός εγγράφου καθορίζεται από το επίπεδο ευαισθησίας του περιεχομένου του σύμφωνα με όσα ορίζονται στο άρθρο 2 στοιχείο δ). Είναι σημαντικό η διαβάθμιση να καθορίζεται σωστά και να χρησιμοποιείται με φειδώ.

Η διαβάθμιση μιας επιστολής ή ενός σημειώματος που περιλαμβάνει επισυναπτόμενα έγγραφα καθορίζεται τουλάχιστον στο επίπεδο της υψηλότερης διαβάθμισης που εφαρμόζεται σε ένα από τα επισυναπτόμενα έγγραφα. Ο αρχικός συντάκτης επισημαίνει σαφώς σε ποιο επίπεδο θα πρέπει να διαβαθμιστεί η επιστολή ή το σημείωμα όταν αποχωριστεί από τα επισυναπτόμενα έγγραφα.

Ο αρχικός συντάκτης ενός εγγράφου το οποίο πρόκειται να λάβει διαβάθμιση οφείλει να ακολουθεί τους προαναφερόμενους κανόνες και να αποφεύγει την τάση προς υπερβολικά υψηλή ή χαμηλή διαβάθμιση.

Επί μέρους σελίδες, παράγραφοι, τμήματα, παραρτήματα και προσαρτήματα ενός εγγράφου καθώς και τα επισυναπτόμενα και εσωκλειόμενα σε αυτό έγγραφα ενδέχεται να απαιτούν διαφορετικές διαβαθμίσεις και διαβαθμίζονται αναλόγως. Η διαβάθμιση του όλου εγγράφου αντιστοιχεί σε εκείνη του τμήματός του με την υψηλότερη διαβάθμιση.

9. **ΕΠΙΘΕΩΡΗΣΕΙΣ**

Η Διεύθυνση Ασφάλειας και Αξιολόγησης Κινδύνου του Ευρωπαϊκού Κοινοβουλίου, η οποία μπορεί να ζητεί τη συνδρομή των αρχών ασφάλειας του Συμβουλίου ή της Επιτροπής, διενεργεί περιοδικές εσωτερικές επιθεωρήσεις των ρυθμίσεων ασφάλειας για την προστασία των διαβαθμισμένων πληροφοριών.

Οι αρχές ασφάλειας και οι αρμόδιες υπηρεσίες των θεσμικών οργάνων της Ένωσης μπορούν να διεξάγουν, στο πλαίσιο συμφωνηθείσας διαδικασίας που κινείται από οιαδήποτε από τις πλευρές αυτές, αξιολογήσεις από ομότιμους, των ρυθμίσεων ασφάλειας για την προστασία των διαβαθμισμένων πληροφοριών που ανταλλάσσονται στο πλαίσιο των σχετικών διοργανικών συμφωνιών.

10. **ΔΙΑΔΙΚΑΣΙΕΣ ΑΠΟΧΑΡΑΚΤΗΡΙΣΜΟΥ ΚΑΙ ΑΦΑΙΡΕΣΗΣ ΣΗΜΑΝΣΗΣ**

10.1. Η CIU εξετάζει τις εμπιστευτικές πληροφορίες που περιέχονται στο μητρώο της και ζητεί τη συγκατάθεση του αρχικού συντάκτη για τον αποχαρακτηρισμό ή την αφαίρεση της σήμανσης ενός εγγράφου σε κάθε περίπτωση το αργότερο το 25ο έτος από τη σύνταξή του. Τα έγγραφα που δεν έχουν αποχαρακτηρισθεί ή στερηθεί της σήμανσης κατά την πρώτη εξέταση επανεξετάζονται περιοδικά και τουλάχιστον ανά πενταετία. Επιπλέον της εφαρμογής της σε έγγραφα που τηρούνται στα ασφαλή αρχεία στον ασφαλή χώρο και έχουν δεόντως διαβαθμισθεί, η διαδικασία αφαίρεσης της σήμανσης μπορεί επίσης να καλύπτει και άλλες εμπιστευτικές πληροφορίες που υπάρχουν είτε σε κοινοβουλευτικό όργανο/αξιωματούχο είτε στην υπηρεσία που είναι αρμόδια για τα ιστορικά αρχεία του Κοινοβουλίου.

10.2 Η απόφαση σχετικά με τον αποχαρακτηρισμό ή την αφαίρεση της σήμανσης εγγράφου κατά γενικό κανόνα λαμβάνεται αποκλειστικά από τον αρχικό συντάκτη ή, κατ' εξαίρεση, σε συνεργασία με το κοινοβουλευτικό όργανο/αξιωματούχο που κατέχει τις πληροφορίες αυτές, προτού οι περιεχόμενες στο έγγραφο πληροφορίες μεταφερθούν στην υπηρεσία που είναι αρμόδια για τα ιστορικά αρχεία του Κοινοβουλίου. Για τον αποχαρακτηρισμό ή την αφαίρεση της σήμανσης διαβαθμισμένων πληροφοριών απαιτείται η προηγούμενη γραπτή συγκατάθεση του αρχικού συντάκτη. Στην περίπτωση «άλλων εμπιστευτικών πληροφοριών», η γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου που κατέχει τις πληροφορίες αυτές αποφασίζει, σε συνεργασία με τον αρχικό συντάκτη, εάν θα αφαιρεθεί η σήμανση από το έγγραφο.

10.3. Η CIU είναι αρμόδια να ενημερώσει για λογαριασμό του αρχικού συντάκτη τους παραλήπτες του εγγράφου για τη μεταβολή στη διαβάθμιση ή σήμανση, οι δε παραλήπτες είναι με τη σειρά τους αρμόδιοι να ενημερώσουν τους διαδοχικούς παραλήπτες στους οποίους έχουν διαβιβάσει το πρωτότυπο ή αντίγραφο του εγγράφου.

10.4. Ο αποχαρακτηρισμός δεν επηρεάζει τυχόν ενδείξεις ασφάλειας ή σημάνσεις που μπορεί να φέρει το έγγραφο.

10.5. Σε περίπτωση αποχαρακτηρισμού, η αρχική διαβάθμιση στο άνω και στο κάτω μέρος κάθε σελίδας διαγράφεται. Η πρώτη σελίδα του εγγράφου σφραγίζεται και συμπληρώνεται με κωδικό της CIU. Σε περίπτωση αφαίρεσης σήμανσης, η αρχική σήμανση στο άνω μέρος κάθε σελίδας διαγράφεται.

10.6. Το κείμενο του αποχαρακτηρισμένου εγγράφου ή του εγγράφου από το οποίο αφαιρέθηκε η σήμανση επισυνάπτεται στο ηλεκτρονικό φύλλο ή στο ισοδύναμο σύστημα στο οποίο έχει καταχωρηθεί.

10.7. Σε περίπτωση εγγράφων που καλύπτονται από την εξαίρεση που αφορά την ιδιωτικότητα και την ακεραιότητα του ατόμου ή τα επαγγελματικά συμφέροντα ενός φυσικού ή νομικού προσώπου και στην περίπτωση ευαίσθητων εγγράφων, εφαρμόζονται οι διατάξεις του άρθρου 2, του κανονισμού (ΕΟΚ, Ευρατόμ) αριθ. 354/83 του Συμβουλίου.

10.8. Επιπλέον των διατάξεων των σημείων 10.1 έως 10.7, εφαρμόζονται οι ακόλουθοι κανόνες:

α) όσον αφορά έγγραφα τρίτων, η CIU συνεννοείται με τον ενδιαφερόμενο τρίτο πριν προβεί στη διαδικασία αποχαρακτηρισμού ή αφαίρεσης σήμανσης.

β) όσον αφορά την εξαίρεση σχετικά με την ιδιωτικότητα και την ακεραιότητα του ατόμου, η διαδικασία αποχαρακτηρισμού αφαίρεσης σήμανσης λαμβάνει ιδίως υπόψη τη συμφωνία του ενδιαφερομένου προσώπου ή, κατά περίπτωση, την αδυναμία ταυτοποίησης του ενδιαφερομένου προσώπου·

γ) όσον αφορά την εξαίρεση σχετικά με τα επαγγελματικά συμφέροντα ενός φυσικού ή νομικού προσώπου, το ενδιαφερόμενο πρόσωπο μπορεί να ενημερωθεί μέσω δημοσίευσης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* μαζί με μία προθεσμία τεσσάρων εβδομάδων από την ημέρα της δημοσίευσης αυτής κατά τη διάρκεια των οποίων υποβάλλει παρατηρήσεις.

Μέρος 2ο

ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ

11. **ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟΥΣ ΒΟΥΛΕΥΤΕΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ**

11.1. Για να έχουν πρόσβαση σε πληροφορίες με τη διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή σε ισοδύναμό του, οι βουλευτές του Ευρωπαϊκού Κοινοβουλίου έχουν λάβει σχετική άδεια είτε σύμφωνα με τη διαδικασία που αναφέρεται στα σημεία 11.3 και 11.4 του παρόντος Παραρτήματος είτε βάσει επίσημης δήλωσης μη κοινολόγησης σύμφωνα με το άρθρο 3 παράγραφος 4 της παρούσας απόφασης.

11.2 Για να έχουν πρόσβαση σε πληροφορίες με τη διαβάθμιση σε επίπεδο SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του, οι βουλευτές του Ευρωπαϊκού Κοινοβουλίου, έχουν λάβει σχετική άδεια σύμφωνα με τη διαδικασία των σημείων 11.3 και 11.14.

11.3. Η άδεια χορηγείται μόνο σε βουλευτές του Ευρωπαϊκού Κοινοβουλίου, οι οποίοι έχουν υποβληθεί σε έλεγχο ασφάλειας από τις αρμόδιες εθνικές αρχές των κρατών μελών, σύμφωνα με τη διαδικασία των σημείων 11.9 έως 11.14. Ο Πρόεδρος είναι αρμόδιος για τη χορήγηση της άδειας στους βουλευτές.

11.4 Ο Πρόεδρος μπορεί να χορηγήσει γραπτή άδεια αφού λάβει τη γνώμη των αρμόδιων εθνικών αρχών των κρατών μελών, βάσει του ελέγχου ασφάλειας που διενεργείται σύμφωνα με τα σημεία 11.8 έως 11.13.

11.5. Η Διεύθυνση Ασφάλειας και Αξιολόγησης Κινδύνου του Ευρωπαϊκού Κοινοβουλίου τηρεί ένα επικαιροποιημένο κατάλογο όλων των βουλευτών του Ευρωπαϊκού Κοινοβουλίου στους οποίους έχει χορηγηθεί άδεια, συμπεριλαμβανομένης και της προσωρινής άδειας κατά την έννοια του σημείου 11.15.

11.6. Η άδεια έχει ισχύ για το συντομότερο εκ των δύο: για πέντε έτη ή για τη διάρκεια των καθηκόντων βάσει των οποίων χορηγείται. Μπορεί να ανανεωθεί σύμφωνα με τη διαδικασία του σημείου 11.4.

11.7. Ο Πρόεδρος ανακαλεί την άδεια στις περιπτώσεις που θεωρεί ότι υπάρχουν αιτιολογημένοι λόγοι για την ανάκληση αυτή. Κάθε απόφαση για την ανάκληση της άδειας κοινοποιείται στον ενδιαφερόμενο βουλευτή του Ευρωπαϊκού Κοινοβουλίου, ο οποίος μπορεί να ζητήσει ακρόαση από τον Πρόεδρο προτού η ανάκληση τεθεί σε εφαρμογή καθώς και από την αρμόδια εθνική αρχή.

11.8. Ο έλεγχος ασφάλειας διενεργείται με τη συνδρομή του ενδιαφερομένου βουλευτή του Ευρωπαϊκού Κοινοβουλίου και κατόπιν αιτήσεως του Προέδρου. Η αρμόδια για τον έλεγχο εθνική αρχή είναι η αρχή του κράτους μέλους του οποίου είναι υπήκοος ο ενδιαφερόμενος βουλευτής.

11.9. Ως μέρος της διαδικασίας ελέγχου, μπορεί να ζητηθεί από τον ενδιαφερόμενο βουλευτή του Ευρωπαϊκού Κοινοβουλίου να συμπληρώσει έντυπο με προσωπικές πληροφορίες.

11.10. Ο Πρόεδρος προσδιορίζει στην αίτησή του στην αρμόδια εθνική αρχή το επίπεδο των διαβαθμισμένων πληροφοριών που πρόκειται να τεθούν στη διάθεση του ενδιαφερομένου βουλευτή, ώστε αυτή να μπορέσει να διενεργήσει τη διαδικασία ελέγχου.

11.11 Ολόκληρη η διαδικασία ελέγχου ασφάλειας που διενεργεί η αρμόδια εθνική αρχή μαζί με τα πορίσματα που προκύπτουν, συνάδει με τους σχετικούς κανόνες και ρυθμίσεις που ισχύουν στο οικείο κράτος μέλος, περιλαμβανομένων αυτών που αφορούν διαδικασίες προσφυγής.

11.2 Όταν η αρμόδια εθνική αρχή διατυπώνει θετική γνώμη, ο Πρόεδρος μπορεί να χορηγήσει άδεια στον ενδιαφερόμενο Βουλευτή του Ευρωπαϊκού Κοινοβουλίου.

11.13. Η αρνητική γνώμη της αρμόδιας εθνικής αρχή γνωστοποιείται στον ενδιαφερόμενο βουλευτή του Ευρωπαϊκού Κοινοβουλίου, ο οποίος μπορεί να ζητήσει ακρόαση από τον Πρόεδρο. Εφόσον το θεωρήσει απαραίτητο, ο Πρόεδρος μπορεί να ζητήσει από την αρμόδια εθνική αρχή περαιτέρω διευκρινίσεις. Εάν επιβεβαιωθεί η αρνητική γνώμη, η άδεια δεν χορηγείται.

11.14. Όλοι οι βουλευτές του Ευρωπαϊκού Κοινοβουλίου που λαμβάνουν άδεια κατά την έννοια του σημείου 11.3 λαμβάνουν, κατά τη χορήγηση της άδειας και στη συνέχεια σε τακτικά διαστήματα, τις τυχόν αναγκαίες κατευθυντήριες γραμμές σχετικά με την προστασία διαβαθμισμένων πληροφοριών και με τα μέσα για τη διασφάλιση της προστασίας αυτής. Οι εν λόγω βουλευτές υπογράφουν δήλωση με την οποία αναγνωρίζουν την παραλαβή αυτών των κατευθυντήριων γραμμών.

11.15. Σε εξαιρετικές περιπτώσεις, ο Πρόεδρος, αφού ειδοποιήσει την αρμόδια εθνική αρχή και υπό τον όρο ότι η εν λόγω αρχή δεν απαντήσει εντός ενός μηνός, μπορεί να χορηγήσει προσωρινή άδεια σε ένα βουλευτή του Ευρωπαϊκού Κοινοβουλίου για περίοδο που δεν υπερβαίνει τους έξι μήνες, εν αναμονή του αποτελέσματος του ελέγχου που αναφέρεται στο σημείο 11.11. Οι ούτως χορηγούμενες προσωρινές άδειες δεν επιτρέπουν την πρόσβαση σε πληροφορίες με διαβάθμιση σε επίπεδο TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του.

12. **ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΥΠΑΛΛΗΛΟΥΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟ ΛΟΙΠΟ ΠΡΟΣΩΠΙΚΟ ΤΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΠΟΥ ΕΡΓΑΖΕΤΑΙ ΓΙΑ ΤΙΣ ΠΟΛΙΤΙΚΕΣ ΟΜΑΔΕΣ**

12.1. Μόνο οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, οι οποίοι, λόγω των καθηκόντων τους και για τις ανάγκες της υπηρεσίας, απαιτείται να λάβουν γνώση ή να κάνουν χρήση διαβαθμισμένων πληροφοριών, δύνανται να έχουν πρόσβαση στις πληροφορίες αυτές.

12.2. Για να έχουν πρόσβαση σε πληροφορίες με τη διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του, οι ενδιαφερόμενοι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες έχουν λάβει σχετική άδεια σύμφωνα με τη διαδικασία που ορίζεται στα σημεία 12.3 και 12.4.

12.3. Η άδεια χορηγείται μόνο στα πρόσωπα που αναφέρονται στο σημείο 12.1 τα οποία έχουν υποστεί έλεγχο ασφάλειας από τις αρμόδιες εθνικές αρχές των κρατών μελών, σύμφωνα με τη διαδικασία των σημείων 12.9 έως 12.14. Ο Γενικός Γραμματέας είναι αρμόδιος για τη χορήγηση της άδειας στους υπαλλήλους του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες.

12.4. Ο Γενικός Γραμματέας μπορεί να χορηγήσει γραπτή άδεια αφού λάβει τη γνώμη των αρμόδιων εθνικών αρχών των κρατών μελών, βάσει του ελέγχου ασφάλειας που διενεργείται σύμφωνα με τα σημεία 12.8 έως 12.13.

12.5. Η Διεύθυνση Ασφάλειας και Αξιολόγησης Κινδύνου του Ευρωπαϊκού Κοινοβουλίου τηρεί ενημερωμένο κατάλογο όλων των θέσεων που απαιτούν έλεγχο ασφάλειας, όπως προβλέπονται από τις σχετικές υπηρεσίες του Ευρωπαϊκού Κοινοβουλίου, καθώς και όλων των προσώπων στα οποία έχει χορηγηθεί άδεια, συμπεριλαμβανομένης της προσωρινής άδειας σύμφωνα με το σημείο 12.15.

12.6. Η άδεια έχει ισχύ για το συντομότερο εκ των δύο: για πέντε έτη ή για τη διάρκεια των καθηκόντων βάσει των οποίων χορηγείται. Μπορεί να ανανεωθεί σύμφωνα με τη διαδικασία του σημείου 12.4.

12.7. Ο Γενικός Γραμματέας ανακαλεί την άδεια στις περιπτώσεις που θεωρεί ότι υπάρχουν αιτιολογημένοι λόγοι για την ανάκληση αυτή. Κάθε απόφαση για την ανάκληση της άδειας κοινοποιείται στον ενδιαφερόμενο υπάλληλο του Ευρωπαϊκού Κοινοβουλίου ή στο μέλος του λοιπού προσωπικού του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, που μπορεί να ζητήσει ακρόαση από το Γενικό Γραμματέα προτού η ανάκληση τεθεί σε εφαρμογή, καθώς και από την αρμόδια εθνική αρχή.

12.8. Ο έλεγχος ασφάλειας διενεργείται με τη συνδρομή του ενδιαφερομένου υπαλλήλου του Ευρωπαϊκού Κοινοβουλίου ή του μέλους του λοιπού προσωπικού του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες και κατόπιν αιτήσεως του Γενικού Γραμματέα. Η αρμόδια για τον έλεγχο εθνική αρχή είναι η αρχή του κράτους μέλους του οποίου είναι υπήκοος το πρόσωπο το οποίο αφορά η άδεια. Όταν επιτρέπεται από την εθνική νομοθεσία και κανονιστικές ρυθμίσεις, οι αρμόδιες εθνικές αρχές μπορούν να διεξαγάγουν έρευνες ασφάλειας σχετικά με μη υπηκόους που ζητούν πρόσβαση σε πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET.

12.9. Ως μέρος της διαδικασίας ελέγχου, μπορεί να ζητηθεί από τον ενδιαφερόμενο υπάλληλο του Ευρωπαϊκού Κοινοβουλίου ή από το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για μία πολιτική ομάδα να συμπληρώσει έντυπο με προσωπικές πληροφορίες.

12.10. Ο Γενικός Γραμματέας προσδιορίζει στην αίτησή του προς την αρμόδια εθνική αρχή το επίπεδο των διαβαθμισμένων πληροφοριών που πρόκειται να τεθούν στη διάθεση του ενδιαφερομένου υπαλλήλου του Ευρωπαϊκού Κοινοβουλίου ή του μέλους του λοιπού προσωπικού του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, ώστε αυτή να μπορέσει να διενεργήσει τη διαδικασία ελέγχου και να δώσει τη γνώμη της ως προς το επίπεδο της άδειας που θα ήταν κατάλληλο να χορηγηθεί στο εν λόγω πρόσωπο.

12.11. Ολόκληρη η διαδικασία ελέγχου ασφάλειας που διενεργούν η αρμόδια εθνική αρχή μαζί με τα πορίσματα που προκύπτουν, συνάδει με τους σχετικούς κανόνες και ρυθμίσεις που ισχύουν στο οικείο κράτος μέλος, περιλαμβανομένων των αυτών που αφορούν διαδικασίες προσφυγής.

12.12. Όταν η αρμόδια εθνική αρχή διατυπώνει θετική γνώμη, ο Γενικός Γραμματέας μπορεί να χορηγήσει άδεια στον ενδιαφερόμενο υπάλληλο του Ευρωπαϊκού Κοινοβουλίου ή στο μέλος του λοιπού προσωπικού του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες.

12.13. Η αρνητική γνώμη της αρμόδιας εθνικής αρχής γνωστοποιείται στον υπάλληλο του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για μία πολιτική ομάδα που μπορεί να ζητήσει ακρόαση από τον Γενικό Γραμματέα. Εφόσον το κρίνει αναγκαίο, ο Γενικός Γραμματέας μπορεί να ζητήσει από την αρμόδια εθνική αρχή οποιαδήποτε περαιτέρω διευκρίνιση μπορεί να παράσχει. Εάν επιβεβαιωθεί η αρνητική γνώμη, η άδεια δεν χορηγείται.

12.14. Όλοι οι υπάλληλοι του Ευρωπαϊκού Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες, στους οποίους χορηγείται άδεια κατά την έννοια των σημείων 12.4 και 12.5, λαμβάνουν, κατά τη στιγμή χορήγησης της άδειας και στη συνέχεια σε τακτικά διαστήματα, τις τυχόν αναγκαίες οδηγίες σχετικά με την προστασία διαβαθμισμένων πληροφοριών και με τα μέσα για τη διασφάλιση της προστασίας αυτής. Οι εν λόγω υπάλληλοι και το λοιπό προσωπικό υπογράφουν δήλωση με την οποία αναγνωρίζουν την παραλαβή των οδηγιών αυτών και δεσμεύονται ότι θα τις τηρήσουν.

12.15. Σε εξαιρετικές περιπτώσεις, ο Γενικός Γραμματέας, αφού ειδοποιήσει την αρμόδια εθνική αρχή και υπό τον όρο ότι η εν λόγω αρχή δεν απαντήσει εντός ενός μηνός, μπορεί να χορηγήσει προσωρινή άδεια σε ένα υπάλληλο του Ευρωπαϊκού Κοινοβουλίου ή στο λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για μία πολιτική ομάδα για μία περίοδο που δεν υπερβαίνει τους έξι μήνες, εν αναμονή του αποτελέσματος του ελέγχου που αναφέρεται στο σημείο 12.11. Οι ούτως χορηγούμενες προσωρινές άδειες δεν επιτρέπουν την πρόσβαση σε πληροφορίες με διαβάθμιση σε επίπεδο TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του.

ΠΑΡΑΡΤΗΜΑ II

ΕΙΣΑΓΩΓΗ

Στις κατωτέρω διατάξεις καθορίζονται οι κοινοποιήσεις ασφαλείας που διέπουν και εγγυώνται την ασφάλεια στον χειρισμό και τη διαχείριση των εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο. Οι εν λόγω κοινοποιήσεις ασφαλείας, σε συνδυασμό με τις οδηγίες χειρισμού, συνιστούν το σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ΣΔΑΠ) που αναφέρεται στο άρθρο 3 παράγραφος 2 της παρούσας απόφασης.

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 1

Η οργάνωση της ασφάλειας στο Ευρωπαϊκό Κοινοβούλιο, για την προστασία των εμπιστευτικών πληροφοριών

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 2

Διαχείριση εμπιστευτικών πληροφοριών

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 3

Η επεξεργασία των εμπιστευτικών πληροφοριών μέσω αυτόματων συστημάτων επικοινωνιών και πληροφοριών (ΣΕΠ)·

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 4

Υλική ασφάλεια

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 5

Βιομηχανική ασφάλεια

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 6

Παραβιάσεις της ασφάλειας, απώλεια ή διαρροή εμπιστευτικών πληροφοριών

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 1

Η ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

1. Ο Γενικός Γραμματέας είναι υπεύθυνος για την πλήρη και συνεπή εφαρμογή της παρούσας απόφασης.

Ο Γενικός Γραμματέας λαμβάνει όλα τα αναγκαία μέτρα για να εξασφαλίσει την εφαρμογή της παρούσας απόφασης στους χώρους του Κοινοβουλίου, για τους σκοπούς του χειρισμού και της αποθήκευσης εμπιστευτικών πληροφοριών, από τους βουλευτές και τους υπαλλήλους του Ευρωπαϊκού Κοινοβουλίου, και από το λοιπό προσωπικό του Κοινοβουλίου που απασχολείται από πολιτικές ομάδες και αναδόχους.

2. Ο Γενικός Γραμματέας είναι η Αρχή Ασφαλείας (SA). Υπό την ιδιότητά του αυτή, ο Γενικός Γραμματέας είναι υπεύθυνος για:

2.1. τον συντονισμό σε όλα τα θέματα που αφορούν τις δραστηριότητες του Κοινοβουλίου σε σχέση με την προστασία των εμπιστευτικών πληροφοριών·

2.2. την έγκριση της εγκατάστασης ενός Ασφαλούς Χώρου, ασφαλών αιθουσών ανάγνωσης και ασφαλούς εξοπλισμού·

2.3. την εφαρμογή αποφάσεων που επιτρέπουν, δυνάμει του άρθρου 6 της παρούσας απόφασης, τη διαβίβαση διαβαθμισμένων πληροφοριών από το Κοινοβούλιο σε τρίτους·

2.4. την έρευνα ή την ανάθεση έρευνας για κάθε διαρροή εμπιστευτικών πληροφοριών που εκ πρώτης όψεως συνέβη στο Κοινοβούλιο, σε επαφή με τον Πρόεδρο του Ευρωπαϊκού Κοινοβουλίου, σε περίπτωση που εμπλέκεται βουλευτής του Ευρωπαϊκού Κοινοβουλίου·

2.5. τη διατήρηση στενής επαφής με τις αρχές ασφαλείας άλλων θεσμικών οργάνων της Ένωσης και με τις εθνικές αρχές ασφαλείας στα κράτη μέλη, προκειμένου να εξασφαλίζεται ο βέλτιστος συντονισμός της πολιτικής ασφαλείας σε σχέση με τις διαβαθμισμένες πληροφορίες·

2.6. τη διαρκή αναθεώρηση της πολιτικής και των διαδικασιών του Κοινοβουλίου στον τομέα της ασφάλειας, και την έκδοση σχετικών συστάσεων·

2.7. την υποβολή εκθέσεων στην εθνική αρχή ασφάλειας (ΕΑΑ) που έχει διεξαγάγει τον έλεγχο ασφάλειας σύμφωνα με το παράρτημα Ι μέρος 2 σημείο 11.3, στις περιπτώσεις όπου υπάρχουν πληροφορίες για απειλή που μπορεί να αφορούν την αρχή αυτή·

3. Στην περίπτωση όπου εμπλέκονται βουλευτές του Ευρωπαϊκού Κοινοβουλίου, ο Γενικός Γραμματέας εκτελεί τα καθήκοντά του σε στενή συνεργασία με τον Πρόεδρο του Ευρωπαϊκού Κοινοβουλίου.

4. Ο Γενικός Γραμματέας επικουρείται στην εκτέλεση των καθηκόντων του από τον Αναπληρωτή Γενικό Γραμματέα, τη Γενική Διεύθυνση Ασφάλειας, τη Διεύθυνση Ασφαλείας και Αξιολόγησης Κινδύνου, τη Διεύθυνση Τεχνολογιών της Πληροφορίας (DIT), και τη Μονάδα Διαβαθμισμένων Πληροφοριών (CIU).

4.1. Η Διεύθυνση Ασφαλείας και Αξιολόγησης Κινδύνου είναι αρμόδια για τη λήψη μέτρων προσωπικής προστασίας και, ιδιαίτερα, για τη διαδικασία ελέγχου ασφάλειας που καθορίζεται στο παράρτημα Ι μέρος 2. Η Διεύθυνση Ασφαλείας και Αξιολόγησης Κινδύνου επίσης:

α) είναι ο σύνδεσμος με τις υπηρεσίες ασφάλειας των άλλων θεσμικών οργάνων της Ένωσης και των ΕΑΑ, για θέματα σχετικά με διαδικασίες ελέγχου ασφάλειας των βουλευτών του Ευρωπαϊκού Κοινοβουλίου και των υπαλλήλων του Ευρωπαϊκού Κοινοβουλίου, και του λοιπού προσωπικού του Κοινοβουλίου που απασχολείται στις πολιτικές ομάδες·

β) παρέχει την απαιτούμενη γενική ενημέρωση ασφάλειας σχετικά με τις υποχρεώσεις προστασίας των διαβαθμισμένων πληροφοριών και τις συνέπειες από την αθέτησή τους·

γ) παρακολουθεί τη λειτουργία του Ασφαλούς Χώρου και των ασφαλών αιθουσών ανάγνωσης στα κτίρια του Κοινοβουλίου, σε συνεργασία, όπου είναι σκόπιμο, με τις υπηρεσίες ασφάλειας των άλλων θεσμικών οργάνων της Ένωσης και των ΕΑΑ·

δ) ελέγχει, σε συνεργασία με τις υπηρεσίες ασφάλειας των λοιπών θεσμικών οργάνων της Ένωσης και ΕΑΑ, τις διαδικασίες διαχείρισης και αποθήκευσης διαβαθμισμένων πληροφοριών, τον Ασφαλή Χώρο και τις ασφαλείς αίθουσες ανάγνωσης στα κτίρια του Κοινοβουλίου όπου γίνεται χειρισμός διαβαθμισμένων πληροφοριών·

ε) προτείνει στον Γενικό Γραμματέα τις κατάλληλες οδηγίες χειρισμού.

4.2. Η DIT είναι υπεύθυνη για την ασφάλεια των συστημάτων πληροφορικής που χρησιμοποιούνται για τον χειρισμό εμπιστευτικών πληροφοριών από το Ευρωπαϊκό Κοινοβούλιο.

4.3. Η CIU είναι υπεύθυνη για:

α) τον προσδιορισμό των αναγκών ασφάλειας για την αποτελεσματική προστασία των εμπιστευτικών πληροφοριών, σε στενή συνεργασία με τη Διεύθυνση Ασφαλείας και Αξιολόγησης Κινδύνου και τη DIT, καθώς και με τις υπηρεσίες ασφαλείας των άλλων θεσμικών οργάνων της Ένωσης·

β) τον προσδιορισμό όλων των πτυχών της διαχείρισης και της αποθήκευσης των εμπιστευτικών πληροφοριών στο Κοινοβούλιο, σύμφωνα με τις οδηγίες χειρισμού·

γ) τη λειτουργία του Ασφαλούς Χώρου·

δ) τη διαχείριση ή τη μελέτη εμπιστευτικών πληροφοριών στον Ασφαλή Χώρο ή στην ασφαλή αίθουσα ανάγνωσης της CIU, σύμφωνα με το άρθρο 7 παράγραφοι 2 και 3 της παρούσας απόφασης·

ε) τη διαχείριση του μητρώου της CIU·

στ) την αναφορά στην SA, οποιασδήποτε αποδεδειγμένης ή εικαζόμενης παραβίασης της ασφάλειας, απώλειας ή διαρροής εμπιστευτικών πληροφοριών που έχει στην κατοχή της η CIU και διατηρούνται στον Ασφαλή Χώρο ή στην ασφαλή αίθουσα ανάγνωσης της CIU.

5. Επιπλέον, ο Γενικός Γραμματέας, ως SA, διορίζει τις ακόλουθες αρχές:

α) Αρχή Διαπίστευσης Ασφάλειας (SAA)·

β) Επιχειρησιακή Αρχή Ασφάλειας των Πληροφοριών (IAOA)·

γ) Αρχή Κρυπτογραφημένης Διανομής (CDA)·

δ) Αρχή TEMPEST (TA)·

ε) Αρχή Ασφάλειας των Πληροφοριών (IAA).

Η άσκηση των ανωτέρω καθηκόντων δεν απαιτεί ενιαίες οργανωτικές οντότητες. Οι εντολές είναι διακριτές. Ωστόσο, τα καθήκοντα αυτά και οι συνακόλουθες αρμοδιότητες μπορεί να συνδυάζονται ή να ενσωματώνονται στην ίδια οργανωτική οντότητα ή να διαιρούνται σε διάφορες οργανωτικές οντότητες, με την προϋπόθεση να αποφεύγονται οι συγκρούσεις συμφερόντων και οι επικαλύψεις καθηκόντων.

6. Η SAA παρέχει συμβουλές για όλα τα θέματα ασφάλειας που αφορούν τη διαπίστευση κάθε συστήματος και δικτύου πληροφορικής στο Κοινοβούλιο:

6.1. εξασφαλίζοντας ότι το ΣΕΠ συμμορφώνεται προς τις σχετικές πολιτικές ασφάλειας και τις κατευθυντήριες γραμμές ασφάλειας, παρέχοντας δήλωση έγκρισης για τον χειρισμό διαβαθμισμένων πληροφοριών από το ΣΕΠ σε καθορισμένο επίπεδο ταξινόμησης στο επιχειρησιακό περιβάλλον της, και αναφέροντας τους όρους και τις προϋποθέσεις διαπίστευσης και τα κριτήρια με βάση τα οποία απαιτείται επανέγκριση·

6.2. καθιερώνοντας διαδικασία διαπίστευσης ασφάλειας σύμφωνα με τις σχετικές πολιτικές, με σαφή αναφορά των όρων έγκρισης για το ΣΕΠ που έχει υπό την αρμοδιότητά της·

6.3. χαράσσοντας στρατηγική διαπίστευσης ασφάλειας που καθορίζει τον βαθμό λεπτομέρειας της διαδικασίας διαπίστευσης ανάλογα με το απαιτούμενο επίπεδο ασφάλειας·

6.4. εξετάζοντας και εγκρίνοντας τεκμηρίωση σχετική με την ασφάλεια, συμπεριλαμβανομένων δηλώσεων διαχείρισης κινδύνου και υπολειπόμενου κινδύνου, τεκμηρίωσης της επαλήθευσης της υλοποίησης των μέτρων ασφάλειας, και επιχειρησιακών διαδικασιών ασφάλειας, και εξασφαλίζοντας τη συμμόρφωσή της προς τους κανόνες και της πολιτικές ασφάλειας του Κοινοβουλίου·

6.5. επαληθεύοντας τη λήψη μέτρων ασφάλειας σε σχέση με το ΣΕΠ, με την ανάληψη ή τη χρηματοδότηση αξιολογήσεων, επιθεωρήσεων ή ελέγχων ασφάλειας·

6.6. προσδιορίζοντας τις απαιτήσεις ασφάλειας (π.χ. επίπεδα ασφάλειας προσωπικού) για ευαίσθητες θέσεις σε σχέση με το ΣΕΠ·

6.7. εγκρίνοντας ή, όπου είναι σκόπιμο, συμμετέχοντας στην κοινή έγκριση της διασύνδεσης δύο ΣΕΠ·

6.8. εγκρίνοντας τα πρότυπα ασφάλειας του τεχνικού εξοπλισμού που προορίζεται για τον ασφαλή χειρισμό και την προστασία των διαβαθμισμένων πληροφοριών·

6.9. εξασφαλίζοντας ότι τα προϊόντα κρυπτογράφησης που χρησιμοποιούνται στο Κοινοβούλιο περιλαμβάνονται στον κατάλογο των εγκεκριμένων σε επίπεδο ΕΕ προϊόντων· και

6.10. παρέχοντας συμβουλές στον πάροχο του συστήματος, στους συντελεστές της ασφάλειας, και στους εκπροσώπους των χρηστών σχετικά με τη διαχείριση των κινδύνων για την ασφάλεια, και ιδιαίτερα για τον υπολειπόμενο κίνδυνο, καθώς και για τους όρους και τις προϋποθέσεις της δήλωσης έγκρισης·

7. Η ΙΑΟΑ είναι αρμόδια για:

7.1. την ανάπτυξη πολιτικών τεκμηρίωσης ασφάλειας και κατευθυντήριων γραμμών ασφάλειας, συμπεριλαμβανομένων ιδιαίτερα της δήλωσης υπολειπόμενου κινδύνου, των επιχειρησιακών διαδικασιών ασφάλειας, και του σχεδίου κρυπτογράφησης στο πλαίσιο της διαδικασίας διαπίστευσης του ΣΕΠ·

7.2. τη συμμετοχή στην επιλογή και τη δοκιμή των ειδικών για το σύστημα μέτρων, συσκευών και λογισμικού τεχνικής ασφάλειας, για την εποπτεία της εφαρμογής τους και προκειμένου να εξασφαλίζεται η ασφαλής εγκατάσταση, ρύθμιση και συντήρησή τους σύμφωνα με τη σχετική τεκμηρίωση ασφάλειας·

7.3. την παρακολούθηση της υλοποίησης και της εφαρμογής των επιχειρησιακών διαδικασιών ασφάλειας και, όπου είναι σκόπιμο, την ανάθεση αρμοδιοτήτων επιχειρησιακής ασφάλειας στον ιδιοκτήτη του συστήματος, δηλαδή το ΣΕΠ·

7.4. τη διαχείριση και τον χειρισμό προϊόντων κρυπτογραφίας, με εξασφάλιση της φύλαξης κρυπτογραφημένων και ελεγχόμενων στοιχείων και, αν απαιτείται, με εξασφάλιση της δημιουργίας κρυπτογραφικών μεταβλητών·

7.5. τη διεξαγωγή αναλύσεων, ελέγχων και δοκιμών ασφάλειας, ιδιαίτερα στο πλαίσιο της εκπόνησης των σχετικών εκθέσεων κινδύνου, όπως απαιτείται από την SAA·

7.6. την παροχή ειδικής κατάρτισης του ΣΕΠ στην ασφάλεια των πληροφοριών·

7.7. την υλοποίηση και την εφαρμογή ειδικών μέτρων ασφάλειας του ΣΕΠ.

8. Η CDA είναι αρμόδια για:

8.1. τη διαχείριση και τη λογιστική για το κρυπτογραφικό υλικό της ΕΕ·

8.2. την εξασφάλιση, σε στενή συνεργασία με την SAA, της επιβολής των κατάλληλων διαδικασιών και της υλοποίησης σχεδίων για τη λογιστική, τον ασφαλή χειρισμό, την αποθήκευση και τη διανομή όλου του κρυπτογραφικού υλικού της ΕΕ· και

8.3. την εξασφάλιση της μεταφοράς του κρυπτογραφικού υλικού της ΕΕ προς ή από τους ιδιώτες ή τις υπηρεσίες που το χρησιμοποιούν.

9. Η ΤΑ είναι αρμόδια για την εξασφάλιση της συμμόρφωσης του ΣΕΠ προς τις πολιτικές και τις οδηγίες χειρισμού TEMPEST. Εγκρίνει αντίμετρα TEMPEST για εγκαταστάσεις και προϊόντα προστασίας των διαβαθμισμένων πληροφοριών σε καθορισμένο επίπεδο διαβάθμισης στο επιχειρησιακό της περιβάλλον.

10. Η ΙΑΑ είναι υπεύθυνη για όλες τις πτυχές της διαχείρισης και του χειρισμού των εμπιστευτικών πληροφοριών στο Κοινοβούλιο και, ειδικότερα, για:

10.1 την ανάπτυξη της προστασίας της ασφάλειας των πληροφοριών και των σχετικών κατευθυντήριων γραμμών, και την παρακολούθηση της αποτελεσματικότητας και της καταλληλότητάς τους·

10.2. τη διασφάλιση και την παροχή τεχνικών πληροφοριών σχετικά με κρυπτογραφικά προϊόντα·

10.3. την εξασφάλιση της συμμόρφωσης όλων των μέτρων διασφάλισης των πληροφοριών για την προστασία των διαβαθμισμένων πληροφοριών προς τις σχετικές πολιτικές που διέπουν την επιλεξιμότητα και την επιλογή τους·

10.4. την εξασφάλιση της επιλογής των κρυπτογραφικών προϊόντων σύμφωνα με τις πολιτικές που διέπουν την επιλεξιμότητα και την επιλογή τους·

10.5. τη διαβούλευση με τον πάροχο του συστήματος, τους συντελεστές της ασφάλειας, και τους εκπροσώπους των χρηστών σχετικά με την προστασία της διασφάλισης των πληροφοριών·

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 2

ΔΙΑΧΕΙΡΙΣΗ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Α. **ΕΙΣΑΓΩΓΗ**

1. Η παρούσα κοινοποίηση ασφαλείας καθορίζει τις διατάξεις για τη διαχείριση εμπιστευτικών πληροφοριών από το Κοινοβούλιο.

2. Κατά την παραγωγή εμπιστευτικών πληροφοριών, ο αρχικός συντάκτης αξιολογεί το επίπεδο εμπιστευτικότητας και αποφασίζει με βάση τις αρχές που καθορίζονται στην παρούσα κοινοποίηση ασφαλείας, για τη διαβάθμιση ή τη σήμανση της συγκεκριμένης πληροφορίας.

Β. **ΔΙΑΒΑΘΜΙΣΗ ΤΩΝ ΔΠΕΕ**

3. Η απόφαση για τη διαβάθμιση ενός εγγράφου λαμβάνεται πριν από τη δημιουργία του. Για τον σκοπό αυτό, η διαβάθμιση πληροφοριών ως ΔΠΕΕ προϋποθέτει την προηγούμενη αξιολόγηση του επιπέδου εμπιστευτικότητάς της και τη λήψη απόφασης από τον αρχικό συντάκτη, ότι η μη εξουσιοδοτημένη αποκάλυψη της συγκεκριμένης πληροφορίας θα βλάψει πολλαπλά τα συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών ή ιδιωτών.

4. Μετά τη λήψη της απόφασης για διαβάθμιση της πληροφορίας, ακολουθεί δεύτερη προηγούμενη αξιολόγηση, για τον προσδιορισμό του κατάλληλου επιπέδου διαβάθμισης. Η διαβάθμιση ενός εγγράφου καθορίζεται από το επίπεδο ευαισθησίας των περιεχομένων του.

5. Την ευθύνη για τη διαβάθμιση των πληροφοριών έχει αποκλειστικά ο αρχικός συντάκτης τους. Οι υπάλληλοι του Κοινοβουλίου διαβαθμίζουν τις πληροφορίες κατ' εντολή ή με εξουσιοδότηση του Γενικού Γραμματέα.

6. Η διαβάθμιση χρησιμοποιείται σωστά και με φειδώ. Ο αρχικός συντάκτης ενός εγγράφου το οποίο πρόκειται διαβαθμιστεί αποφεύγει την τάση προς υπερβολικά υψηλή ή χαμηλή διαβάθμιση.

7. Το επίπεδο διαβάθμισης των πληροφοριών καθορίζει το επίπεδο προστασίας τους στους τομείς της ασφάλειας προσωπικού, υλικής ασφάλειας, διαδικαστικής ασφάλειας και ασφάλειας των πληροφοριών.

8. Οι πληροφορίες που χρειάζονται διαβάθμιση υφίστανται σχετική σήμανση και χειρισμό, ανεξάρτητα από την υλική τους μορφή. Η διαβάθμιση κοινοποιείται σαφώς στους αποδέκτες της, είτε με σήμανση διαβάθμισης ασφάλειας (αν δίνεται σε έγγραφη μορφή, είτε σε χαρτί είτε σε ΣΕΠ) ή με ανακοίνωση (αν δίνεται προφορικά, όπως κατά τη διάρκεια συνομιλίας ή σε συνεδρίαση κεκλεισμένων των θυρών). Το διαβαθμισμένο υλικό έχει υλική σήμανση προκειμένου να αναγνωρίζεται εύκολα η διαβάθμιση ασφαλείας του.

9. ΔΠΕΕ σε ηλεκτρονική μορφή μπορούν να δημιουργηθούν μόνο στο πλαίσιο διαπιστευμένων ΣΕΠ. Οι διαβαθμισμένες πληροφορίες, όπως επίσης το όνομα του ηλεκτρονικού αρχείου που τις περιέχει και η μονάδα αποθήκευσης στην οποία βρίσκονται (αν είναι εξωτερική, όπως CD-ROM ή κλειδί USB) φέρουν την αντίστοιχη σήμανση διαβάθμισης ασφάλειας.

10. Οι πληροφορίες διαβαθμίζονται μόλις αποκτούν μορφή. Για παράδειγμα, οι προσωπικές σημειώσεις, τα σχέδια ή τα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν πληροφορίες οι οποίες χρειάζονται διαβάθμιση σημαίνονται από την αρχή ως ΔΠΕΕ και υφίστανται χειρισμό σύμφωνα με την παρούσα απόφαση και τις σχετικές οδηγίες της σε υλικό και σε τεχνικό επίπεδο. Οι πληροφορίες αυτές μπορεί να εξελιχτούν στη συνέχεια σε επίσημο έγγραφο, το οποίο με τη σειρά του υπόκειται σε σήμανση και χειρισμό. Κατά τη διαδικασία της σύνταξης, ένα επίσημο έγγραφο μπορεί να χρειαστεί να αξιολογηθεί εκ νέου και να διαβαθμιστεί υψηλότερα ή χαμηλότερα κατά την εξέλιξή του.

11. Ο αρχικός συντάκτης μπορεί να αποφασίσει να τυποποιήσει το επίπεδο διαβάθμισης των κατηγοριών πληροφοριών που δημιουργεί σε τακτική βάση. Ωστόσο, ο αρχικός συντάκτης εξασφαλίζει ότι στο πλαίσιο αυτό δεν διαβαθμίζει υπερβολικά υψηλά ή χαμηλά τις επιμέρους πληροφορίες.

12. Οι ΔΠΕΕ έχουν πάντα σήμανση διαβάθμισης ασφάλειας που να αντιστοιχεί στο επίπεδο διαβάθμισής τους.

Β.1. ***Επίπεδα διαβάθμισης***

13. Οι ΔΠΕΕ διαβαθμίζονται σε ένα από τα ακόλουθα επίπεδα:

— «TRÈS SECRET UE/EU TOP SECRET», όπως ορίζεται στο στοιχείο δ) του άρθρου 2 της παρούσας απόφασης, όταν η αποκάλυψή τους θα ήταν πιθανό:

α) να απειλήσει άμεσα την εσωτερική σταθερότητα της Ένωσης ή ενός ή περισσοτέρων κρατών μελών της ή τρίτων χωρών ή διεθνών οργανισμών·

β) να βλάψει εξαιρετικά σοβαρά τις σχέσεις με τρίτες χώρες ή διεθνείς οργανισμούς·

γ) να προκαλέσει άμεσα εκτεταμένη απώλεια ανθρώπινων ζωών·

δ) να επιφέρει εξαιρετικά σοβαρή ζημία στην επιχειρησιακή αποτελεσματικότητα ή την ασφάλεια του προσωπικού που έχουν αναπτύξει κράτη μέλη ή άλλοι συνεισφέροντες, ή να διακόψει την αποτελεσματικότητα εξαιρετικά χρήσιμων επιχειρήσεων ασφάλειας ή απόκτησης πληροφοριών· ή

ε) να προκαλέσει σοβαρή μακροπρόθεσμη ζημία στην οικονομία της Ένωσης ή κρατών μελών·

— «SECRET UE/EU SECRET», όπως ορίζεται στο στοιχείο δ) του άρθρου 2 της παρούσας απόφασης, όταν η αποκάλυψή τους θα ήταν πιθανό:

α) να προκαλέσει διεθνείς εντάσεις σε σημαντικό βαθμό·

β) να βλάψει σοβαρά τις σχέσεις με τρίτες χώρες και διεθνείς οργανισμούς·

γ) να απειλήσει άμεσα την ανθρώπινη ζωή ή να υπονομεύσει σοβαρά τη δημόσια τάξη ή την ατομική ασφάλεια ή ελευθερία·

δ) να βλάψει σημαντικές εμπορικές ή πολιτικές διαπραγματεύσεις, προκαλώντας σημαντικά επιχειρησιακά προβλήματα για την Ένωση ή για κράτη μέλη·

ε) να επιφέρει σοβαρή ζημία στην επιχειρησιακή αποτελεσματικότητα κρατών μελών, ή στην αποτελεσματικότητα εξαιρετικά χρήσιμων επιχειρήσεων ασφάλειας ή απόκτησης πληροφοριών·

στ) να βλάψει σοβαρά και ουσιαστικά τα χρηματοπιστωτικά, νομισματικά, οικονομικά και εμπορικά συμφέροντα της Ένωσης ή κράτους μέλους·

ζ) να υπονομεύσει σοβαρά την οικονομική βιωσιμότητα μεγάλων οργανισμών ή φορέων εκμετάλλευσης· ή

η) να παρακωλύσει σημαντικά την ανάπτυξη ή την εφαρμογή πολιτικών της Ένωσης με μείζονες οικονομικές, εμπορικές και χρηματοπιστωτικές συνέπειες·

— «CONFIDENTIEL UE/EU CONFIDENTIAL», όπως ορίζεται στο στοιχείο δ) του άρθρου 2 της παρούσας απόφασης, όταν η αποκάλυψή τους θα ήταν πιθανό:

α) να βλάψει σημαντικά διπλωματικές σχέσεις, π.χ. αν προκαλέσει επίσημη διαμαρτυρία ή άλλες κυρώσεις·

β) να θέσει σε κίνδυνο την ασφάλεια ή την ελευθερία προσώπων·

γ) να θέσει την έκβαση σοβαρών εμπορικών ή πολιτικών διαπραγματεύσεων σε σοβαρό κίνδυνο, προκαλώντας επιχειρησιακά προβλήματα για την Ένωση ή για κράτη μέλη·

δ) να επιφέρει ζημία στην επιχειρησιακή αποτελεσματικότητα κρατών μελών ή στην αποτελεσματικότητα επιχειρήσεων ασφάλειας ή απόκτησης πληροφοριών·

ε) να υπονομεύσει ουσιαστικά την οικονομική βιωσιμότητα μεγάλων οργανισμών ή φορέων εκμετάλλευσης·

στ) να παρακωλύσει την έρευνα ή να διευκολύνει τη διάπραξη εγκλημάτων ή τρομοκρατικών ενεργειών·

ζ) να αποβεί ουσιαστικά εις βάρος των χρηματοπιστωτικών, νομισματικών, οικονομικών και εμπορικών συμφερόντων της Ένωσης ή κρατών μελών· ή

η) να παρακωλύσει σοβαρά την ανάπτυξη ή την εφαρμογή πολιτικών της Ένωσης με μείζονες οικονομικές, εμπορικές και χρηματοπιστωτικές συνέπειες·

— «RESTREINT UE/EU RESTRICTED», όπως ορίζεται στο στοιχείο δ) του άρθρου 2 της παρούσας απόφασης, όταν η αποκάλυψή τους θα ήταν πιθανό:

α) να βλάψει τα γενικά συμφέροντα της Ένωσης·

β) να βλάψει τις διπλωματικές σχέσεις·

γ) να θέσει σε δυσχερή θέση πρόσωπα ή επιχειρήσεις·

δ) να αποδυναμώσει τη θέση της Ένωσης ή κρατών μελών σε εμπορικές ή πολιτικές διαπραγματεύσεις·

ε) να δυσχεράνει ουσιαστικά τη διατήρηση της ασφάλειας στην Ένωση ή σε κράτη μέλη·

στ) να εμποδίσει την ουσιαστική ανάπτυξη ή την εφαρμογή πολιτικών της Ένωσης·

ζ) να υπονομεύσει την ορθή διαχείριση της Ένωσης και των επιχειρήσεών της·

η) να προκαλέσει την αθέτηση ανειλημμένων δεσμεύσεων του Κοινοβουλίου σχετικά με τη διατήρηση της διαβάθμισης πληροφοριών που έχει λάβει από τρίτα μέρη·

θ) να παραβιάσει συμβατικούς περιορισμούς σχετικά με την αποκάλυψη πληροφοριών·

ι) να προκαλέσει οικονομική ζημία ή να διευκολύνει αθέμιτα κέρδη ή πλεονεκτήματα για πρόσωπα ή επιχειρήσεις· ή

ια) να βλάψει την έρευνα ή διευκολύνει τη διάπραξη εγκλημάτων.

Β.2. ***Διαβάθμιση συλλογών, διαβιβαστικών και περιλήψεων***

14. Η διαβάθμιση μιας επιστολής ή ενός σημειώματος που περιλαμβάνει συνημμένα έγγραφα καθορίζεται στο επίπεδο της υψηλότερης διαβάθμισης που εφαρμόζεται σε ένα από τα συνημμένα έγγραφα. Ο αρχικός συντάκτης επισημαίνει σαφώς σε ποιο επίπεδο πρέπει να διαβαθμιστεί η επιστολή ή το σημείωμα όταν αποχωριστεί από τα επισυναπτόμενα έγγραφα. Αν το διαβιβαστικό σημείωμα ή η διαβιβαστική επιστολή δεν χρειάζεται διαβάθμιση, περιλαμβάνει την ακόλουθη διατύπωση: «Το παρόν σημείωμα/η παρούσα επιστολή δεν έχει διαβάθμιση όταν δεν συνοδεύει τα συνημμένα έγγραφα.»

15. Έγγραφα ή αρχεία που περιλαμβάνουν στοιχεία με διαφορετικά επίπεδα διαβάθμισης πρέπει όποτε είναι δυνατόν να διαρθρώνονται με τρόπο ώστε τα στοιχεία που έχουν διαφορετικό επίπεδο διαβάθμισης να εντοπίζονται εύκολα και να διαχωρίζονται αν χρειαστεί. Το γενικό επίπεδο διαβάθμισης ενός εγγράφου ή αρχείου είναι τουλάχιστον εκείνο του υψηλότερα διαβαθμισμένου στοιχείου του.

16 Επιμέρους σελίδες, παράγραφοι, τμήματα, παραρτήματα, προσαρτήματα και συνημμένα ενός εγγράφου ενδέχεται να απαιτούν διαφορετικές διαβαθμίσεις και διαβαθμίζονται ανάλογα. Στα έγγραφα που περιέχουν ΔΠΕΕ μπορούν να χρησιμοποιούνται τυποποιημένες συντμήσεις για την επισήμανση του επιπέδου διαβάθμισης τμημάτων ή εδαφίων μικρότερων από μία σελίδα.

17. Κατά τη συγχώνευση πληροφοριών από διάφορες πηγές, το τελικό προϊόν επανεξετάζεται για να προσδιοριστεί το γενικό επίπεδο διαβάθμισής του, δεδομένου ότι μπορεί να απαιτεί υψηλότερο επίπεδο διαβάθμισης από το συστατικό στοιχείο του.

Γ. **ΑΛΛΕΣ ΕΜΠΙΣΤΕΥΤΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ**

18. Οι «άλλες εμπιστευτικές πληροφορίες» σημαίνονται σύμφωνα με το σημείο Ε της παρούσας κοινοποίησης ασφαλείας και τις οδηγίες χειρισμού.

Δ. **ΔΗΜΙΟΥΡΓΙΑ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

19. Εμπιστευτικές πληροφορίες μπορούν να δημιουργούν μόνο τα πρόσωπα που εξουσιοδοτούνται από την παρούσα απόφαση ή που εξουσιοδοτεί η SA.

20. Οι εμπιστευτικές πληροφορίες δεν καταχωρίζονται σε διαδικτυακά ή ενδοδικτυακά συστήματα διαχείρισης εγγράφων.

Δ.1. ***Δημιουργία ΔΠΕΕ***

21. Για τη δημιουργία ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET, οι ενδιαφερόμενοι εξουσιοδοτούνται με βάση την παρούσα απόφαση ή έχουν λάβει προηγουμένως εξουσιοδότηση δυνάμει του άρθρου 4 παράγραφος 1 της παρούσας απόφασης.

22. ΔΠΕΕ με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL δημιουργούνται μόνο στον Ασφαλή Χώρο.

23. Για τη δημιουργία ΔΠΕΕ ισχύουν οι ακόλουθοι κανόνες:

α) κάθε σελίδα σημειώνεται σαφώς με το αντίστοιχο επίπεδο διαβάθμισης·

β) σε κάθε σελίδα αναγράφονται ο αριθμός της και ο συνολικός αριθμός σελίδων·

γ) στην πρώτη σελίδα του εγγράφου αναφέρονται ο αριθμός αναφοράς και το θέμα του, που δεν συνιστά το ίδιο διαβαθμισμένη πληροφορία, εκτός αν υπάρχει σχετική αναφορά·

δ) στην πρώτη σελίδα του εγγράφου αναγράφεται η ημερομηνία·

ε) στην πρώτη σελίδα κάθε εγγράφου με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET περιλαμβάνεται κατάλογος όλων των παραρτημάτων και προσαρτημάτων·

στ) τα έγγραφα με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET περιλαμβάνουν σε όλες τις σελίδες τους τον αριθμό του αντιτύπου, αν διανέμονται σε περισσότερα αντίτυπα. Στην πρώτη σελίδα κάθε αντιτύπου αναγράφονται επίσης ο συνολικός αριθμός αντιτύπων και σελίδων, καθώς επίσης

ζ) αν το έγγραφο περιλαμβάνει παραπομπές σε άλλα έγγραφα με διαβαθμισμένες πληροφορίες που έχουν ληφθεί από θεσμικά όργανα της Ένωσης, ή αν περιλαμβάνει διαβαθμισμένες πληροφορίες από τέτοια έγγραφα, έχει το ίδιο επίπεδο διαβάθμισης με τα έγγραφα αυτά και δεν επιτρέπεται να διανέμεται, χωρίς τη γραπτή έγκριση του αρχικού συντάκτη του, σε πρόσωπα άλλα από εκείνα που αναφέρονται στον κατάλογο παραληπτών του αρχικού εγγράφου ή των αρχικών εγγράφων που περιέχουν τις διαβαθμισμένες πληροφορίες.

24. Ο αρχικός συντάκτης διατηρεί τον έλεγχο των ΔΠΕΕ που έχει δημιουργήσει. Ζητείται η γραπτή έγκρισή του προκειμένου οι συγκεκριμένες ΔΠΕΕ

α) να περάσουν σε χαμηλότερο επίπεδο διαβάθμισης ή να αποχαρακτηριστούν·

β) να χρησιμοποιηθούν για σκοπούς άλλους από εκείνους που έχει ορίσει ο αρχικός συντάκτης·

γ) να κοινοποιηθούν σε τρίτο κράτος ή σε διεθνή οργανισμό·

δ) να κοινοποιηθούν σε οποιοδήποτε πρόσωπο, ίδρυμα, κράτος ή διεθνή οργανισμό άλλο από εκείνα που περιλαμβάνονται στον αρχικό κατάλογο παραληπτών που συνέταξε ο αρχικός συντάκτης·

ε) να κοινοποιηθούν σε ανάδοχο ή δυνητικό ανάδοχο που βρίσκεται σε τρίτη χώρα·

στ) να αντιγραφούν ή να μεταφραστούν, αν οι πληροφορίες έχουν διαβάθμιση σε επίπεδο TRES SECRET UE/EU TOP SECRET·

ζ) να καταστραφούν.

Δ.2. ***Δημιουργία άλλων εμπιστευτικών πληροφοριών***

25. Ο Γενικός Γραμματέας, υπό την ιδιότητά του ως SA μπορεί να αποφασίζει σχετικά με την έγκριση της δημιουργίας «άλλων εμπιστευτικών πληροφοριών» από όργανο, υπηρεσία και/ή ιδιώτη.

26. Οι «άλλες εμπιστευτικές πληροφορίες» φέρουν μία από τις σημάνσεις που ορίζονται στις οδηγίες χειρισμού.

27. Για τη δημιουργία «άλλων εμπιστευτικών πληροφοριών» ισχύουν οι ακόλουθοι κανόνες:

α) η σήμανση τοποθετείται στην κορυφή της πρώτης σελίδας του εγγράφου·

β) σε κάθε σελίδα αναγράφονται ο αριθμός της και ο συνολικός αριθμός σελίδων·

γ) στην πρώτη σελίδα του εγγράφου αναφέρονται ο αριθμός αναφοράς και το θέμα του·

δ) στην πρώτη σελίδα του εγγράφου αναγράφεται η ημερομηνία, και

ε) η τελευταία σελίδα του εγγράφου περιλαμβάνει κατάλογο όλων των παραρτημάτων και προσαρτημάτων.

28. Η δημιουργία «άλλων εμπιστευτικών πληροφοριών» υπόκειται σε ειδικούς κανόνες και διαδικασίες, που καθορίζονται στις οδηγίες χειρισμού.

Ε. **ΕΝΔΕΙΞΕΙΣ ΚΑΙ ΣΗΜΑΝΣΕΙΣ ΑΣΦΑΛΕΙΑΣ**

29. Οι ενδείξεις και οι σημάνσεις ασφάλειας στα έγγραφα έχουν ως στόχο τον έλεγχο της ροής των πληροφοριών και τον περιορισμό της πρόσβασης στις εμπιστευτικές πληροφορίες με βάση την αρχή της «ανάγκης γνώσης».

30. Όταν χρησιμοποιούνται ή τοποθετούνται ενδείξεις και/ή σημάνσεις ασφάλειας, λαμβάνεται μέριμνα για την αποφυγή της σύγχυσης με τις διαβαθμίσεις ασφάλειας των ΔΠΕΕ: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET.

31. Στις οδηγίες χειρισμού περιλαμβάνονται ειδικοί κανόνες για τη χρήση ενδείξεων και σημάνσεων ασφάλειας, καθώς και κατάλογος των εγκεκριμένων σημάνσεων ασφάλειας του Ευρωπαϊκού Κοινοβουλίου.

Ε.1. ***Ενδείξεις ασφάλειας***

32. Οι ενδείξεις ασφάλειας μπορούν να χρησιμοποιούνται μόνο σε συνδυασμό με μια διαβάθμιση ασφάλειας και δεν εφαρμόζονται χωριστά σε έγγραφα. Στις ΔΠΕΕ μπορεί να εφαρμοστεί ένδειξη ασφάλειας, για

α) τον περιορισμό της ισχύος της διαβάθμισης (που σημαίνει για τις διαβαθμισμένες πληροφορίες αυτόματο υποχαρακτηρισμό ή αποχαρακτηρισμό).

β) τον περιορισμό της διανομής των ΔΠΕΕ·

γ) τον καθορισμό ειδικών ρυθμίσεων χειρισμού, επιπλέον εκείνων που αντιστοιχούν στο επίπεδο διαβάθμισης ασφάλειας.

33. Οι πρόσθετοι έλεγχοι που εφαρμόζονται στον χειρισμό και την αποθήκευση εγγράφων που περιέχουν ΔΠΕΕ επιβάλλουν πρόσθετο φόρτο σε όλους τους εμπλεκόμενους. Για την ελαχιστοποίηση της απαιτούμενης εργασίας, στο πλαίσιο αυτό, αποτελεί ορθή πρακτική να καθορίζεται κατά τη δημιουργία τέτοιου είδους εγγράφων το χρονικό διάστημα ή το γεγονός μετά το οποίο η διαβάθμιση παύει αυτομάτως να ισχύει και οι πληροφορίες που περιέχονται στο έγγραφο υποχαρακτηρίζονται ή αποχαρακτηρίζονται.

34. Όταν ένα έγγραφο αφορά συγκεκριμένο τομέα εργασίας και η διανομή του πρέπει να περιορίζεται και/ή να υπόκειται σε ειδικό χειρισμό, μπορεί να προστίθεται στη διαβάθμισή του σχετική δήλωση που διευκολύνει τον προσδιορισμό του κοινού στο οποίο απευθύνεται.

Ε.2. ***Σημάνσεις***

35. Οι σημάνσεις δεν συνιστούν διαβάθμιση ασφάλειας. Εξυπηρετούν απλώς ως πρόσθετες εντολές χειρισμού του εγγράφου, και δεν χρησιμοποιούνται για την περιγραφή των περιεχομένων του.

36. Οι σημάνσεις μπορούν να χρησιμοποιούνται χωριστά σε έγγραφα ή σε συνδυασμό με διαβάθμιση ασφάλειας.

37. Κατά γενικό κανόνα, οι σημάνσεις εφαρμόζονται σε πληροφορίες που καλύπτονται από το επαγγελματικό απόρρητο όπως αναφέρεται στο άρθρο 339 ΣΛΕΕ και στο άρθρο 17 του Κανονισμού Υπηρεσιακής Κατάστασης, ή οι οποίες πρέπει να προστατευτούν για νομικούς λόγους από το Κοινοβούλιο, αλλά δεν χρειάζεται ή δεν είναι δυνατόν να διαβαθμιστούν.

Ε.3. ***Χρήση σημάνσεων σε ΣΕΠ***

38. Οι κανόνες για τη χρήση σημάνσεων έχουν εφαρμογή και στα διαπιστευμένα ΣΕΠ.

39. Η SAA θεσπίζει τους ειδικούς κανόνες για τη χρήση σημάνσεων στα διαπιστευμένα ΣΕΠ.

ΣΤ. **ΠΑΡΑΛΑΒΗ ΠΛΗΡΟΦΟΡΙΩΝ**

40. Μόνο η CIU έχει δικαίωμα στο Κοινοβούλιο να λαμβάνει πληροφορίες διαβαθμισμένες σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL; SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET, ή σε ισοδύναμό του από τρίτα μέρη.

41. Για πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και για «άλλες εμπιστευτικές πληροφορίες», τόσο η CIU όσο και το αρμόδιο κοινοβουλευτικό όργανο/αξιωματούχος μπορεί να έχουν την ευθύνη για την παραλαβή τους από τρίτα μέρη, και για την εφαρμογή των αρχών που καθορίζονται στην παρούσα κοινοποίηση ασφάλειας.

Ζ. **ΚΑΤΑΧΩΡΙΣΗ**

42. «Καταχώριση»: η εφαρμογή των διαδικασιών για την καταγραφή του κύκλου ζωής των εμπιστευτικών πληροφοριών, συμπεριλαμβανομένων της διάδοσης και της καταστροφής τους.

43. Για τους σκοπούς της παρούσας κοινοποίησης ασφάλειας, «βιβλίο καταγραφής» είναι ένα μητρώο στο οποίο καταγράφονται ειδικότερα οι ημερομηνίες και οι ώρες κατά τις οποίες εμπιστευτικές πληροφορίες

α) λαμβάνονται ή αποστέλλονται από την αντίστοιχη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου ή, κατά περίπτωση, από την CIU·

β) ανακτώνται από ή διαβιβάζονται σε πρόσωπο που έχει υποστεί έλεγχο ασφάλειας· και

γ) καταστρέφονται.

44. Ο αρχικός συντάκτης των διαβαθμισμένων πληροφοριών είναι υπεύθυνος για την αρχική δήλωση κατά τη δημιουργία εγγράφου που περιλαμβάνει τέτοιες πληροφορίες. Η δήλωση κοινοποιείται στην CIU όταν δημιουργείται το έγγραφο.

45. Η CIU μπορεί να καταχωρίζει πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του μόνο για σκοπούς ασφάλειας. Οι πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και οι «άλλες εμπιστευτικές πληροφορίες» που λαμβάνονται από τρίτα μέρη καταχωρίζονται από την υπηρεσία που είναι αρμόδια για την επίσημη παραλαβή του εγγράφου, είτε αυτή είναι η CIU είτε η γραμματεία του αρμόδιου κοινοβουλευτικού οργάνου/αξιωματούχου, για διοικητικούς σκοπούς. Οι «άλλες εμπιστευτικές πληροφορίες» που δημιουργούνται στο Κοινοβούλιο καταχωρίζονται από τον αρχικό συντάκτη για διοικητικούς σκοπούς.

46. ΔΠΕΕ με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του καταχωρίζονται ιδιαίτερα όταν:

α) δημιουργούνται·

β) λαμβάνονται από την CIU ή αποστέλλονται από εκεί· και

γ) λαμβάνονται από το ΣΕΠ ή αποστέλλονται από εκεί.

47. Πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του καταχωρίζονται ιδιαίτερα όταν:

α) δημιουργούνται·

β) λαμβάνονται από την αντίστοιχη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου ή στην CIU ή αποστέλλονται από εκεί· και

γ) λαμβάνονται από ένα ΣΕΠ ή αποστέλλονται από εκεί.

48. Η καταχώριση εμπιστευτικών πληροφοριών μπορεί να πραγματοποιείται σε χαρτί ή σε ηλεκτρονικά βιβλία καταγραφής/ΣΕΠ.

49. Για πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό τους και για «άλλες εμπιστευτικές πληροφορίες», καταγράφονται τουλάχιστον τα ακόλουθα:

α) η ημερομηνία και η ώρα που λαμβάνονται ή αποστέλλονται από την αντίστοιχη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου ή, κατά περίπτωση, από την CIU·

β) ο τίτλος του εγγράφου, το επίπεδο διαβάθμισης και οποιοσδήποτε αριθμός αναφοράς που έχει δοθεί στο έγγραφο,

50. Για πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του, και για «άλλες εμπιστευτικές πληροφορίες», καταγράφονται τουλάχιστον τα ακόλουθα:

α) η ημερομηνία και η ώρα λήψης ή αποστολής από την CIU·

β) ο τίτλος του εγγράφου, το επίπεδο διαβάθμισης ή η σήμανση, οποιοσδήποτε αριθμός αναφοράς που έχει δοθεί στο έγγραφο, και η καταληκτική ημερομηνία της διαβάθμισης/σήμανσης

γ) τα στοιχεία του αρχικού συντάκτη·

δ) ο κατάλογος με τα στοιχεία των προσώπων στα οποία επιτράπηκε η πρόσβαση στο έγγραφο, και η ημερομηνία πρόσβασης·

ε) ο κατάλογος των αντιγράφων ή μεταφράσεων του εγγράφου·

στ) η ημερομηνία και η ώρα κατά την οποία αποστέλλονται από την CIU ή επιστρέφονται σε αυτήν αντίγραφα ή μεταφράσεις του εγγράφου, καθώς και λεπτομερή στοιχεία για το πού στάλθηκαν και ποιος τα επέστρεψε·

ζ) η ημερομηνία και η ώρα καταστροφής του εγγράφου, και η ταυτότητα του προσώπου που το κατέστρεψε, σύμφωνα με τους κανόνες ασφάλειας του Κοινοβουλίου που ισχύουν για την καταστροφή· και

η) ο αποχαρακτηρισμός ή ο υποχαρακτηρισμός του εγγράφου.

51. Τα βιβλία καταγραφής διαβαθμίζονται ή σημαίνονται ανάλογα. Τα βιβλία καταγραφής πληροφοριών με διαβάθμιση σε επίπεδο TRES SECRET UE/EU TOP SECRET ή σε ισοδύναμό του καταχωρίζονται στο ίδιο επίπεδο.

52. Οι διαβαθμισμένες πληροφορίες μπορούν να καταχωρίζονται:

α) σε ενιαίο βιβλίο καταγραφής· ή

β) σε χωριστά βιβλία καταγραφής ανάλογα με το επίπεδο διαβάθμισής τους, το αν είναι εισερχόμενες ή εξερχόμενες πληροφορίες και την προέλευση ή τον προορισμό τους.

53. Στην περίπτωση ηλεκτρονικού χειρισμού στο πλαίσιο ΣΕΠ, μπορεί να εκτελούνται μέσα στο ίδιο το ΣΕΠ διαδικασίες καταχώρισης οι οποίες πληρούν απαιτήσεις ισοδύναμες με τις προαναφερόμενες. Όταν ΔΠΕΕ βγαίνουν από την περίμετρο του ΣΕΠ, εφαρμόζεται η διαδικασία καταχώρισης που περιγράφεται ανωτέρω.

54. Η CIU τηρεί μητρώο όλων των διαβαθμισμένων πληροφοριών που έχει κοινοποιήσει το Κοινοβούλιο σε τρίτους, και των διαβαθμισμένων πληροφοριών που έχει λάβει το Κοινοβούλιο από τρίτους.

55. Όταν ολοκληρώνεται η καταχώριση πληροφοριών με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του, η CIU ελέγχει αν ο παραλήπτης έχει έγκυρη άδεια ασφαλείας. Στην περίπτωση αυτή, ο παραλήπτης ειδοποιείται από την CIU. Η ανάκτηση διαβαθμισμένων πληροφοριών μπορεί να γίνει μόνο μετά την καταχώριση του εγγράφου που τις περιέχει.

Η. **ΔΙΑΝΟΜΗ**

56. Ο αρχικός συντάκτης καταρτίζει τον αρχικό κατάλογο παραληπτών για τις ΔΠΕΕ που έχει δημιουργήσει.

57. Πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED και άλλες εμπιστευτικές πληροφορίες που δημιουργεί το Κοινοβούλιο διανέμονται στο εσωτερικό του Κοινοβουλίου από τον αρχικό συντάκτη σύμφωνα με τις σχετικές οδηγίες χειρισμού και με βάση την αρχή της «ανάγκης γνώσης». Για πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET, που δημιουργεί το Κοινοβούλιο στον Ασφαλή Χώρο, ο κατάλογος παραληπτών (και τυχόν περαιτέρω οδηγίες σχετικά με τη διανομή) κοινοποιείται στην CIU, η οποία είναι υπεύθυνη για τη διαχείρισή του.

58. ΔΠΕΕ που δημιουργεί το Κοινοβούλιο μπορούν να διανέμονται σε τρίτους μόνο από την CIU, με βάση την αρχή της «ανάγκης γνώσης».

59. Εμπιστευτικές πληροφορίες που λαμβάνονται είτε από την CIU είτε από κοινοβουλευτικό όργανο/αξιωματούχο που έχει υποβάλει σχετικό αίτημα διανέμονται σύμφωνα με τις οδηγίες που λαμβάνονται από τον αρχικό συντάκτη.

Θ. **ΧΕΙΡΙΣΜΟΣ, ΑΠΟΘΗΚΕΥΣΗ ΚΑΙ ΕΞΕΤΑΣΗ**

60. Ο χειρισμός, η αποθήκευση και η εξέταση εμπιστευτικών πληροφοριών διεξάγονται σύμφωνα με την κοινοποίηση ασφάλειας 4 και τις οδηγίες χειρισμού.

Ι. **ΑΝΤΙΓΡΑΦΗ/ΜΕΤΑΦΡΑΣΗ/ΔΙΕΡΜΗΝΕΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

61. Έγγραφα που περιέχουν πληροφορίες με διαβάθμιση σε επίπεδο TRES SECRET UE/EU TOP SECRET ή σε ισοδύναμό του δεν επιτρέπεται να αντιγράφονται ή να μεταφράζονται χωρίς την προηγούμενη γραπτή συγκατάθεση του αρχικού συντάκτη. Τα έγγραφα με διαβάθμιση σε επίπεδο SECRET UE/EU SECRET ή σε ισοδύναμό του, ή σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή σε ισοδύναμό του επιτρέπεται να αντιγραφούν ή να μεταφραστούν καθ' υπόδειξη του κατόχου, με την προϋπόθεση ότι δεν το απαγορεύει ο αρχικός συντάκτης.

62. Κάθε αντίγραφο εγγράφου που περιέχει πληροφορίες με διαβάθμιση σε ε επίπεδο TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET ή CONFIDENTIEL UE/EU CONFIDENTIAL ή σε ισοδύναμό του καταχωρίζονται για λόγους ασφαλείας.

63. Τα μέτρα ασφαλείας που εφαρμόζονται για το αρχικό έγγραφο που περιέχει διαβαθμισμένες πληροφορίες εφαρμόζονται επίσης στα αντίγραφα και τις μεταφράσεις του.

64. Τα έγγραφα που λαμβάνονται από το Συμβούλιο θα πρέπει να λαμβάνονται σε όλες τις επίσημες γλώσσες.

65. Μπορούν να ζητούνται από τον αρχικό συντάκτη ή τον κάτοχο αντιτύπου αντίγραφα και/ή μεταφράσεις εγγράφων που περιέχουν διαβαθμισμένες πληροφορίες. Αντίγραφα εγγράφων που περιέχουν πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του επιτρέπεται να δημιουργούνται στον ασφαλή χώρο και σε φωτοαντιγραφικά μηχανήματα που ανήκουν σε διαπιστευμένο ΣΕΠ. Αντίγραφα εγγράφων που περιέχουν πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλες εμπιστευτικές πληροφορίες» δημιουργούνται σε διαπιστευμένο εξοπλισμό αναπαραγωγής στα κτίρια του Κοινοβουλίου.

66. Όλα τα αντίγραφα και οι μεταφράσεις οποιουδήποτε εγγράφου ή μερών εγγράφων που περιέχουν διαβαθμισμένες πληροφορίες σημαίνονται, αριθμούνται και καταχωρίζονται κατάλληλα.

67. Δεν επιτρέπεται η δημιουργία περισσότερων αντιγράφων από όσα είναι αυστηρά αναγκαία. Όλα τα αντίγραφα καταστρέφονται σύμφωνα με τις οδηγίες χειρισμού, στη λήξη της περιόδου μελέτης τους.

68. Μόνο διερμηνείς και μεταφραστές που είναι μόνιμοι υπάλληλοι του Κοινοβουλίου έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες.

69. Οι διερμηνείς και οι μεταφραστές που έχουν πρόσβαση σε έγγραφα με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του έχουν το κατάλληλο επίπεδο ελέγχου ασφαλείας.

70. Ο χειρισμός εγγράφων με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του από διερμηνείς και μεταφραστές γίνεται στον Ασφαλή Χώρο.

IA. **ΥΠΟΧΑΡΑΚΤΗΡΙΣΜΟΣ, ΑΠΟΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΑΙ ΑΦΑΙΡΕΣΗ ΣΗΜΑΝΣΗΣ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ.**

IA.1. ***Γενικές αρχές***

71. Οι εμπιστευτικές πληροφορίες αποχαρακτηρίζονται, υποχαρακτηρίζονται ή χάνουν τη σήμανση ασφάλειας όταν η προστασία τους δεν είναι πλέον αναγκαία ή δεν χρειάζεται να είναι πλέον στο ίδιο επίπεδο.

72. Αποφάσεις για υποχαρακτηρισμό, αποχαρακτηρισμό ή αφαίρεση σήμανσης πληροφοριών που περιέχονται σε έγγραφα τα οποία έχουν δημιουργηθεί στο Κοινοβούλιο λαμβάνονται και σε μεμονωμένη βάση, για παράδειγμα ως απόκριση σε αίτημα για πρόσβαση που υποβάλλεται από το κοινό ή από άλλο θεσμικό όργανο της Ένωσης, ή με πρωτοβουλία της CIU ή κοινοβουλευτικού οργάνου/αξιωματούχου.

73. Κατά τη δημιουργία ΔΠΕΕ, ο αρχικός συντάκτες υποδεικνύει, εφόσον είναι δυνατόν, αν η συγκεκριμένη ΔΠΠΕ μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί σε συγκεκριμένη ημερομηνία ή έπειτα από συγκεκριμένο γεγονός. Αν δεν είναι πρακτικά εφικτή η συγκεκριμένη υπόδειξη, ο αρχικός συντάκτης, η CIU ή το κοινοβουλευτικό όργανο/αξιωματούχος που έχει στην κατοχή του την πληροφορία επανεξετάζει το επίπεδο διαβάθμισης της ΔΠΕΕ τουλάχιστον ανά πενταετία. Σε κάθε περίπτωση, η ΔΠΕΕ μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί μόνο με την προηγούμενη γραπτή συγκατάθεση του αρχικού συντάκτη.

74. Αν δεν είναι δυνατός ο προσδιορισμός ή ο εντοπισμός του αρχικού συντάκτη εγγράφου των ΔΠΕΕ που δημιουργήθηκε στο Κοινοβούλιο, η Αρχή Ασφάλειας επανεξετάζει το επίπεδο διαβάθμισης των σχετικών ΔΠΕΕ με βάση πρόταση του κοινοβουλευτικού οργάνου/αξιωματούχου που έχει στην κατοχή του την πληροφορία, που για τον σκοπό αυτό μπορεί να συμβουλευτεί την CIU.

75. Η CIU ή το κοινοβουλευτικό όργανο/αξιωματούχος που έχει στην κατοχή του την πληροφορία έχει την ευθύνη της ειδοποίησης των παραληπτών σχετικά με τον αποχαρακτηρισμό ή τον υποχαρακτηρισμό των πληροφοριών, οι δε παραλήπτες έχουν από την πλευρά τους την ευθύνη για την ειδοποίηση επόμενων παραληπτών στους οποίους έχουν διαβιβάσει το έγγραφο ή αντίγραφά του.

76. Ο αποχαρακτηρισμός, ο υποχαρακτηρισμός ή η αφαίρεση της σήμανσης των πληροφοριών που περιέχονται σε ένα έγγραφο καταγράφονται.

IA.2. ***Αποχαρακτηρισμός***

77. Οι ΔΠΕΕ μπορούν να αποχαρακτηρίζονται πλήρως ή εν μέρει. Οι ΔΠΕΕ μπορούν να αποχαρακτηρίζονται εν μέρει, όταν η προστασία τους δεν κρίνεται πλέον αναγκαία για ένα συγκεκριμένο μέρος του εγγράφου που τις περιέχει αλλά εξακολουθεί να δικαιολογείται για το υπόλοιπο έγγραφο.

78. Όταν η επανεξέταση ΔΠΕΕ που περιέχονται σε ένα έγγραφο το οποίο δημιουργήθηκε στο Κοινοβούλιο καταλήγει σε απόφαση για τον αποχαρακτηρισμό του, εξετάζεται κατά πόσο το έγγραφο μπορεί να δημοσιοποιηθεί ή αν πρέπει να φέρει σήμανση διανομής (δηλ. απαγορεύεται η δημοσίευση).

79. Όταν αποχαρακτηρίζονται ΔΠΕΕ, ο αποχαρακτηρισμός τους καταχωρείται στο βιβλίο καταγραφής μαζί με τα ακόλουθα στοιχεία: ημερομηνία αποχαρακτηρισμού, ονόματα των προσώπων που ζήτησαν τον αποχαρακτηρισμό και των προσώπων που τον επέτρεψαν, αριθμό αναφοράς του αποχαρακτηρισμένου εγγράφου και τελικό προορισμό του.

80. Οι επισημάνσεις της παλαιάς διαβάθμισης του αποχαρακτηρισμένου εγγράφου και όλων των αντιγράφων του διαγράφονται. Τα έγγραφα και όλα τα αντίγραφά τους αποθηκεύονται αντίστοιχα.

81. Μετά τον μερικό αποχαρακτηρισμό διαβαθμισμένων πληροφοριών, το μέρος που έχει αποχαρακτηριστεί θα παράγεται στη μορφή αποσπάσματος και θα αποθηκεύεται αντίστοιχα. Η αρμόδια υπηρεσία καταχωρεί:

α) την ημερομηνία του μερικού αποχαρακτηρισμού·

β) τα ονόματα των προσώπων που ζήτησαν τον αποχαρακτηρισμό και των προσώπων που τον επέτρεψαν· και

γ) τον αριθμό αναφοράς του αποχαρακτηρισμένου αποσπάσματος.

IA.3. ***Υποχαρακτηρισμός***

82. Μετά τον υποχαρακτηρισμό διαβαθμισμένων πληροφοριών, το έγγραφο που τις περιέχει θα είναι καταχωρισμένο τόσο στα βιβλία καταγραφής που αντιστοιχούν στο παλιό επίπεδο διαβάθμισης όσο και σε κείνα που αντιστοιχούν στο νέο. Καταγράφονται η ημερομηνία του υποχαρακτηρισμού καθώς και το όνομα του προσώπου που τον επέτρεψε.

83. Το έγγραφο που περιέχει τις υποχαρακτηρισμένες πληροφορίες και όλα τα αντίγραφά του διαβαθμίζονται σε νέο επίπεδο και αποθηκεύονται αντίστοιχα.

IB. **ΚΑΤΑΣΤΡΟΦΗ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

84. Οι εμπιστευτικές πληροφορίες (είτε σε χαρτί είτε σε ηλεκτρονική μορφή) που δεν χρειάζονται πλέον καταστρέφονται ή σβήνονται, σύμφωνα με τις οδηγίες χειρισμού και τους αντίστοιχους κανόνες αρχειοθέτησης.

85. Οι πληροφορίες με διαβάθμιση σε επίπεδο TRES SECRET UE/EU TOP SECRET ή SECRET UE/EU SECRET ή σε ισοδύναμό του καταστρέφονται από την CIU. Η καταστροφή τους γίνεται παρουσία προσώπου το οποίο έχει επίπεδο ελέγχου ασφάλειας που αντιστοιχεί τουλάχιστον στο επίπεδο διαβάθμισης των καταστρεφόμενων πληροφοριών.

86. Πληροφορίες με διαβάθμιση σε επίπεδο TRES SECRET UE/EU TOP SECRET ή σε ισοδύναμό του καταστρέφονται μόνο με την προηγούμενη γραπτή συγκατάθεση του αρχικού συντάκτη.

87. Η CIU καταστρέφει και εξαφανίζει πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του κατ' εντολή του αρχικού συντάκτη ή αρμόδιας αρχής. Τα βιβλία καταγραφής και άλλα μητρώα ενημερώνονται αντίστοιχα. Πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του καταστρέφονται και εξαφανίζονται είτε από την CIU είτε από το αρμόδιο κοινοβουλευτικό όργανο/αξιωματούχο.

88. Το πρόσωπο που είναι επίσημα υπεύθυνο για την καταστροφή και ο μάρτυρας για την καταστροφή υπογράφουν πιστοποιητικό καταστροφής, το οποίο καταχωρείται και αρχειοθετείται στην CIU. Η CIU διατηρεί, μαζί με τα έντυπα καταστροφής, τα πιστοποιητικά καταστροφής πληροφοριών με διαβάθμιση σε επίπεδο TRES SECRET UE/EU TOP SECRET ή σε ισοδύναμό του, για διάστημα τουλάχιστον δέκα ετών, και σε περίπτωση πληροφοριών με διαβάθμιση σε επίπεδο SECRET UE/EU SECRET ή σε ισοδύναμό του και CONFIDENTIEL UE/EU CONFIDENTIAL ή σε ισοδύναμό του για διάστημα τουλάχιστον πέντε ετών.

89. Έγγραφα που περιέχουν διαβαθμισμένες πληροφορίες καταστρέφονται με μεθόδους που ανταποκρίνονται στα σχετικά πρότυπα της Ένωσης ή σε ισοδύναμα πρότυπα, προκειμένου να μην είναι δυνατή η πλήρης ή μερική ανασύνθεσή τους.

90. Η καταστροφή μέσων αποθήκευσης σε υπολογιστή που χρησιμοποιούνται για διαβαθμισμένες πληροφορίες γίνεται σύμφωνα με τις σχετικές οδηγίες χειρισμού.

91. Η καταστροφή διαβαθμισμένων πληροφοριών καταχωρείται στο σχετικό βιβλίο καταγραφής με τα ακόλουθα στοιχεία:

α) ημερομηνία και ώρα της καταστροφής·

β) όνομα του υπαλλήλου που ήταν υπεύθυνος για την καταστροφή·

γ) προσδιορισμός του εγγράφου ή των αντιτύπων που καταστράφηκαν·

δ) αρχική υλική μορφή των ΔΠΕΕ που καταστράφηκαν·

ε) μέσα που χρησιμοποιήθηκαν για την καταστροφή· και

στ) τόπος καταστροφής.

ΙΓ. **ΑΡΧΕΙΟΘΕΤΗΣΗ**

92. Διαβαθμισμένες πληροφορίες, συμπεριλαμβανομένων τυχόν διαβιβαστικού σημειώματος/επιστολής, των παραρτημάτων, του φακέλου κατάθεσης ή/και άλλων μερών του φακέλου, μεταφέρονται στον Ασφαλή Χώρο έξι μήνες μετά την τελευταία εξέτασή τους ή, το αργότερο, ένα έτος μετά την κατάθεσή τους. Οι λεπτομερείς κανόνες για την αρχειοθέτηση των διαβαθμισμένων πληροφοριών καθορίζονται στις οδηγίες χειρισμού.

93. Για τις «άλλες εμπιστευτικές πληροφορίες», οι γενικοί κανόνες διαχείρισης εγγράφων εφαρμόζονται με την επιφύλαξη άλλων ειδικών ρυθμίσεων σχετικά με τον χειρισμό τους.

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 3

Η ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕΣΩ ΑΥΤΟΜΑΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ (ΣΕΠ)

Α. **ΔΙΑΣΦΑΛΙΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΔΙΑΚΙΝΟΥΜΕΝΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΩΝ**

1. «Διασφάλιση των πληροφοριών» (ΙΑ) στον τομέα των συστημάτων πληροφοριών είναι η βεβαιότητα ότι τα συστήματα αυτά θα προστατεύουν τις διαβαθμισμένες πληροφορίες που χειρίζονται και θα λειτουργούν οσοδήποτε και οποτεδήποτε χρειάζεται υπό τον έλεγχο των νομίμων χρηστών. Η αποτελεσματική ΙΑ εξασφαλίζει κατάλληλα επίπεδα εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας, μη άρνησης αναγνώρισης των πληροφοριών και γνησιότητας. Η ΙΑ βασίζεται σε διαδικασία διαχείρισης κινδύνων.

2. Ως «σύστημα επικοινωνίας και πληροφοριών» (ΣΕΠ) για τον χειρισμό διαβαθμισμένων πληροφοριών νοείται σύστημα που επιτρέπει τον χειρισμό πληροφοριών σε ηλεκτρονική μορφή. Ένα τέτοιο σύστημα πληροφοριών περιλαμβάνει το σύνολο των στοιχείων που απαιτούνται για τη λειτουργία του, συμπεριλαμβανομένων της υποδομής, της οργάνωσης, του προσωπικού και των πληροφοριών.

3. Τα ΣΕΠ χειρίζονται τις διαβαθμισμένες πληροφορίες σύμφωνα με την έννοια της ΙΑ.

4. Τα ΣΕΠ υποβάλλονται σε διαδικασία έγκρισης της λειτουργίας. Η έγκριση λειτουργίας αποσκοπεί στη βεβαίωση ότι έχουν εφαρμοσθεί όλα τα ενδεδειγμένα μέτρα ασφαλείας και ότι έχει επιτευχθεί ικανοποιητικό επίπεδο προστασίας των διαβαθμισμένων πληροφοριών και του ΣΕΠ, σύμφωνα με την παρούσα κοινοποίηση ασφαλείας. Η δήλωση έγκρισης λειτουργίας καθορίζει το μέγιστο επιτρεπτό επίπεδο διαβάθμισης των πληροφοριών που μπορεί να χειρισθεί το ΣΕΠ, καθώς και τους αντίστοιχους όρους και προϋποθέσεις.

5. Οι ακόλουθες ιδιότητες και έννοιες ΙΑ είναι ουσιαστικές για την ασφάλεια και την ορθή εφαρμογή δράσεων στο πλαίσιο συστημάτων ΣΕΠ:

α) γνησιότητα: η εγγύηση ότι οι πληροφορίες είναι γνήσιες και ότι προέρχονται από καλόπιστες πηγές

β) διαθεσιμότητα: η ιδιότητα του συστήματος να είναι διαθέσιμο και έτοιμο προς χρήση κατόπιν αιτήματος εξουσιοδοτημένου φορέα

γ) εμπιστευτικότητα: η ιδιότητα της μη κοινολόγησης πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα, φορείς ή διαδικασίες

δ) ακεραιότητα: η ιδιότητα της διαφύλαξης της ακρίβειας και της πληρότητας των πληροφοριών και των στοιχείων

ε) μη άρνηση αναγνώρισης: η ικανότητα απόδειξης της διεξαγωγής ενέργειας ή γεγονότος, ούτως ώστε να μην είναι δυνατή η άρνηση της εν λόγω ενέργειας ή του γεγονότος.

Β. **ΑΡΧΕΣ ΤΗΣ ΔΙΑΣΦΑΛΙΣΗΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

6. Οι κατωτέρω διατάξεις αποτελούν τη βάση για την ασφάλεια όλων των ΣΕΠ που χειρίζονται διαβαθμισμένες πληροφορίες. Λεπτομερείς απαιτήσεις για την εφαρμογή των διατάξεων αυτών θα καθορισθούν σε πολιτικές ασφαλείας ΙΑ και κατευθυντήριες γραμμές ασφαλείας.

Β.1. ***Διαχείριση των κινδύνων κατά της ασφάλειας***

7. Η διαχείριση κινδύνων κατά της ασφαλείας αποτελεί αναπόσπαστο μέρος του σχεδιασμού, της ανάπτυξης, της λειτουργίας και της συντήρησης των ΣΕΠ. Η διαχείριση του κινδύνου (αξιολόγηση, χειρισμός, αποδοχή και κοινοποίηση) διεξάγεται ως επαναληπτική διαδικασία, από κοινού από τους εκπροσώπους των ιδιοκτητών των συστημάτων, τις αρχές των προγραμμάτων, τις επιχειρησιακές αρχές και τις αρχές έγκρισης ασφαλείας, όπως ορίζεται στην κοινοποίηση ασφαλείας 1, με χρήση δοκιμασμένης, διαφανούς και πλήρως κατανοητής διαδικασίας αξιολόγησης του κινδύνου. Το πεδίο εφαρμογής των ΣΕΠ και τα στοιχεία τους ορίζονται με σαφήνεια στην αρχή της διαδικασίας διαχείρισης του κινδύνου.

8. Οι αρμόδιες αρχές, όπως ορίζονται στην κοινοποίηση ασφαλείας 1, εξετάζουν τις εν δυνάμει απειλές που αντιμετωπίζουν τα ΣΕΠ και διατηρούν ενημερωμένες και ακριβείς αξιολογήσεις κινδύνου που αντιστοιχούν στο τρέχον επιχειρησιακό περιβάλλον. Ενημερώνουν διαρκώς τις γνώσεις τους ως προς τα ζητήματα τρωτότητας και επανεξετάζουν περιοδικά την αξιολόγηση τρωτότητας προκειμένου να ανταποκρίνονται στο εξελισσόμενο περιβάλλον της τεχνολογίας των πληροφοριών (ΤΠ).

9. Ο χειρισμός των κινδύνων για την ασφάλεια αποσκοπεί στην εφαρμογή δέσμης μέτρων ασφαλείας που αποτελούν μια ικανοποιητική ισορροπία μεταξύ των απαιτήσεων των χρηστών, του κόστους και του υπολειπόμενου κινδύνου για την ασφάλεια.

10. Η έγκριση λειτουργίας ενός ΣΕΠ περιλαμβάνει τυπική δήλωση υπολειπόμενου κινδύνου και την αποδοχή του υπολειπόμενου κινδύνου από υπεύθυνη αρχή. Οι ειδικές προδιαγραφές, η κλίμακα και ο βαθμός των λεπτομερειών που καθορίζονται από την αρμόδια SAA για την έγκριση της λειτουργίας ενός ΣΕΠ είναι αναλογικές προς τον αξιολογούμενο κίνδυνο, λαμβάνουν δε υπόψη όλους τους συναφείς παράγοντες και μεταξύ άλλων το επίπεδο διαβάθμισης των διαβαθμισμένων πληροφοριών που τυγχάνουν χειρισμού σε ΣΕΠ.

Β.2. ***Ασφάλεια καθ' όλη τη διάρκεια του κύκλου ζωής του ΣΕΠ***

11. Η εγγύηση της ασφάλειας αποτελεί απαίτηση σε όλη τη διάρκεια του κύκλου ζωής του ΣΕΠ από τον σχεδιασμό έως την απόσυρση από την υπηρεσία.

12. Ο ρόλος και η συμβολή κάθε συμμετέχοντος σε ΣΕΠ φορέα ως προς την ασφάλεια του συστήματος προσδιορίζεται σε κάθε φάση του κύκλου ζωής.

13. Τα ΣΕΠ, συμπεριλαμβανομένων των τεχνικών και μη τεχνικών μέτρων ασφαλείας, υποβάλλονται σε δοκιμές ασφαλείας κατά τη διάρκεια της διαδικασίας έγκρισης προκειμένου να εξασφαλίζεται ότι έχει επιτευχθεί το κατάλληλο επίπεδο ασφαλείας και να επαληθεύεται ότι τα ΣΕΠ, συμπεριλαμβανομένων των τεχνικών και μη τεχνικών μέτρων ασφαλείας, έχουν ορθώς εφαρμοσθεί, ολοκληρωθεί και διαμορφωθεί.

14. Αξιολογήσεις ασφαλείας, επιθεωρήσεις και έλεγχοι διεξάγονται κατά τακτά διαστήματα στη διάρκεια της λειτουργίας και της συντήρησης του ΣΕΠ καθώς και όταν προκύπτουν έκτακτες καταστάσεις.

15. Η τεκμηρίωση ασφαλείας ενός ΣΕΠ εξελίσσεται κατά τη διάρκεια του κύκλου ζωής του ως αναπόσπαστο μέρος της διαδικασίας διαχείρισης της αλλαγής.

16. Οι διαδικασίες καταχώρισης που εκτελεί ένα ΣΕΠ, εφόσον απαιτείται, επαληθεύονται ως μέρος της διαδικασίας έγκρισης.

Β.3. ***Βέλτιστη πρακτική***

17. Η αρχή ΙΑ αναπτύσσει τη βέλτιστη πρακτική για την προστασία των διαβαθμισμένων πληροφοριών τις οποίες χειρίζονται τα ΣΕΠ. Οι κατευθυντήριες γραμμές βέλτιστων πρακτικών περιλαμβάνουν κατάλογο μέτρων τεχνικής, υλικής, οργανωτικής και διαδικαστικής ασφαλείας για ΣΕΠ των οποίων έχει αποδειχθεί η αποτελεσματικότητα στην αντιμετώπιση δεδομένων απειλών και τρωτών σημείων.

18. Η προστασία των διαβαθμισμένων πληροφοριών τις οποίες χειρίζονται τα ΣΕΠ επωφελείται από τα διδάγματα που έχουν αποκομίσει οι αρχές που συμμετέχουν σε ΙΑ.

19. Η διάδοση και επακόλουθη εφαρμογή βέλτιστων πρακτικών βοηθούν στην επίτευξη ισοδύναμου επιπέδου διασφάλισης για τα ΣΕΠ που χρησιμοποιούνται από τη Γραμματεία του Κοινοβουλίου και τα οποία χειρίζονται διαβαθμισμένες πληροφορίες.

Β.4. ***Ασφάλεια εις βάθος***

20. Για τον περιορισμό του κινδύνου που αντιμετωπίζουν τα ΣΕΠ, εφαρμόζεται σειρά τεχνικών και μη τεχνικών μέτρων ασφαλείας, τα οποία οργανώνονται ως πολλαπλά επίπεδα άμυνας. Τα επίπεδα αυτά περιλαμβάνουν τα εξής:

α) αποτροπή: μέτρα ασφαλείας που αποσκοπούν στην αποτροπή οποιουδήποτε αντίπαλου σχεδιασμού για επίθεση σε ΣΕΠ,

β) πρόληψη: μέτρα ασφαλείας που αποσκοπούν στην παρεμπόδιση ή στην ανάσχεση επίθεσης σε ΣΕΠ,

γ) ανίχνευση: μέτρα ασφαλείας που αποσκοπούν στον εντοπισμό της εμφάνισης επίθεσης σε ΣΕΠ,

δ) ανθεκτικότητα: μέτρα ασφαλείας που αποσκοπούν στον περιορισμό των συνεπειών της επίθεσης σε ελάχιστο σύνολο πληροφοριών ή στοιχείων ΣΕΠ και στην πρόληψη περαιτέρω ζημιών, και

ε) ανάκτηση: μέτρα ασφαλείας που αποσκοπούν στην αποκατάσταση της ασφάλειας του ΣΕΠ.

Ο βαθμός αυστηρότητας των εν λόγω μέτρων ασφαλείας καθορίζεται από την αξιολόγηση κινδύνου.

21. Οι αρμόδιες αρχές, όπως καθορίζονται στην κοινοποίηση ασφαλείας 1, διασφαλίζουν ότι μπορούν να αντιμετωπίζουν συμβάντα που ενδέχεται να υπερβαίνουν τα όρια οργανισμών για τον συντονισμό των αντιδράσεων και την ανταλλαγή πληροφοριών ως προς τα συμβάντα αυτά και τον συναφή κίνδυνο (ικανότητες αντιμετώπισης έκτακτων αναγκών στην πληροφορική).

Β.5. ***Αρχή των μινιμαλιστικών και ελάχιστων προνομίων***

22. Προκειμένου να αποφεύγονται περιττοί κίνδυνοι, θα χρησιμοποιούνται μόνο οι βασικές λειτουργίες, συσκευές και υπηρεσίες για την κάλυψη των λειτουργικών απαιτήσεων.

23. Στους χρήστες ΣΕΠ και στις αυτοματοποιημένες διαδικασίες θα παρέχονται μόνο οι απαραίτητες δυνατότητες πρόσβασης, προνόμια ή εξουσιοδοτήσεις για την εκτέλεση των καθηκόντων τους προκειμένου να περιορίζονται τυχόν βλάβες λόγω ατυχήματος, σφάλματος ή μη εξουσιοδοτημένης χρήσης των πόρων των ΣΕΠ.

Β.6. ***Ευαισθητοποίηση ως προς τη διασφάλιση πληροφοριών***

24. Η ευαισθητοποίηση ως προς τους κινδύνους και τα διαθέσιμα μέτρα ασφαλείας αποτελεί την πρώτη γραμμή άμυνας για την ασφάλεια των ΣΕΠ. Ειδικότερα, το σύνολο του προσωπικού που συμμετέχει στον κύκλο ζωής του ΣΕΠ, περιλαμβανομένων και των χρηστών, κατανοεί:

α) ότι οι διαρροές ασφαλείας μπορούν να βλάψουν σημαντικά το ΣΕΠ που χειρίζεται τις διαβαθμισμένες πληροφορίες·

β) τις ενδεχόμενες βλάβες σε τρίτους που μπορεί να προκύψουν από τη διασυνδεσιμότητα και την αλληλεξάρτηση, και

γ) την ατομική ευθύνη και την υποχρέωση λογοδοσίας τους ως προς την ασφάλεια των ΣΕΠ ανάλογα με τον δικό τους ρόλο στο πλαίσιο των συστημάτων και διαδικασιών.

25. Για να διασφαλισθεί ότι γίνονται αντιληπτές οι ευθύνες ως προς την ασφάλεια, η εκπαίδευση και η ευαισθητοποίηση σε θέματα ΙΑ είναι υποχρεωτική για όλα τα μέλη του προσωπικού, συμπεριλαμβανομένων των ανώτερων στελεχών, των βουλευτών του Ευρωπαϊκού Κοινοβουλίου και των χρηστών ΣΕΠ.

Β.7. ***Αξιολόγηση και έγκριση προϊόντων ασφαλείας ΤΠ***

26. Τα ΣΕΠ που χειρίζονται πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του προστατεύονται κατά τρόπον ώστε οι διαβαθμισμένες πληροφορίες να μην μπορούν να διαρρεύσουν μέσω ακούσιων ηλεκτρομαγνητικών εκπομπών («μέτρα ασφαλείας TEMPEST»).

27. Όταν η προστασία των διαβαθμισμένων πληροφοριών παρέχεται με κρυπτογραφικά προϊόντα, τα προϊόντα αυτά πιστοποιούνται από την SAA ως μέρος των εγκεκριμένων σε επίπεδο ΕΕ κρυπτογραφικών προϊόντων.

28. Κατά τη μετάδοση διαβαθμισμένων πληροφοριών με ηλεκτρονικά μέσα χρησιμοποιούνται εγκεκριμένα σε επίπεδο ΕΕ κρυπτογραφικά προϊόντα. Παρά την απαίτηση αυτή, μπορούν να χρησιμοποιούνται ειδικές διαδικασίες ή ειδικές τεχνικές διαμορφώσεις σε καταστάσεις έκτακτης ανάγκης όπως ορίζονται στα σημεία 41 έως 44.

29. Ο απαιτούμενος βαθμός εμπιστοσύνης στα μέτρα ασφαλείας, οριζόμενος ως επίπεδο διασφάλισης, καθορίζεται ανάλογα με την έκβαση της διαδικασίας διαχείρισης κινδύνων και σύμφωνα με τις οικείες πολιτικές και κατευθυντήριες γραμμές ασφαλείας.

30. Το επίπεδο διασφάλισης επαληθεύεται με τη χρήση διεθνώς αναγνωρισμένων ή εθνικά εγκεκριμένων διαδικασιών και μεθόδων. Πρόκειται κυρίως για τη διενέργεια αξιολογήσεων και διεξαγωγή ελέγχων.

31. Η SAA εγκρίνει κατευθυντήριες γραμμές ασφαλείας για την αποδοχή και έγκριση μη κρυπτογραφικών προϊόντων ασφαλείας ΤΠ.

Β.8. ***Διαβίβαση εντός του ασφαλούς χώρου***

32. Όταν η διαβίβαση διαβαθμισμένων πληροφοριών περιορίζεται εντός του ασφαλούς χώρου, μπορεί να χρησιμοποιηθεί μη κρυπτογραφημένη διανομή ή κρυπτογράφηση χαμηλότερου επιπέδου βάσει του αποτελέσματος της διαδικασίας διαχείρισης κινδύνων και εφόσον χορηγηθεί έγκριση από την SAA.

B.9. ***Ασφαλής διασύνδεση ΣΕΠ***

33. Ως διασύνδεση νοείται η άμεση σύνδεση μονής ή πολλαπλής κατεύθυνσης δύο ή περισσότερων συστημάτων ΤΠ για την ανταλλαγή δεδομένων και άλλων πληροφοριών.

34. Ένα ΣΕΠ αντιμετωπίζει οποιοδήποτε διασυνδεδεμένο σύστημα ΤΠ ως μη έμπιστο και να εφαρμόζει μέτρα προστασίας για τον έλεγχο της ανταλλαγής διαβαθμισμένων πληροφοριών με οποιοδήποτε άλλο ΣΕΠ.

35. Για όλες τις διασυνδέσεις ΣΕΠ με άλλο σύστημα ΤΠ τηρούνται οι ακόλουθες βασικές απαιτήσεις:

α) οι αρμόδιες αρχές αναφέρουν και εγκρίνουν τις επαγγελματικές ή λειτουργικές απαιτήσεις για τις διασυνδέσεις αυτές·

β) η διασύνδεση υποβάλλεται σε διαδικασία διαχείρισης κινδύνου και έγκρισης και απαιτεί την έγκριση της αρμόδιας SAA·

γ) στην περίμετρο των ΣΕΠ συστήνονται υπηρεσίες προστασίας (PS).

36. Δεν επιτρέπεται διασύνδεση μεταξύ ενός ΣΕΠ που έχει λάβει έγκριση με μη προστατευόμενο ή δημόσιο δίκτυο, εκτός εάν το ΣΕΠ έχει εγκρίνει υπηρεσίες προστασίας (PS) που έχουν εγκατασταθεί για τον σκοπό αυτό μεταξύ του ΣΕΠ και του μη προστατευόμενου ή δημόσιου δικτύου. Τα μέτρα ασφαλείας για τις διασυνδέσεις αυτές επανεξετάζονται από την αρμόδια IAA και εγκρίνονται από την αρμόδια SAA.

37. Όταν το μη προστατευόμενο ή δημόσιο δίκτυο χρησιμοποιείται αποκλειστικά ως φορέας και τα δεδομένα έχουν κρυπτογραφηθεί από κρυπτογραφικό προϊόν το οποίο έχει λάβει έγκριση σε επίπεδο ΕΕ σύμφωνα με το άρθρο 27, η σύνδεση αυτή δεν θεωρείται διασύνδεση.

38. Απαγορεύεται η άμεση ή διαδοχική σύνδεση ενός ΣΕΠ που έχει λάβει έγκριση να χειρίζεται πληροφορίες με διαβάθμιση σε επίπεδο TRES SECRET UE/EU TOP SECRET ή σε ισοδύναμό του και πληροφορίες με διαβάθμιση σε επίπεδο SECRET UE/EU SECRET ή σε ισοδύναμό του, με μη προστατευόμενο ή δημόσιο δίκτυο.

B.10. ***Ηλεκτρονικοί φορείς αποθήκευσης***

39. Οι ηλεκτρονικοί φορείς αποθήκευσης καταστρέφονται σύμφωνα με εγκεκριμένες από την αρμόδια αρχή ασφαλείας διαδικασίες.

40. Οι ηλεκτρονικοί φορείς αποθήκευσης επαναχρησιμοποιούνται, υποχαρακτηρίζονται ή αποχαρακτηρίζονται σύμφωνα με τις οδηγίες χειρισμού.

B.11. ***Καταστάσεις έκτακτης ανάγκης***

41. Οι κατωτέρω περιγραφόμενες ειδικές διαδικασίες μπορούν να εφαρμόζονται σε περιπτώσεις έκτακτης ανάγκης, όπως καταστάσεις επικείμενης ή πραγματικής κρίσης, σύγκρουσης ή πολέμου ή υπό εξαιρετικές επιχειρησιακές περιστάσεις.

42. Οι διαβαθμισμένες πληροφορίες μπορούν να διαβιβάζονται με τη συγκατάθεση της αρμόδιας αρχής, με τη χρήση κρυπτογραφικών προϊόντων που έχουν λάβει έγκριση για χαμηλότερο επίπεδο διαβάθμισης ή χωρίς κρυπτογράφηση, εάν οποιαδήποτε καθυστέρηση θα ήταν ικανή να προξενήσει ζημιά σαφώς μεγαλύτερη από τη ζημιά που θα προκαλούσε η τυχόν κοινολόγηση του διαβαθμισμένου υλικού και εφόσον:

α) ο αποστολέας και ο παραλήπτης δεν διαθέτουν αντιστοίχως τους απαιτούμενους κρυπτογραφικούς χώρους ή καθόλου κρυπτογραφικούς χώρους, και

β) δεν υπάρχει άλλος τρόπος έγκαιρης μετάδοσης του διαβαθμισμένου υλικού.

43. Οι διαβαθμισμένες πληροφορίες που διαβιβάζονται υπό τις περιστάσεις που περιγράφονται στην παράγραφο 41 δεν φέρουν σημάνσεις ή ενδείξεις που τις διακρίνουν από μη διαβαθμισμένες πληροφορίες ή από πληροφορίες που μπορούν να προστατευθούν με τα διαθέσιμα κρυπτογραφικά προϊόντα. Οι παραλήπτες τους ενημερώνονται αμελλητί για το επίπεδο διαβάθμισης με άλλα μέσα.

44. Σε περίπτωση εφαρμογής των παραγράφων 41 ή 42, αποστέλλεται σχετική έκθεση στην αρμόδια αρχή.

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 4

ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

Α. **ΕΙΣΑΓΩΓΗ**

Με την παρούσα κοινοποίηση ασφαλείας καθορίζονται οι αρχές ασφαλείας για τη δημιουργία ασφαλούς περιβάλλοντος για την εξασφάλιση του ορθού χειρισμού διαβαθμισμένων πληροφοριών στο Ευρωπαϊκό Κοινοβούλιο. Οι αρχές αυτές, συμπεριλαμβανομένων αυτών που αφορούν την τεχνική ασφάλεια, θα συμπληρωθούν με τις οδηγίες χειρισμού.

Β. **ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ**

1. Οι κίνδυνοι κατά των διαβαθμισμένων πληροφοριών αντιμετωπίζονται στο πλαίσιο διαδικασίας. Η διαδικασία αυτή αποσκοπεί στον προσδιορισμό των γνωστών κινδύνων κατά της ασφάλειας, τον καθορισμό μέτρων ασφαλείας για τον περιορισμό των κινδύνων αυτών σε αποδεκτό επίπεδο σύμφωνα με τις βασικές αρχές και τις ελάχιστες προδιαγραφές της παρούσας κοινοποίησης ασφαλείας και στην εφαρμογή των εν λόγω μέτρων σύμφωνα με την έννοια της ασφάλειας εις βάθος όπως ορίζεται στην κοινοποίηση ασφαλείας 3. Η αποτελεσματικότητα τέτοιων μέτρων αξιολογείται διαρκώς.

2. Τα μέτρα ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής τους είναι ανάλογα, ιδίως προς τη διαβάθμιση ασφαλείας τους, τη μορφή και τον όγκο των σχετικών πληροφοριών ή του σχετικού υλικού, την τοποθεσία και την κατασκευή των εγκαταστάσεων όπου ευρίσκονται διαβαθμισμένες πληροφορίες και την επιτόπου εκτιμώμενη απειλή δόλιων ή/και εγκληματικών δραστηριοτήτων, συμπεριλαμβανομένης της κατασκοπείας, της δολιοφθοράς και της τρομοκρατίας.

3. Τα σχέδια έκτακτης ανάγκης λαμβάνουν υπόψη την ανάγκη προστασίας των διαβαθμισμένων πληροφοριών σε καταστάσεις έκτακτης ανάγκης προκειμένου να εμποδίζονται η μη εξουσιοδοτημένη πρόσβαση, η κοινολόγηση και η απώλεια ακεραιότητας ή διαθεσιμότητας.

4. Προληπτικά και επανορθωτικά μέτρα με στόχο να ελαχιστοποιούνται οι συνέπειες σοβαρών αστοχιών ή συμβάντων κατά τον χειρισμό και την αποθήκευση διαβαθμισμένων πληροφοριών περιλαμβάνονται στα σχέδια συνέχισης των δραστηριοτήτων.

Γ. **ΓΕΝΙΚΕΣ ΑΡΧΕΣ**

5. Το επίπεδο διαβάθμισης ή σήμανσης των πληροφοριών καθορίζει το επίπεδο προστασίας τους στους τομείς της υλικής ασφάλειας.

6. Οι πληροφορίες που χρειάζονται διαβάθμιση υφίστανται σχετική σήμανση και χειρισμό, ανεξάρτητα από την υλική τους μορφή. Η διαβάθμιση κοινοποιείται σαφώς στους αποδέκτες της, είτε με σήμανση διαβάθμισης (αν δίνεται σε έγγραφη μορφή, είτε σε χαρτί είτε σε ΣΕΠ) ή με ανακοίνωση (αν δίνεται προφορικά, όπως κατά τη διάρκεια συνομιλίας ή παρουσίασης). Το διαβαθμισμένο υλικό έχει υλική σήμανση προκειμένου να διευκολύνεται η αναγνώριση της διαβάθμισης ασφαλείας του.

7. Οι διαβαθμισμένες πληροφορίες δεν διαβάζονται σε καμία περίπτωση σε δημόσιους χώρους όπου είναι εκτεθειμένες σε άτομα τα οποία δεν χρειάζεται τις γνωρίζουν, π.χ. τρένα, αεροπλάνα, καφέ, μπαρ κ.λπ. Δεν αφήνονται σε θυρίδες ασφαλείας ή δωμάτια ξενοδοχείων. Δεν εγκαταλείπονται αφύλακτες σε δημόσιους χώρους.

Δ. **ΑΡΜΟΔΙΟΤΗΤΕΣ**

8. Η CIU είναι αρμόδια για την εξασφάλιση της υλικής ασφάλειας κατά τη διαχείριση των εμπιστευτικών πληροφοριών που κατατίθενται στις ασφαλείς της εγκαταστάσεις. Η CIU είναι επίσης αρμόδια για τη διαχείριση των ασφαλών της εγκαταστάσεων.

9. Η υλική ασφάλεια κατά τη διαχείριση πληροφοριών με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλων εμπιστευτικών πληροφοριών» αποτελεί αρμοδιότητα του αντίστοιχου κοινοβουλευτικού οργάνου/αξιωματούχου.

10. Η Διεύθυνση Ασφαλείας και Αξιολόγησης Κινδύνου είναι αρμόδια για την προσωπική ασφάλεια και τον έλεγχο ασφαλείας που απαιτούνται για την εξασφάλιση του ασφαλούς χειρισμού των εμπιστευτικών πληροφοριών στο Ευρωπαϊκό Κοινοβούλιο.

11. Η DIT παρέχει συμβουλές και εξασφαλίζει ότι κάθε δημιουργούμενο ή χρησιμοποιούμενο ΣΕΠ συμμορφώνεται πλήρως με την κοινοποίηση ασφαλείας 3 και τις αντίστοιχες οδηγίες χειρισμού.

Ε. **ΑΣΦΑΛΕΙΣ ΕΓΚΑΤΑΣΤΑΣΕΙΣ**

12. Στο πλαίσιο των προτύπων τεχνικής ασφαλείας και σύμφωνα με το επίπεδο που καθορίζεται για τις διαβαθμισμένες πληροφορίες, όπως ορίζεται στο άρθρο 7, είναι δυνατή η διευθέτηση χωριστών ασφαλών εγκαταστάσεων.

13. Οι ασφαλείς εγκαταστάσεις πιστοποιούνται από την SAA και λαμβάνουν έγκριση από την SA.

ΣΤ. **ΕΞΕΤΑΣΗ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

14. Όταν πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλες εμπιστευτικές πληροφορίες» έχουν κατατεθεί στην CIU και πρέπει να εξεταστούν εκτός του ασφαλούς χώρου, η CIU διαβιβάζει αντίγραφο στην αντίστοιχη εξουσιοδοτημένη υπηρεσία, η οποία εξασφαλίζει ότι η εξέταση και ο χειρισμός των εν λόγω πληροφοριών συμμορφώνεται με το άρθρο 8 παράγραφος 2 και το άρθρο 10 της παρούσας απόφασης και τις αντίστοιχες οδηγίες χειρισμού.

15. Όταν πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλες εμπιστευτικές πληροφορίες» έχουν κατατεθεί σε κοινοβουλευτικό όργανο/αξιωματούχο εκτός της CIU, η γραμματεία του εν λόγω κοινοβουλευτικού οργάνου/αξιωματούχου εξασφαλίζει ότι η εξέταση και ο χειρισμός των εν λόγω πληροφοριών συμμορφώνεται με το άρθρο 7 παράγραφος 3, το άρθρο 8 παράγραφοι 1, 2 και 4, το άρθρο 9 παράγραφοι 3, 4 και 5, το άρθρο 10 παράγραφοι 2 έως 6, και το άρθρο 11 της παρούσας απόφασης και τις αντίστοιχες οδηγίες χειρισμού.

16. Όταν πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του πρέπει να εξεταστούν στον ασφαλή χώρο, η CIU εξασφαλίζει ότι η εξέταση και ο χειρισμός των εν λόγω πληροφοριών συμμορφώνεται με τα άρθρα 9 και 10 της παρούσας απόφασης και τις αντίστοιχες οδηγίες χειρισμού.

Ζ. **ΤΕΧΝΙΚΗ ΑΣΦΑΛΕΙΑ**

17. Τα μέτρα τεχνικής ασφαλείας αποτελούν αρμοδιότητα της SAA, η οποία καθορίζει στο πλαίσιο των αντίστοιχων οδηγιών χειρισμού τα ειδικά μέτρα τεχνικής ασφαλείας που πρέπει να εφαρμόζονται.

18. Οι ασφαλείς αίθουσες ανάγνωσης για την εξέταση πληροφοριών με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλων εμπιστευτικών πληροφοριών» συμμορφώνονται με ειδικά μέτρα τεχνικής ασφαλείας, όπως προβλέπεται στις οδηγίες χειρισμού.

19. Ο ασφαλής χώρος αποτελείται από τις παρακάτω εγκαταστάσεις:

α) αίθουσα ελέγχου πρόσβασης ασφαλείας (SAS), η οποία διευθετείται σύμφωνα με τα μέτρα τεχνικής ασφαλείας που καθορίζονται στο πλαίσιο των οδηγιών χειρισμού. Η πρόσβαση στην εγκατάσταση αυτή καταχωρείται. Η SAS ανταποκρίνεται σε υψηλά πρότυπα όσον αφορά την ταυτοποίηση των ατόμων που διαθέτουν πρόσβαση, την εγγραφή βίντεο και τον ασφαλή χώρο για την κατάθεση προσωπικών αντικειμένων τα οποία δεν επιτρέπονται στις ασφαλείς αίθουσες (τηλέφωνα, στυλογράφοι κ.λπ.)·

β) αίθουσα επικοινωνιών για τη διαβίβαση και λήψη εμπιστευτικών πληροφοριών, συμπεριλαμβανομένων διαβαθμισμένων πληροφοριών, σύμφωνα με την κοινοποίηση ασφαλείας 3 και τις αντίστοιχες οδηγίες χειρισμού·

γ) ασφαλές αρχείο, στο οποίο χρησιμοποιούνται εγκεκριμένοι και πιστοποιημένοι φωριαμοί χωριστά για τις πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL και/ή SECRET EU/EU SECRET ή σε ισοδύναμό του. Οι πληροφορίες με διαβάθμιση σε επίπεδο TRES SECRETUE/EU TOP SECRET ή σε ισοδύναμό του τοποθετούνται σε χωριστή αίθουσα, σε ειδικό πιστοποιημένο φωριαμό. Το μόνο πρόσθετο υλικό που βρίσκεται στην αίθουσα αυτή είναι το γραφείο υποστήριξης για τον χειρισμό του αρχείου από την CIU·

δ) αίθουσα καταχώρισης, η οποία διαθέτει τα απαραίτητα εργαλεία για την πραγματοποίηση της καταχώρισης σε χαρτί ή ηλεκτρονικά, και παράλληλα είναι εξοπλισμένη με τις απαραίτητες ασφαλείς εγκαταστάσεις για την εγκατάσταση του κατάλληλου ΣΕΠ. Μόνο η αίθουσα καταχώρισης μπορεί να περιέχει εγκεκριμένες και διαπιστευμένες συσκευές αναπαραγωγής (για τη δημιουργία αντιγράφων σε έντυπη ή ηλεκτρονική μορφή). Οι οδηγίες χειρισμού ορίζουν τις εγκεκριμένες και διαπιστευμένες συσκευές αναπαραγωγής. Η αίθουσα καταχώρισης διαθέτει επίσης τα απαραίτητα μέσα για την αποθήκευση και τον χειρισμό του διαπιστευμένου υλικού που απαιτείται για τη σήμανση, την αντιγραφή και την αποστολή εμπιστευτικών πληροφοριών σε υλική μορφή, κατά επίπεδο διαβάθμισης. Το σύνολο του διαπιστευμένου υλικού ορίζεται από την CIU και λαμβάνει διαπίστευση από την SAA, σύμφωνα με τις συμβουλές που παρέχει η IAOA. Η αίθουσα καταχώρισης διαθέτει επίσης τη διαπιστευμένη συσκευή καταστροφής που έχει εγκριθεί για το υψηλότερο επίπεδο διαβάθμισης, όπως περιγράφεται στις οδηγίες χειρισμού. Η μετάφραση των πληροφοριών με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL EU, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του πραγματοποιείται στην αίθουσα καταχώρισης, στο κατάλληλο και διαπιστευμένο σύστημα. Η αίθουσα καταχώρισης διαθέτει χώρους εργασίας για έως δύο μεταφραστές ταυτόχρονα και για το ίδιο έγγραφο. Στην αίθουσα παρευρίσκεται ένα μέλος του προσωπικού της CIU.

ε) αίθουσα ανάγνωσης, για ατομική εξέταση διαβαθμισμένων πληροφοριών από δεόντως εξουσιοδοτημένα πρόσωπα. Η αίθουσα ανάγνωσης διαθέτει επαρκή χώρο για δύο άτομα, μεταξύ των οποίων ένα μέλος του προσωπικού της CIU, το οποίο παρευρίσκεται στην αίθουσα καθόλη τη διάρκεια κάθε εξέτασης. Το επίπεδο ασφαλείας για την αίθουσα αυτή είναι επαρκές για εξέταση διαβαθμισμένων πληροφοριών σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του. Η αίθουσα ανάγνωσης μπορεί να διαθέτει εξοπλισμό TEMPEST για την εξέταση πληροφοριών σε ηλεκτρονική μορφή, όταν είναι απαραίτητο, σύμφωνα με το επίπεδο διαβάθμισης των σχετικών πληροφοριών.

στ) αίθουσα συνεδριάσεων, η οποία διαθέτει επαρκή χώρο για έως 25 άτομα, για τη συζήτηση πληροφοριών με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET EU/EU SECRET ή σε ισοδύναμό του. Η αίθουσα συνεδριάσεων διαθέτει τις απαραίτητες τεχνικώς ασφαλείς και πιστοποιημένες εγκαταστάσεις για διερμηνεία σε έως και δύο γλώσσες. Όταν δεν χρησιμοποιείται για συνεδριάσεις, η αίθουσα συνεδριάσεων μπορεί επίσης να χρησιμοποιηθεί ως πρόσθετη αίθουσα ανάγνωσης για ατομική εξέταση. Σε εξαιρετικές περιπτώσεις, η CIU μπορεί να επιτρέψει την εξέταση διαβαθμισμένων πληροφοριών από περισσότερα από ένα εξουσιοδοτημένα πρόσωπα, εφόσον το επίπεδο ελέγχου ασφαλείας και η ανάγκη γνώσης είναι ίδια για όλα τα πρόσωπα στην αίθουσα. Δεν επιτρέπεται η εξέταση διαβαθμισμένων πληροφοριών από περισσότερα από τέσσερα πρόσωπα ταυτόχρονα. Η εκεί παρουσία υπαλλήλων της CIU είναι ενισχυμένη.

ζ) τεχνικώς ασφαλείς αίθουσες για την τοποθέτηση του συνόλου του τεχνικού εξοπλισμού που συνδέεται με την ασφάλεια ολόκληρου του ασφαλούς χώρου, και των ασφαλών διακομιστών ΤΠ.

20. Ο ασφαλής χώρος συμμορφώνεται με τα διεθνή πρότυπα ασφαλείας που έχουν εφαρμογή και πιστοποιείται από τη Διεύθυνση Ασφαλείας και Αξιολόγησης Κινδύνου. Ο ασφαλής χώρος περιέχει τον παρακάτω ελάχιστο εξοπλισμό τεχνικής ασφαλείας:

α) συστήματα συναγερμού και παρακολούθησης·

β) εξοπλισμό ασφαλείας και συστήματα έκτακτης ανάγκης (αμφίδρομο σύστημα προειδοποίησης)·

γ) σύστημα CCTV·

δ) σύστημα ανίχνευσης εισβολών·

ε) έλεγχο πρόσβασης (συμπεριλαμβανομένου βιομετρικού συστήματος ασφαλείας)·

στ) φωριαμούς·

ζ) ερμάρια·

η) διατάξεις ηλεκτρομαγνητικής προστασίας.

21. Όταν είναι απαραίτητα τυχόν πρόσθετα μέτρα τεχνικής ασφαλείας, η SAA μπορεί να τα λάβει ενεργώντας σε στενή συνεργασία με την CIU και ακολουθώντας την έγκριση της SA.

22. Ο εξοπλισμός υποδομής μπορεί να συνδέεται με τα συστήματα γενικής διαχείρισης του κτιρίου στο οποίο βρίσκεται ο ασφαλής χώρος. Ωστόσο, ο εξοπλισμός ασφαλείας που προορίζεται για τον έλεγχο πρόσβασης και για το ΣΕΠ είναι ανεξάρτητος από οποιαδήποτε άλλα υφιστάμενα συστήματα στο Ευρωπαϊκό Κοινοβούλιο.

Η. **ΕΠΙΘΕΩΡΗΣΕΙΣ ΤΟΥ ΑΣΦΑΛΟΥΣ ΧΩΡΟΥ**

23. Οι επιθεωρήσεις του ασφαλούς χώρου διενεργούνται τακτικά από την SAA και κατόπιν αιτήματος της CIU.

24. Η SAA καταρτίζει και επικαιροποιεί τη λίστα ελέγχου της επιθεώρησης ασφαλείας, στην οποία περιλαμβάνονται τα στοιχεία που πρέπει να ελέγχονται κατά τη διάρκεια των επιθεωρήσεων σύμφωνα με τις οδηγίες χειρισμού.

Θ. **ΜΕΤΑΦΟΡΑ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

25. Κατά τη μεταφορά τους. οι εμπιστευτικές πληροφορίες είναι κατάλληλα καλυμμένες, χωρίς ένδειξη του εμπιστευτικού χαρακτήρα του περιεχομένου, σύμφωνα με τις οδηγίες χειρισμού.

26. Μόνο κλητήρες ή προσωπικό με κατάλληλο επίπεδο άδειας ασφαλείας μπορεί να μεταφέρει πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του.

27. Οι εμπιστευτικές πληροφορίες μπορούν να αποστέλλονται με χρήση εξωτερικής αλληλογραφίας ή με ιδιόχειρη μεταφορά εκτός κτιρίου μόνο σύμφωνα με τις προϋποθέσεις που ορίζονται στις οδηγίες χειρισμού.

28. Οι πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του δεν αποστέλλονται ποτέ μέσω ηλεκτρονικού ταχυδρομείου ή φαξ, ακόμη και αν έχει εγκατασταθεί «ασφαλές» σύστημα ηλεκτρονικού ταχυδρομείου ή κρυπτογραφικό φαξ. Οι πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλες εμπιστευτικές πληροφορίες» μπορούν να αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου, με τη χρήση διαπιστευμένου κρυπτογραφικού συστήματος.

Ι. **ΑΠΟΘΗΚΕΥΣΗ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

29. Το επίπεδο διαβάθμισης ή σήμανσης των εμπιστευτικών πληροφοριών καθορίζει το επίπεδο προστασίας τους όσον αφορά την αποθήκευση. Αποθηκεύονται στον αντίστοιχα πιστοποιημένο εξοπλισμό σύμφωνα με τις οδηγίες χειρισμού.

30. Οι πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμο του και οι «άλλες εμπιστευτικές πληροφορίες»:

α) αποθηκεύονται σε τυπικό, ατσάλινο ερμάριο με κλειδαριά, εντός γραφείου ή χώρου εργασίας, όταν δεν χρησιμοποιούνται·

β) δεν εγκαταλείπονται αφύλακτες, παρά μόνον αν έχουν κλειδωθεί και αποθηκευτεί κατάλληλα·

γ) δεν αφήνονται πάνω σε γραφείο, τραπέζι κ.λπ. με τρόπο ώστε οποιοδήποτε μη εξουσιοδοτημένο άτομο, π.χ. επισκέπτες, προσωπικό καθαρισμού, προσωπικό συντήρησης κ.λπ. να είναι σε θέση να τις διαβάσει ή να τις αφαιρέσει·

δ) δεν επιδεικνύονται, ούτε αποτελούν αντικείμενο συζήτησης με οποιοδήποτε μη εξουσιοδοτημένο άτομο.

31. Οι πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED ή σε ισοδύναμό του και «άλλες εμπιστευτικές πληροφορίες» αποθηκεύονται μόνο στη γραμματεία του κοινοβουλευτικού οργάνου/αξιωματούχου, ή στην CIU σύμφωνα με τις οδηγίες χειρισμού.

32. Οι πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET ή σε ισοδύναμό του:

α) αποθηκεύονται στον ασφαλή χώρο, σε φωριαμό ασφαλείας ή σε θωρακισμένη αίθουσα. Κατ' εξαίρεση, για παράδειγμα αν η CIU είναι κλειστή, μπορούν να αποθηκευτούν σε εγκεκριμένη και πιστοποιημένη θυρίδα ασφαλείας εντός των υπηρεσιών ασφαλείας·

β) δεν εγκαταλείπονται σε καμία περίπτωση αφύλακτες εντός του ασφαλούς χώρου, χωρίς να κλειδωθούν πρώτα σε εγκεκριμένο χρηματοκιβώτιο (ακόμη και σε περιπτώσεις σύντομης απουσίας)·

γ) δεν αφήνονται πάνω σε γραφείο, τραπέζι κ.λπ. με τρόπο ώστε οποιοδήποτε μη εξουσιοδοτημένο πρόσωπο να είναι σε θέση να τις διαβάσει ή να τις αφαιρέσει, ακόμη και αν το υπεύθυνο μέλος του προσωπικού της CIU παραμείνει στην αίθουσα.

Όταν ένα έγγραφο που περιέχει διαβαθμισμένες πληροφορίες δημιουργείται σε ηλεκτρονική μορφή στον ασφαλή χώρο, ο υπολογιστής κλειδώνεται και η οθόνη καθίσταται μη προσβάσιμη, εάν ο συντάκτης του εγγράφου ή το υπεύθυνο μέλος του προσωπικού της CIU εγκαταλείψει την αίθουσα (ακόμη και σε περιπτώσεις σύντομης απουσίας). Η αυτόματη ενεργοποίηση κλειδώματος ασφαλείας μετά από μερικά λεπτά δεν θεωρείται επαρκές μέτρο.

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 5

ΒΙΟΜΗΧΑΝΙΚΗ ΑΣΦΑΛΕΙΑ

Α. **ΕΙΣΑΓΩΓΗ**

1. Η παρούσα κοινοποίηση ασφαλείας αφορά μόνο τις διαβαθμισμένες πληροφορίες.

2. Καθορίζει διατάξεις για την εφαρμογή των κοινών ελάχιστων προτύπων του παραρτήματος I μέρος 1 της παρούσας απόφασης.

3. Ως «βιομηχανική ασφάλεια» νοείται η εφαρμογή μέτρων διασφάλισης της προστασίας των διαβαθμισμένων πληροφοριών από τους εργολάβους ή τους υπεργολάβους κατά τις διαπραγματεύσεις πριν από την ανάθεση της σύμβασης και καθ' όλη τη διάρκεια του κύκλου ζωής των διαβαθμισμένων συμβάσεων. Οι συμβάσεις αυτές δεν περιλαμβάνουν πρόσβαση σε πληροφορίες με διαβάθμιση σε επίπεδο TRÈS SECRET UE/EU TOP SECRET.

4. Κατά την ανάθεση διαβαθμισμένων συμβάσεων σε βιομηχανικούς ή άλλους φορείς, το Ευρωπαϊκό Κοινοβούλιο διασφαλίζει, ως αναθέτουσα αρχή, ότι τηρούνται οι ελάχιστες προδιαγραφές βιομηχανικής ασφάλειας που καθορίζονται στην παρούσα απόφαση και αναφέρονται στη σύμβαση.

Β. **ΣΤΟΙΧΕΙΑ ΑΣΦΑΛΕΙΑΣ ΣΕ ΔΙΑΒΑΘΜΙΣΜΕΝΗ ΣΥΜΒΑΣΗ**

Β.1. ***Οδηγός Διαβάθμισης Ασφαλείας (ΟΔΑ)***

5. Πριν από την έναρξη διαδικασίας πρόσκλησης υποβολής προσφορών ή τη σύναψη διαβαθμισμένης σύμβασης, το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, καθορίζει τη διαβάθμιση ασφαλείας κάθε πληροφορίας που πρέπει να παρέχεται στους υποβάλλοντες προσφορά και στους εργολάβους, καθώς και τη διαβάθμιση ασφαλείας κάθε πληροφορίας που παράγεται από τον εργολάβο. Προς τούτου, το Ευρωπαϊκό Κοινοβούλιο καταρτίζει Οδηγό Διαβάθμισης Ασφαλείας (ΟΔΑ) που θα χρησιμοποιείται για την εκτέλεση της σύμβασης.

6. Προκειμένου να καθορισθεί το επίπεδο διαβάθμισης ασφαλείας των διάφορων στοιχείων μιας διαβαθμισμένης σύμβασης, εφαρμόζονται οι ακόλουθες αρχές:

α) κατά την κατάρτιση ΟΔΑ, το Ευρωπαϊκό Κοινοβούλιο λαμβάνει υπόψη κάθε σχετικό ζήτημα ασφαλείας, συμπεριλαμβανομένης της διαβάθμισης ασφαλείας των πληροφοριών που παρέχονται και που εγκρίνονται προς χρήση για τη σύμβαση από τον αρχικό συντάκτη των πληροφοριών·

β) η συνολική διαβάθμιση ασφαλείας της σύμβασης δεν επιτρέπεται να είναι κατώτερη από το ανώτατο επίπεδο διαβάθμισης οποιουδήποτε μέρους της.

Β.2. ***Έγγραφο θεμάτων ασφαλείας (ΕΘΑ)***

7. Οι προδιαγραφές ασφαλείας της εκάστοτε σύμβασης περιγράφονται σε έγγραφο θεμάτων ασφαλείας (ΕΘΑ). Εφόσον απαιτείται, το ΕΘΑ περιλαμβάνει τον ΟΔΑ και αποτελεί αναπόσπαστο μέρος διαβαθμισμένης σύμβασης ή υπεργολαβίας.

8. Το ΕΘΑ περιέχει τις διατάξεις που προβλέπουν ότι ο εργολάβος και/ή ο υπεργολάβος οφείλει να συμμορφώνεται προς τις ελάχιστες προδιαγραφές της παρούσας απόφασης. Η μη συμμόρφωση με αυτές τις ελάχιστες προδιαγραφές μπορεί να συνιστά λόγο καταγγελίας της σύμβασης.

Β.3. ***Εντολές ασφαλείας του προγράμματος/έργου (PSI)***

9. Ανάλογα με το πεδίο εφαρμογής προγραμμάτων ή έργων που αφορούν την πρόσβαση σε ΔΠΕΕ ή τον χειρισμό ή την αποθήκευσή τους, η αρχή ανάθεσης η οποία έχει αναλάβει τη διαχείριση του σχετικού προγράμματος ή έργου μπορεί να εκπονήσει ειδικές εντολές ασφαλείας του προγράμματος/έργου (PSI).

Γ. **ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΑΣΦΑΛΕΙΑΣ ΦΟΡΕΑ (FSC)**

10. Η FSC χορηγείται από την ΕΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας κράτους μέλους και δηλώνει, βάσει των εθνικών νομοθετικών και κανονιστικών διατάξεων, ότι ένας βιομηχανικός ή άλλος φορέας μπορεί να προστατεύει στις εγκαταστάσεις του τις ΔΠΕΕ με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET ή σε ισοδύναμό του. Απόδειξη της χορήγησης FSC προσκομίζεται στο Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, προκειμένου να παρασχεθούν ΔΠΕΕ σε εργολάβο ή υπεργολάβο ή ενδεχόμενο εργολάβο ή υπεργολάβο ή να εγκριθεί η πρόσβαση των εν λόγω προσώπων σε ΔΠΕΕ.

11. Η FSC:

α) αξιολογεί την ακεραιότητα του βιομηχανικού ή άλλου φορέα·

β) αξιολογεί την κυριότητα, τον έλεγχο, ή/και τη δυνατότητα άσκησης αθέμιτης επιρροής που θα μπορούσε να θεωρηθεί ως κίνδυνος κατά της ασφάλειας·

γ) εξακριβώνει ότι ο βιομηχανικός ή άλλος φορέας έχει θεσπίσει σύστημα ασφαλείας στις εγκαταστάσεις του το οποίο καλύπτει όλα τα ενδεδειγμένα μέτρα ασφαλείας τα οποία είναι αναγκαία για την προστασία πληροφοριών ή υλικού με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET σύμφωνα με τις απαιτήσεις της παρούσας απόφασης·

δ) εξακριβώνει ότι το καθεστώς ασφαλείας του προσωπικού –διευθυντικών στελεχών, ιδιοκτητών, εργαζομένων– που πρέπει να έχουν πρόσβαση στις πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET έχει καθορισθεί σύμφωνα με τις απαιτήσεις της παρούσας απόφασης· και

ε) εξακριβώνει ότι ο βιομηχανικός ή άλλος φορέας έχει διορίσει υπάλληλο υπεύθυνο για την ασφάλεια της εγκατάστασης ο οποίος είναι υπόλογος στη διεύθυνση για την τήρηση των υποχρεώσεων ασφαλείας εντός του φορέα.

12. Οσάκις απαιτείται, το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, ενημερώνει την αρμόδια ΕΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας ότι απαιτείται FSC κατά το προσυμβατικό στάδιο ή για την εκτέλεση της σύμβασης. Απαιτείται FSC ή ΕΑΠ (PSC) κατά το προσυμβατικό στάδιο όταν πρέπει να παρασχεθούν πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET κατά τη διάρκεια της διαδικασίας υποβολής προσφορών.

13. Η αναθέτουσα αρχή δεν αναθέτει διαβαθμισμένη σύμβαση στον προτιμώμενο υποψήφιο προτού λάβει επιβεβαίωση από την ΕΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας του κράτους μέλους στο οποίο έχει την έδρα του ο εργολάβος ή υπεργολάβος ότι έχει εκδοθεί η δέουσα FSC όπου απαιτείται.

14. Κάθε αρμόδια αρχή ασφαλείας που έχει εκδώσει FSC γνωστοποιεί στο Ευρωπαϊκό Κοινοβούλιο, υπό την ιδιότητά του ως αναθέτουσας αρχής, τυχόν αλλαγές που επηρεάζουν την FSC. Σε περίπτωση υπεργολαβίας, η αρμόδια αρχή ασφαλείας ενημερώνεται αναλόγως.

15. Η ανάκληση FSC από την αρμόδια ΕΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας συνιστά επαρκή λόγο για το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, να καταγγείλει διαβαθμισμένη σύμβαση ή να αποκλείσει συμμετέχοντα από τον διαγωνισμό.

Δ. **ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΒΑΣΕΙΣ ΕΡΓΟΛΑΒΙΑΣ ΚΑΙ ΥΠΕΡΓΟΛΑΒΙΑΣ**

16. Όταν, κατά το προσυμβατικό στάδιο, παρέχονται διαβαθμισμένες πληροφορίες σε πιθανό υποψήφιο, η πρόσκληση υποβολής προσφοράς περιέχει διάταξη που να υποχρεώνει τον υποψήφιο ο οποίος τελικά δεν υποβάλλει προσφορά ή δεν επιλέγεται, να επιστρέψει όλα τα διαβαθμισμένα έγγραφα εντός συγκεκριμένου χρονικού διαστήματος.

17. Μόλις ανατεθεί διαβαθμισμένη σύμβαση εργολαβίας ή υπεργολαβίας, το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, ενημερώνει την ΕΑΑ του εργολάβου ή του υπεργολάβου ή/και οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας σχετικά με τις διατάξεις ασφαλείας της διαβαθμισμένης σύμβασης.

18. Σε περίπτωση καταγγελίας των συμβάσεων αυτών, το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή (ή/και η αρμόδια αρχή ασφαλείας, αναλόγως, σε περίπτωση υπεργολαβίας), ενημερώνει αμέσως την ΕΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας του κράτους μέλους στο οποίο έχει την έδρα του ο εργολάβος ή ο υπεργολάβος.

19. Κατά κανόνα, ο εργολάβος ή υπεργολάβος οφείλει να επιστρέψει στην αναθέτουσα αρχή, σε περίπτωση καταγγελίας της διαβαθμισμένης σύμβασης εργολαβίας ή υπεργολαβίας, τυχόν διαβαθμισμένες πληροφορίες που έχει στην κατοχή του.

20. Ειδικές διατάξεις για τη διάθεση των διαβαθμισμένων πληροφοριών κατά την εκτέλεση της σύμβασης ή κατά την καταγγελία της ορίζονται στο ΕΘΑ.

21. Όταν ο εργολάβος ή ο υπεργολάβος έχει δικαίωμα διατήρησης των διαβαθμισμένων πληροφοριών μετά τη λύση της σύμβασης, οι ελάχιστες προδιαγραφές που προβλέπονται στην παρούσα απόφαση συνεχίζουν να τηρούνται και το απόρρητο των ΔΠΕΕ προστατεύεται από τον εργολάβο ή τον υπεργολάβο.

22. Οι όροι υπό τους οποίους ο κύριος εργολάβος μπορεί να συνάπτει σύμβαση υπεργολαβίας καθορίζονται στην προσφορά και στη σύμβαση.

23. Ο εργολάβος λαμβάνει άδεια από το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, προτού αναθέσει τμήματα διαβαθμισμένης σύμβασης σε υπεργολάβους. Δεν ανατίθεται σύμβαση υπεργολαβίας σε βιομηχανικούς ή άλλους φορείς οι οποίοι έχουν την έδρα τους σε τρίτο κράτος το οποίο δεν έχει συνάψει συμφωνία ασφάλειας πληροφοριών με την Ένωση.

24. Ο εργολάβος μεριμνά ώστε όλες οι υπεργολαβικές δραστηριότητες να αναλαμβάνονται σύμφωνα με τις ελάχιστες προδιαγραφές της παρούσας απόφασης και δεν παρέχει ΔΠΕΕ σε υπεργολάβο χωρίς την προηγούμενη γραπτή συγκατάθεση της αναθέτουσας αρχής.

25. Όσον αφορά τις διαβαθμισμένες πληροφορίες τις οποίες παράγει ή χειρίζεται ο εργολάβος ή ο υπεργολάβος, τα δικαιώματα του φορέα προέλευσης ασκούνται από την αναθέτουσα αρχή.

Ε. **ΕΠΙΣΚΕΨΕΙΣ ΣΕ ΣΥΝΑΡΤΗΣΗ ΜΕ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΒΑΣΕΙΣ**

26. Όταν το Ευρωπαϊκό Κοινοβούλιο, οι εργολάβοι ή υπεργολάβοι χρειάζονται πρόσβαση σε πληροφορίες με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET στις αντίστοιχες εγκαταστάσεις τους για την εκτέλεση διαβαθμισμένης σύμβασης, διοργανώνονται επισκέψεις σε συνεργασία με τις ΕΑΑ ή κάθε άλλη οικεία αρμόδια αρχή ασφαλείας. Ωστόσο, στο πλαίσιο ειδικών σχεδίων, οι ΕΑΑ μπορούν επίσης να συμφωνούν διαδικασία απευθείας οργάνωσης των επισκέψεων.

27. Όλοι οι επισκέπτες φέρουν τη δέουσα ΕΑΠ και έχουν «ανάγκη γνώσης» προκειμένου να τους επιτραπεί πρόσβαση στις διαβαθμισμένες πληροφορίες που σχετίζονται με τη σύμβαση του Ευρωπαϊκού Κοινοβουλίου.

28. Οι επισκέπτες δικαιούνται πρόσβαση μόνο στις διαβαθμισμένες πληροφορίες που έχουν σχέση με τον σκοπό της επίσκεψης.

ΣΤ. **ΔΙΑΒΙΒΑΣΗ ΚΑΙ ΜΕΤΑΦΟΡΑ ΤΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

29. Όσον αφορά τη διαβίβαση διαβαθμισμένων πληροφοριών με ηλεκτρονικά μέσα, ισχύουν οι οικείες διατάξεις της κοινοποίησης ασφαλείας 3.

30. Όσον αφορά τη μεταφορά διαβαθμισμένων πληροφοριών, ισχύουν οι οικείες διατάξεις της κοινοποίησης ασφαλείας 4 και οι αντίστοιχες οδηγίες χειρισμού.

31. Κατά τον καθορισμό των ρυθμίσεων ασφαλείας για τη μεταφορά διαβαθμισμένου υλικού ως φορτίου, εφαρμόζονται οι ακόλουθες αρχές:

α) η ασφάλεια πρέπει να είναι εγγυημένη σε όλα τα στάδια της μεταφοράς από το αρχικό σημείο προέλευσης ως τον τελικό προορισμό·

β) ο βαθμός προστασίας κάθε αποστολής στοιχείων προσδιορίζεται με βάση την ανώτατη διαβάθμιση του υλικού που περιέχεται στην αποστολή·

γ) χορηγείται FSC στο κατάλληλο επίπεδο για τις εταιρείες που πραγματοποιούν τη μεταφορά. Στις περιπτώσεις αυτές, το προσωπικό που χειρίζεται την αποστολή στοιχείων λαμβάνει εξουσιοδότηση ασφαλείας σύμφωνα με το παράρτημα Ι·

δ) πριν από κάθε διασυνοριακή μεταφορά υλικού με διαβάθμιση σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET ή σε ισοδύναμό του, ο αποστολέας καταρτίζει σχέδιο μεταφοράς το οποίο εγκρίνεται από τον Γενικό Γραμματέα·

ε) οι μεταφορές εκτελούνται κατά το δυνατόν από γνωστό σημείο αναχώρησης σε γνωστό σημείο άφιξης και ολοκληρώνονται όσο πιο γρήγορα το επιτρέπουν οι εκάστοτε συνθήκες·

στ) τα δρομολόγια που ακολουθούνται διέρχονται εφόσον είναι εφικτό, από το έδαφος κρατών μελών.

Ζ. **ΜΕΤΑΦΟΡΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΕΡΓΟΛΑΒΟΥΣ ΠΟΥ ΒΡΙΣΚΟΝΤΑΙ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ**

32. Η μεταφορά διαβαθμισμένων πληροφοριών σε εργολάβους και υπεργολάβους που βρίσκονται σε τρίτα κράτη διεξάγεται σύμφωνα με τα μέτρα ασφαλείας που έχουν συμφωνηθεί μεταξύ του Ευρωπαϊκού Κοινοβουλίου, ως αναθέτουσας αρχής, και του οικείου τρίτου κράτους όπου έχει την έδρα του ο εργολάβος.

Η. **ΧΕΙΡΙΣΜΟΣ ΚΑΙ ΑΠΟΘΗΚΕΥΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕ ΔΙΑΒΑΘΜΙΣΗ ΣΕ ΕΠΙΠΕΔΟ RESTREINT UE/EU RESTRICTED**

33. Σε συνεργασία με την ΕΑΑ του οικείου κράτους μέλους κατά περίπτωση, το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, έχει δικαίωμα διεξαγωγής επισκέψεων στις εγκαταστάσεις των εργολάβων/υπεργολάβων βάσει συμβατικών διατάξεων προκειμένου να εξακριβώσει ότι έχουν τεθεί σε ισχύ τα οικεία μέτρα ασφαλείας για την προστασία των ΔΠΕΕ στο επίπεδο RESTREINT UE/EU RESTRICTED όπως απαιτείται στο πλαίσιο της σύμβασης.

34. Στον βαθμό που απαιτείται δυνάμει εθνικών νομοθετικών και κανονιστικών διατάξεων, το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, γνωστοποιεί στις ΕΑΑ ή σε οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας τις συμβάσεις ή τις συμβάσεις υπεργολαβίας που περιέχουν πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED.

35. Δεν απαιτείται FSC ή ΕΑΠ για τους εργολάβους ή τους υπεργολάβους και το προσωπικό τους για τις συμβάσεις που ανατίθενται από το Ευρωπαϊκό Κοινοβούλιο και οι οποίες περιέχουν πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE /EU RESTRICTED.

36. Το Ευρωπαϊκό Κοινοβούλιο, ως αναθέτουσα αρχή, εξετάζει τις απαντήσεις στις προσκλήσεις υποβολής προσφορών για τις συμβάσεις που απαιτούν πρόσβαση σε πληροφορίες με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED, παρά τις οποιεσδήποτε απαιτήσεις σχετικά με FSC ή ΕΑΠ που ενδέχεται να υπάρχουν βάσει των εθνικών νομοθετικών και κανονιστικών διατάξεων.

37. Οι όροι υπό τους οποίους ο κύριος εργολάβος μπορεί να συνάπτει σύμβαση υπεργολαβίας καθορίζονται στην προσφορά και στη σύμβαση.

38. Όταν μια σύμβαση αφορά τον χειρισμό πληροφοριών με διαβάθμιση σε επίπεδο RESTREINT UE/EU RESTRICTED σε συστήματα επικοινωνίας και πληροφοριών που διαχειρίζεται εργολάβος, το Ευρωπαϊκό Κοινοβούλιο ως αναθέτουσα αρχή μεριμνά ώστε η σύμβαση ή οι τυχόν συμβάσεις υπεργολαβίας να καθορίζουν τις απαραίτητες τεχνικές και διοικητικές προδιαγραφές όσον αφορά τη διαπίστευση των συστημάτων επικοινωνίας και πληροφοριών σε αναλογία προς τον αξιολογούμενο κίνδυνο, λαμβάνοντας υπόψη όλους τους συναφείς παράγοντες. Το πεδίο διαπίστευσης των εν λόγω συστημάτων επικοινωνίας και πληροφοριών συμφωνείται μεταξύ της αναθέτουσας αρχής και της οικείας ΕΑΑ.

ΚΟΙΝΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ 6

ΠΑΡΑΒΙΑΣΕΙΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ, ΑΠΩΛΕΙΑ Η ΔΙΑΡΡΟΗ ΕΜΠΙΣΤΕΥΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

1. Παραβίαση της ασφάλειας προκύπτει ως αποτέλεσμα πράξης ή παράλειψης η οποία μπορεί να θέσει σε κίνδυνο εμπιστευτικές πληροφορίες ή να οδηγήσει στη διαρροή αυτών.

2. Διαρροή εμπιστευτικών πληροφοριών προκύπτει όταν οι πληροφορίες αυτές έχουν καταλήξει εξ ολοκλήρου ή εν μέρει στην κατοχή μη εξουσιοδοτημένων προσώπων, δηλαδή προσώπων που είτε δεν διαθέτουν το κατάλληλο επίπεδο ελέγχου ασφαλείας είτε δεν έχουν την απαραίτητη «ανάγκη γνώσης», ή όταν θεωρείται πιθανό να έχει συμβεί κάτι τέτοιο.

3. Οι εμπιστευτικές πληροφορίες μπορούν να διαρρεύσουν ως αποτέλεσμα απροσεξίας, αμέλειας ή ακριτομυθίας, καθώς και ως συνέπεια των δραστηριοτήτων υπηρεσιών που έχουν ως στόχο την Ένωση ή ανατρεπτικών οργανώσεων.

4. Όταν ο Γενικός Γραμματέας ανακαλύπτει ή πληροφορείται αποδεδειγμένη ή εικαζόμενη παραβίαση της ασφάλειας, απώλεια ή διαρροή εμπιστευτικών πληροφοριών:

α) διαπιστώνει τα πραγματικά περιστατικά,

β) εκτιμά και ελαχιστοποιεί την επελθούσα ζημία,

γ) λαμβάνει μέτρα προκειμένου να μην επαναληφθεί το συμβάν,

δ) ενημερώνει την αρμόδια αρχή του τρίτου κράτους ή του κράτους μέλους το οποίο συνέταξε ή διαβίβασε τις εμπιστευτικές πληροφορίες.

Όταν το συμβάν αφορά βουλευτή του Ευρωπαϊκού Κοινοβουλίου, ο Γενικός Γραμματέας ενεργεί από κοινού με τον Πρόεδρο του Κοινοβουλίου.

Αν οι πληροφορίες έχουν ληφθεί από άλλα θεσμικά όργανα της Ένωσης, ο Γενικός Γραμματέας ενεργεί σύμφωνα με τα κατάλληλα μέτρα ασφαλείας για διαβαθμισμένες πληροφορίες και τις καθορισμένες ρυθμίσεις που ορίζονται στη συμφωνία-πλαίσιο με την Επιτροπή ή στη διοργανική συμφωνία με το Συμβούλιο.

5. Όλα τα πρόσωπα τα οποία απαιτείται να χειρίζονται εμπιστευτικές πληροφορίες ενημερώνονται αναλυτικά για τις ρυθμίσεις ασφαλείας, τους κινδύνους τυχόν ακριτομυθιών και τις σχέσεις τους με τον Τύπο και, κατά περίπτωση, υπογράφουν δήλωση ότι δεν θα αποκαλύψουν το περιεχόμενο εμπιστευτικών πληροφοριών σε τρίτους, ότι θα σέβονται τις υποχρεώσεις προστασίας διαβαθμισμένων πληροφοριών και ότι αναγνωρίζουν τις συνέπειες της μη εκπλήρωσης αυτών. Η πρόσβαση σε διαβαθμισμένες πληροφορίες ή η χρήση αυτών από πρόσωπο που δεν έχει ενημερωθεί και δεν έχει υπογράψει την αντίστοιχη δήλωση θεωρείται παραβίαση της ασφάλειας.

6. Οι βουλευτές του Ευρωπαϊκού Κοινοβουλίου, οι υπάλληλοι του Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες ή εργολάβους αναφέρουν αμέσως στον Γενικό Γραμματέα οποιαδήποτε παραβίαση της ασφάλειας, απώλεια ή διαρροή εμπιστευτικών πληροφοριών η οποία μπορεί να υποπέσει στην αντίληψή τους.

7. Κάθε πρόσωπο υπεύθυνο για τη διαρροή εμπιστευτικών πληροφοριών υπόκειται σε πειθαρχικές κυρώσεις σύμφωνα με τους οικείους κανόνες και κανονισμούς. Οι κυρώσεις επιβάλλονται με την επιφύλαξη τυχόν περαιτέρω δικαστικών ενεργειών, σύμφωνα με τις εφαρμοστέες διατάξεις.

8. Με την επιφύλαξη τυχόν περαιτέρω δικαστικών ενεργειών, οι παραβιάσεις που διαπράττονται από υπαλλήλους του Κοινοβουλίου και το λοιπό προσωπικό του Κοινοβουλίου που εργάζεται για τις πολιτικές ομάδες συνεπάγονται την εφαρμογή των διαδικασιών και την επιβολή των κυρώσεων που προβλέπονται από τον τίτλο VI του κανονισμού υπηρεσιακής κατάστασης.

9. Με την επιφύλαξη τυχόν περαιτέρω δικαστικών ενεργειών, οι παραβιάσεις που διαπράττονται από βουλευτές του Ευρωπαϊκού Κοινοβουλίου αντιμετωπίζονται σύμφωνα με το άρθρο 9 παράγραφος 2 και τα άρθρα 152, 153 και 154 του Κανονισμού του Ευρωπαϊκού Κοινοβουλίου.