ΑΠΟΦΑΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 4ης Μαΐου 2010

όσον αφορά το σχέδιο ασφαλείας για το κεντρικό SIS II και την επικοινωνιακή υποδομή

(2010/261/ΕΕ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη:

τη συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

τον κανονισμό (ΕΚ) αριθ. 1987/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Δεκεμβρίου 2006, σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) [1], και ιδίως το άρθρο 16,

την απόφαση 2007/533/ΔΕΥ του Συμβουλίου, της 12ης Ιουνίου 2007, σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) [2], και ιδίως το άρθρο 16,

Εκτιμώντας τα ακόλουθα:

(1) Το άρθρο 16 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 16 της απόφασης 2007/533/ΔΕΥ ορίζουν ότι η διαχειριστική αρχή και η Επιτροπή λαμβάνουν, σε σχέση με το κεντρικό SIS II και την επικοινωνιακή υποδομή αντίστοιχα, τα απαιτούμενα μέτρα, στα οποία συμπεριλαμβάνεται σχέδιο ασφαλείας.

(2) Το άρθρο 15 παράγραφος 4 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 15 παράγραφος 4 της απόφασης 2007/533/ΔΕΥ ορίζουν ότι η Επιτροπή, κατά τη μεταβατική περίοδο προτού αναλάβει τις αρμοδιότητές της η διαχειριστική αρχή, φέρει την ευθύνη για την επιχειρησιακή διαχείριση του κεντρικού SIS II.

(3) Δεδομένου ότι δεν έχει συσταθεί ακόμη διαχειριστική αρχή, το σχέδιο ασφαλείας που θα καταρτίσει η Επιτροπή θα πρέπει, κατά τη μεταβατική περίοδο, να εφαρμοσθεί και στο κεντρικό SIS II.

(4) Ο κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [3] εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από την Επιτροπή κατά την άσκηση των καθηκόντων της ως υπεύθυνης για την επιχειρησιακή διαχείριση του SIS II.

(5) Το άρθρο 15 παράγραφος 7 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 15 παράγραφος 7 της απόφασης 2007/533/ΔΕΥ ορίζουν ότι σε περίπτωση που η Επιτροπή μεταβιβάσει την ευθύνη κατά τη μεταβατική περίοδο προτού αναλάβει τις αρμοδιότητές της η διαχειριστική αρχή, μεριμνά ώστε η μεταβίβαση αυτή να μη θίγει το μηχανισμό αποτελεσματικού ελέγχου κατ' εφαρμογή του κοινοτικού δικαίου, είτε αυτός ασκείται από το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων είτε από το Ελεγκτικό Συνέδριο είτε από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων.

(6) Η διαχειριστική αρχή καταρτίζει το δικό της σχέδιο ασφαλείας σε σχέση με το κεντρικό SIS II, μόλις αναλάβει τις αρμοδιότητές της. Ως εκ τούτου, το παρόν σχέδιο ασφαλείας δεν ισχύει, στο βαθμό που σχετίζεται με το κεντρικό SIS II, αφότου η διαχειριστική αρχή αναλάβει τις αρμοδιότητές της.

(7) Το άρθρο 4 παράγραφος 3 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 4 παράγραφος 3 της απόφασης 2007/533/ΔΕΥ ορίζουν ότι το CS-SIS, το οποίο παρέχει την τεχνική εποπτεία και διοίκηση, εδρεύει στο Στρασβούργο (Γαλλία), ενώ στο Sankt Johann στο Pongau (Αυστρία) βρίσκεται το εφεδρικό σύστημα CS-SIS το οποίο θα μπορεί να διενεργεί όλες τις λειτουργίες του βασικού CS-SIS σε περίπτωση που εκείνο υποστεί βλάβη.

(8) Το σχέδιο ασφαλείας θα πρέπει να προβλέπει έναν υπεύθυνο ασφαλείας του συστήματος που θα ασκεί καθήκοντα σχετικά με την ασφάλεια τόσο του κεντρικού SIS II όσο και της επικοινωνιακής υποδομής, και δύο τοπικούς υπεύθυνους ασφαλείας που θα ασκούν καθήκοντα σχετικά με την ασφάλεια του κεντρικού SIS II και της επικοινωνιακής υποδομής, αντίστοιχα. Οι ρόλοι των υπευθύνων ασφαλείας θα καθορίζονται με σκοπό να εξασφαλισθεί η αποτελεσματική και άμεση ανταπόκριση σε περιστατικά που αφορούν την ασφάλεια και να υποβάλλονται οι σχετικές αναφορές.

(9) Θα πρέπει να καταρτιστεί πολιτική ασφαλείας που να προσδιορίζει όλες τις τεχνικές και οργανωτικές λεπτομέρειες σύμφωνα με τις διατάξεις της παρούσας απόφασης.

(10) Θα πρέπει να οριστούν μέτρα που να εξασφαλίζουν το κατάλληλο επίπεδο ασφαλείας στη λειτουργία τόσο του κεντρικού SIS II όσο και της επικοινωνιακής υποδομής,

[1] ΕΕ L 381 της 28.12.2006, σ. 4.
[2] ΕΕ L 205 της 7.8.2007, σ. 63.
[3] ΕΕ L 8 της 12.1.2001, σ. 1

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

ΚΕΦΑΛΑΙΟ I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο

1. Η παρούσα απόφαση θεσπίζει την οργάνωση και τα μέτρα ασφαλείας (σχέδιο ασφαλείας) για την προστασία του κεντρικού SIS II και των δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιό του, κατά απειλών σε βάρος της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητάς τους κατά την έννοια του άρθρου 16 παράγραφος 1 του κανονισμού (ΕΚ) αριθ. 1987/2006 και του άρθρου 16 παράγραφος 1 της απόφασης 2007/533/ΔΕΥ σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II), κατά τη διάρκεια μεταβατικής περιόδου, μέχρι να αναλάβει τις αρμοδιότητές της η διαχειριστική αρχή.

2. Η παρούσα απόφαση καθορίζει την οργάνωση και τα μέτρα ασφαλείας (σχέδιο ασφαλείας) για την προστασία της επικοινωνιακής υποδομής, κατά κινδύνων που απειλούν τη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητά της, κατά την έννοια του άρθρου 16 του κανονισμού (ΕΚ) αριθ. 1987/2006 και του άρθρου 16 της απόφασης 2007/533/ΔΕΥ σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II).

ΚΕΦΑΛΑΙΟ II

ΟΡΓΑΝΩΣΗ, ΑΡΜΟΔΙΟΤΗΤΕΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ

Άρθρο 2

Καθήκοντα της Επιτροπής

1. Η Επιτροπή εφαρμόζει και παρακολουθεί την αποτελεσματικότητα των μέτρων ασφαλείας για το κεντρικό SIS II που αναφέρονται στην παρούσα απόφαση.

2. Η Επιτροπή εφαρμόζει και παρακολουθεί την αποτελεσματικότητα των μέτρων ασφαλείας για την επικοινωνιακή υποδομή που αναφέρονται στην παρούσα απόφαση.

3. Η Επιτροπή ορίζει έναν από τους υπαλλήλους της ως υπεύθυνο ασφαλείας του συστήματος. Ο υπεύθυνος ασφαλείας του συστήματος ορίζεται από τον γενικό διευθυντή της Γενικής Διεύθυνσης Δικαιοσύνης, Ελευθερίας και Ασφάλειας της Επιτροπής. Ο υπεύθυνος ασφαλείας του συστήματος έχει, ειδικότερα, τα εξής καθήκοντα:

α) προετοιμάζει την πολιτική ασφαλείας, όπως αυτή περιγράφεται στο άρθρο 7 της παρούσας απόφασης·

β) παρακολουθεί την αποτελεσματικότητα της εφαρμογής των διαδικασιών ασφαλείας του κεντρικού SIS II·

γ) παρακολουθεί την αποτελεσματικότητα της εφαρμογής των διαδικασιών ασφαλείας της επικοινωνιακής υποδομής·

δ) συμβάλλει στην προετοιμασία των εκθέσεων σε σχέση με την ασφάλεια, όπως αναφέρεται στο άρθρο 50 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 66 της απόφασης 2007/533/ΔΕΥ·

ε) ασκεί καθήκοντα συντονισμού και παροχής βοήθειας κατά τη διενέργεια των ελέγχων από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων, όπως αναφέρεται στο άρθρο 45 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 61 της απόφασης 2007/533/ΔΕΥ, και κοινοποιεί περιστατικά, κατά την έννοια του άρθρου 5 παράγραφος 2 στον υπεύθυνο προστασίας δεδομένων της Επιτροπής·

στ) ελέγχει εάν η παρούσα απόφαση και η πολιτική ασφαλείας εφαρμόζονται ορθά και πλήρως από όλους τους εργολήπτες, συμπεριλαμβανομένων των υπεργολάβων που συμμετέχουν με οποιονδήποτε τρόπο στη διαχείριση του κεντρικού SIS II·

ζ) ελέγχει εάν η παρούσα απόφαση και η πολιτική ασφαλείας εφαρμόζονται ορθά και ολοκληρωμένα από όλους τους εργολήπτες, συμπεριλαμβανομένων των υπεργολάβων που συμμετέχουν με οποιονδήποτε τρόπο στη διαχείριση της επικοινωνιακής υποδομής·

η) διατηρεί κατάλογο των εθνικών σημείων επαφής για την ασφάλεια του SIS II, τον οποίο γνωστοποιεί στον τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή·

θ) γνωστοποιεί τον κατάλογο που αναφέρεται στο σημείο η) στον τοπικό υπεύθυνο ασφαλείας για το κεντρικό SIS II.

Άρθρο 3

Τοπικός υπεύθυνος ασφαλείας για το κεντρικό SIS II

1. Με την επιφύλαξη του άρθρου 8, η Επιτροπή ορίζει από τους υπαλλήλους της έναν τοπικό υπεύθυνο ασφαλείας για το κεντρικό SIS II. Αποφεύγεται κάθε σύγκρουση συμφερόντων μεταξύ των καθηκόντων του τοπικού υπεύθυνου ασφαλείας και κάθε άλλου υπηρεσιακού καθήκοντος. Ο τοπικός υπεύθυνος ασφαλείας για το κεντρικό SIS II ορίζεται από τον γενικό διευθυντή της Γενικής Διεύθυνσης Δικαιοσύνης, Ελευθερίας και Ασφάλειας της Επιτροπής.

2. Ο τοπικός υπεύθυνος ασφαλείας για το κεντρικό SIS II μεριμνά ώστε τα μέτρα ασφαλείας που αναφέρονται στην παρούσα απόφαση να εφαρμόζονται, και οι σχετικές διαδικασίες να ακολουθούνται στο κύριο CS-SIS. Όσον αφορά το εφεδρικό CS-SIS, ο τοπικός υπεύθυνος ασφαλείας για το κεντρικό SIS II μεριμνά επίσης ώστε τα μέτρα ασφαλείας που αναφέρονται στην παρούσα απόφαση, με εξαίρεση αυτά που αναφέρονται στο άρθρο 9, να εφαρμόζονται και οι σχετικές διαδικασίες ασφαλείας να ακολουθούνται.

3. Ο τοπικός υπεύθυνος ασφαλείας για το κεντρικό SIS II μπορεί να αναθέτει οποιοδήποτε από τα καθήκοντά του σε υφισταμένους του. Αποφεύγεται κάθε σύγκρουση συμφερόντων μεταξύ της υποχρέωσης εκτέλεσης των εν λόγω καθηκόντων και κάθε άλλου υπηρεσιακού καθήκοντος. Η επικοινωνία με τον τοπικό υπεύθυνο ασφαλείας ή τον εν υπηρεσία υφιστάμενό του είναι δυνατή ανά πάσα στιγμή, μέσω ενός αριθμού τηλεφώνου και μιας διεύθυνσης επαφής.

4. Ο τοπικός υπεύθυνος ασφαλείας για το κεντρικό SIS II εκτελεί τα καθήκοντα που προκύπτουν από τη λήψη μέτρων ασφαλείας στο χώρο εγκατάστασης του κύριου και του εφεδρικού CS-SIS, εντός των ορίων της παραγράφου 1, και συγκεκριμένα:

α) ασκεί καθήκοντα σχετικά με την τοπική λειτουργική ασφάλεια, στα οποία περιλαμβάνονται ο έλεγχος των ζωνών ασφαλείας, οι τακτικές δοκιμές ασφαλείας, ο γενικός έλεγχος και η υποβολή εκθέσεων·

β) παρακολουθεί την αποτελεσματικότητα του σχεδίου αδιάκοπτης λειτουργίας και εξασφαλίζει την τακτική διενέργεια ασκήσεων·

γ) εξασφαλίζει αποδεικτικά στοιχεία και αναφέρει στον υπεύθυνο ασφαλείας του συστήματος κάθε περιστατικό στο κεντρικό SIS II που ενδέχεται να έχει επίπτωση στην ασφάλεια του κεντρικού SIS II ή της επικοινωνιακής υποδομής·

δ) ενημερώνει τον υπεύθυνο ασφαλείας του συστήματος εάν απαιτείται τροποποίηση της πολιτικής ασφαλείας·

ε) ελέγχει εάν η παρούσα απόφαση και η πολιτική ασφαλείας εφαρμόζονται από όλους τους εργολήπτες, συμπεριλαμβανομένων των υπεργολάβων που συμμετέχουν με οποιονδήποτε τρόπο στη λειτουργική επιχειρησιακή διαχείριση του κεντρικού SIS II·

στ) εξασφαλίζει ότι το προσωπικό γνωρίζει τις υποχρεώσεις του και παρακολουθεί την εφαρμογή της πολιτικής ασφαλείας·

ζ) παρακολουθεί τις εξελίξεις όσον αφορά την ασφάλεια των πληροφοριακών συστημάτων και μεριμνά για την ανάλογη επιμόρφωση του προσωπικού·

η) συγκεντρώνει τις σχετικές πληροφορίες και προτείνει επιλογές για τη θέσπιση, ενημέρωση και αναθεώρηση της πολιτικής ασφαλείας, σύμφωνα με το άρθρο 7.

Άρθρο 4

Τοπικός υπεύθυνος ασφαλείας για την επικοινωνιακή υποδομή

1. Με την επιφύλαξη του άρθρου 8, η Επιτροπή ορίζει από τους υπαλλήλους της έναν τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή. Αποφεύγεται κάθε σύγκρουση συμφερόντων μεταξύ των καθηκόντων του υπεύθυνου τοπικής ασφαλείας και κάθε άλλου υπηρεσιακού καθήκοντος. Ο τοπικός υπεύθυνος ασφαλείας για την επικοινωνιακή υποδομή ορίζεται από τον γενικό διευθυντή της Γενικής Διεύθυνσης Δικαιοσύνης, Ελευθερίας και Ασφάλειας της Επιτροπής.

2. Ο τοπικός υπεύθυνος ασφαλείας για την επικοινωνιακή υποδομή παρακολουθεί τη λειτουργία της επικοινωνιακής υποδομής και μεριμνά ώστε τα μέτρα ασφαλείας να εφαρμόζονται, και οι σχετικές διαδικασίες να ακολουθούνται.

3. Ο τοπικός υπεύθυνος ασφαλείας για την επικοινωνιακή υποδομή μπορεί να αναθέτει οποιοδήποτε από τα καθήκοντά του σε υφισταμένους του. Αποφεύγεται κάθε σύγκρουση συμφερόντων μεταξύ της υποχρέωσης εκτέλεσης των εν λόγω καθηκόντων και κάθε άλλου υπηρεσιακού καθήκοντος. Η επικοινωνία με τον τοπικό υπεύθυνο ασφαλείας ή τον εν υπηρεσία υφιστάμενό του είναι δυνατή ανά πάσα στιγμή, μέσω ενός αριθμού τηλεφώνου και μιας διεύθυνσης επαφής.

4. Ο τοπικός υπεύθυνος ασφαλείας για την επικοινωνιακή υποδομή εκτελεί τα καθήκοντα που προκύπτουν από τη λήψη μέτρων ασφαλείας στην επικοινωνιακή υποδομή, και συγκεκριμένα:

α) εκτελεί όλα τα καθήκοντα λειτουργικής ασφαλείας που σχετίζονται με την επικοινωνιακή υποδομή, στα οποία περιλαμβάνονται ο έλεγχος των ζωνών ασφαλείας, οι τακτικές δοκιμές ασφαλείας, ο γενικός έλεγχος και η υποβολή εκθέσεων·

β) παρακολουθεί την αποτελεσματικότητα του σχεδίου αδιάκοπτης λειτουργίας και εξασφαλίζει την τακτική διενέργεια ασκήσεων·

γ) διαφυλάττει αποδεικτικά στοιχεία και υποβάλλει εκθέσεις στον υπεύθυνο ασφαλείας του σχετικά με κάθε περιστατικό που συνέβη στην επικοινωνιακή υποδομή και ενδέχεται να έχει αντίκτυπο στην ασφάλεια του κεντρικού SIS II ή της επικοινωνιακής υποδομής·

δ) ενημερώνει τον υπεύθυνο ασφαλείας του συστήματος για ενδεχόμενες τροποποιήσεις που χρειάζεται η πολιτική ασφαλείας·

ε) ελέγχει εάν η παρούσα απόφαση και η πολιτική ασφαλείας εφαρμόζονται από όλους τους εργολήπτες, συμπεριλαμβανομένων των υπεργολάβων που συμμετέχουν με οποιονδήποτε τρόπο στη διαχείριση της επικοινωνιακής υποδομής·

στ) εξασφαλίζει ότι το προσωπικό γνωρίζει τις υποχρεώσεις του και παρακολουθεί την εφαρμογή της πολιτικής ασφαλείας·

ζ) παρακολουθεί τις εξελίξεις όσον αφορά την ασφάλεια των πληροφοριακών συστημάτων και μεριμνά για την ανάλογη επιμόρφωση του προσωπικού·

η) συγκεντρώνει τις σχετικές πληροφορίες και προτείνει επιλογές για τη θέσπιση, ενημέρωση και αναθεώρηση της πολιτικής ασφαλείας σύμφωνα με το άρθρο 7.

Άρθρο 5

Περιστατικά που θέτουν σε κίνδυνο την ασφάλεια

1. Κάθε γεγονός που έχει ή ενδέχεται να έχει επίπτωση στην ασφάλεια του SIS II και μπορεί να προκαλέσει ζημία ή απώλεια στο SIS II θεωρείται ως περιστατικό που θέτει σε κίνδυνο την ασφάλεια, ιδίως όταν πρόκειται για πρόσβαση σε δεδομένα ή σε περιπτώσεις που θίγεται ή ενδέχεται να θιγεί η διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα δεδομένων.

2. Περιστατικά που θέτουν σε κίνδυνο την ασφάλεια αντιμετωπίζονται κατά τρόπο που να εξασφαλίζεται η γρήγορη, αποτελεσματική και ενδεδειγμένη ανάληψη δράσης σύμφωνα με την πολιτική ασφαλείας. Θεσπίζονται διαδικασίες αποκατάστασης των ζημιών από ανάλογα περιστατικά.

3. Οι πληροφορίες σχετικά με περιστατικά που θέτουν σε κίνδυνο την ασφάλεια και έχουν ή ενδέχεται να έχουν επίπτωση στη λειτουργία του SIS II σε κράτος μέλος ή στη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των δεδομένων που εισάγονται ή αποστέλλονται από κράτος μέλος, γνωστοποιούνται στο ενδιαφερόμενο κράτος μέλος. Τα περιστατικά που θέτουν σε κίνδυνο την ασφάλεια κοινοποιούνται στον υπεύθυνο προστασίας δεδομένων της Επιτροπής.

Άρθρο 6

Διαχείριση περιστατικών

1. Όλα τα μέλη του προσωπικού και οι εργολήπτες που συμμετέχουν στην ανάπτυξη, διαχείριση ή λειτουργία του SIS II υποχρεούνται να σημειώνουν και να αναφέρουν στον υπεύθυνο ασφαλείας του συστήματος ή στον τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή κάθε διαπιστωμένη ή εικαζόμενη αδυναμία όσον αφορά την ασφάλεια της υποδομής αυτής.

2. Σε περίπτωση περιστατικού που έχει ή ενδέχεται να έχει αντίκτυπο στην ασφάλεια του SIS II, ο τοπικός υπεύθυνος ασφαλείας για την επικοινωνιακή υποδομή ενημερώνει το ταχύτερο δυνατό τον υπεύθυνο ασφαλείας του συστήματος και, ανάλογα με την περίπτωση, το ενιαίο εθνικό σημείο επαφής για την ασφάλεια του SIS II, εφόσον το σχετικό κράτος μέλος διαθέτει σημείο επαφής, γραπτά ή, σε περιπτώσεις άκρως έκτακτης ανάγκης, με άλλα μέσα επικοινωνίας. Η έκθεση περιέχει περιγραφή του περιστατικού που θέτει σε κίνδυνο την ασφάλεια, το επίπεδο του κινδύνου, τις πιθανές συνέπειες και τα μέτρα που έχουν ληφθεί ή θα πρέπει να ληφθούν για να μετριασθεί ο κίνδυνος.

3. Κάθε αποδεικτικό στοιχείο σχετικό με το περιστατικό που θέτει σε κίνδυνο την ασφάλεια διαφυλάσσεται αμέσως από τον τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή. Στον βαθμό που αυτό είναι δυνατό βάσει των ισχυουσών διατάξεων για την προστασία των δεδομένων, τα αποδεικτικά αυτά στοιχεία τίθενται στη διάθεση του υπεύθυνου ασφαλείας του συστήματος μετά την υποβολή σχετικής αίτησης εκ μέρους του.

4. Στην πολιτική για την ασφάλεια καθορίζονται διαδικασίες ανατροφοδότησης, ώστε να εξασφαλισθεί ότι πληροφορίες σχετικά με το είδος, την αντιμετώπιση και την έκβαση περιστατικών που θέτουν σε κίνδυνο την ασφάλεια κοινοποιούνται στον υπεύθυνο ασφαλείας του συστήματος ή στον τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή, μετά τη διευθέτηση και τη λήξη του περιστατικού.

5. Οι παράγραφοι 1 έως 4 εφαρμόζονται, τηρουμένων των αναλογιών, σε περιστατικά στο κεντρικό SIS II. Στο βαθμό αυτό, κάθε αναφορά στον τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή στις παραγράφους 1 έως 4 νοείται ως αναφορά στον τοπικό υπεύθυνο ασφαλείας για το κεντρικό SIS II.

ΚΕΦΑΛΑΙΟ III

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Άρθρο 7

Πολιτική ασφαλείας

1. Η πολιτική ασφαλείας είναι δεσμευτική και θεσπίζεται, ενημερώνεται και αναθεωρείται τακτικά από τον γενικό διευθυντή της Γενικής Διεύθυνσης Δικαιοσύνης, Ελευθερίας και Ασφάλειας, σύμφωνα με την παρούσα απόφαση. Η πολιτική ασφαλείας προβλέπει λεπτομερείς διαδικασίες και μέτρα προστασίας από απειλές σε βάρος της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας της επικοινωνιακής υποδομής, συμπεριλαμβανομένου του προγραμματισμού σε περιπτώσεις έκτακτης ανάγκης, προκειμένου να εξασφαλισθεί το κατάλληλο επίπεδο ασφαλείας που ορίζει η παρούσα απόφαση. Η πολιτική ασφαλείας συμμορφώνεται προς την παρούσα απόφαση.

2. Η πολιτική ασφαλείας βασίζεται σε εκτίμηση των κινδύνων. Τα μέτρα που περιγράφονται στην πολιτική ασφαλείας είναι ανάλογα των προσδιορισμένων κινδύνων.

3. Η εκτίμηση των κινδύνων και η πολιτική ασφαλείας ενημερώνονται, όταν το απαιτούν τεχνολογικές αλλαγές, νέες απειλές ή οποιεσδήποτε άλλες περιστάσεις. Η πολιτική ασφαλείας αναθεωρείται οπωσδήποτε σε ετήσια βάση, ώστε να εξασφαλισθεί ότι θα ανταποκρίνεται με τον δέοντα τρόπο στην πλέον πρόσφατη εκτίμηση κινδύνων ή σε οποιαδήποτε άλλη πρόσφατη τεχνολογική αλλαγή, απειλή ή άλλη σχετική περίσταση.

4. Η πολιτική ασφαλείας προετοιμάζεται από τον υπεύθυνο ασφαλείας του συστήματος, σε συντονισμό με τον τοπικό υπεύθυνο ασφαλείας για το κεντρικό SIS II και τον τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή.

5. Οι παράγραφοι 1 έως 4 εφαρμόζονται, τηρουμένων των αναλογιών, στην πολιτική ασφαλείας για το κεντρικό SIS II. Στον βαθμό αυτό, κάθε αναφορά στον τοπικό υπεύθυνο ασφαλείας για την επικοινωνιακή υποδομή στις παραγράφους 1 έως 4 νοείται ως αναφορά στον τοπικό υπεύθυνο ασφαλείας για το κεντρικό SIS II.

Άρθρο 8

Εφαρμογή των μέτρων ασφαλείας

1. Η άσκηση των καθηκόντων και τήρηση των απαιτήσεων που ορίζονται στην παρούσα απόφαση, συμπεριλαμβανομένου του καθήκοντος ορισμού υπεύθυνου τοπικής ασφαλείας, μπορεί να ανατεθεί με σύμβαση ή να μεταβιβαστεί σε ιδιωτικούς ή δημόσιους φορείς.

2. Στην περίπτωση αυτή, η Επιτροπή εξασφαλίζει με νομικά δεσμευτική συμφωνία ότι οι απαιτήσεις που ορίζονται στην παρούσα απόφαση και στην πολιτική ασφαλείας τηρούνται πλήρως. Σε περίπτωση μεταβίβασης ή ανάθεσης με σύμβαση του καθήκοντος ορισμού τοπικού υπεύθυνου ασφαλείας, η Επιτροπή εξασφαλίζει με νομικά δεσμευτική συμφωνία ότι θα γνωμοδοτήσει σχετικά με το άτομο που πρόκειται να οριστεί ως τοπικός υπεύθυνος ασφαλείας.

Άρθρο 9

Έλεγχος της εισόδου στις εγκαταστάσεις

3. Χρησιμοποιούνται περίμετροι ασφαλείας με προστατευτικά κιγκλιδώματα και ελέγχους εισόδου για την προστασία των χώρων που περιέχουν εγκαταστάσεις επεξεργασίας δεδομένων.

2. Εντός των περιμέτρων ασφαλείας, καθορίζονται ασφαλείς χώροι για την προστασία των υλικών στοιχείων (περιουσιακών στοιχείων), συμπεριλαμβανομένου του υλικού, των μέσων αποθήκευσης δεδομένων, των κονσολών, των σχεδίων και άλλων εγγράφων για το SIS II, καθώς και των γραφείων και άλλων τόπων εργασίας του προσωπικού που σχετίζεται με τη λειτουργία του SIS II. Οι εν λόγω ασφαλείς χώροι προστατεύονται με τους κατάλληλους ελέγχους εισόδου, που σκοπό έχουν να εξασφαλιστεί ότι η πρόσβαση επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό. Η εργασία στους ασφαλείς χώρους υπόκειται σε λεπτομερείς κανόνες ασφαλείας που καθορίζονται στην πολιτική ασφαλείας.

3. Προβλέπονται και εγκαθίστανται συστήματα ασφαλείας για γραφεία, αίθουσες και εγκαταστάσεις. Σημεία πρόσβασης, όπως χώροι παράδοσης και φόρτωσης, καθώς και άλλα σημεία, όπου είναι δυνατή η είσοδος μη εξουσιοδοτημένων ατόμων, ελέγχονται και, εφόσον είναι δυνατό, απομονώνονται από τις εγκαταστάσεις επεξεργασίας ώστε να αποφεύγεται το ενδεχόμενο μη εξουσιοδοτημένης πρόσβασης.

4. Αναλόγως του κινδύνου, καθορίζονται και εφαρμόζονται μέτρα προστασίας των περιμέτρων ασφαλείας κατά ζημιών από φυσικές καταστροφές ή δολιοφθορές.

5. Ο εξοπλισμός προστατεύεται από υλικές και περιβαλλοντικές ζημίες και από το ενδεχόμενο μη εξουσιοδοτημένης πρόσβασης.

6. Εάν η Επιτροπή διαθέτει σχετικές πληροφορίες, προσθέτει στον κατάλογο που αναφέρεται στο άρθρο 2 παράγραφος 3 στοιχείο η) ένα σημείο επαφής για την παρακολούθηση της εφαρμογής των διατάξεων του παρόντος άρθρου στους χώρους εγκατάστασης του εφεδρικού CS-SIS.

Άρθρο 10

Μέσα αποθήκευσης δεδομένων και έλεγχος περιουσιακών στοιχείων

1. Τα αφαιρετά μέσα αποθήκευσης που περιέχουν δεδομένα προστατεύονται κατά της μη εξουσιοδοτημένης πρόσβασης, κατάχρησης ή αλλοίωσης, και η αναγνωσιμότητά τους εξασφαλίζεται καθ' όλη τη διάρκεια ζωής των δεδομένων.

2. Τα μέσα αποθήκευσης, όταν δεν είναι πλέον αναγκαία, καταστρέφονται με τρόπο σίγουρο και ασφαλή, σύμφωνα με τις λεπτομερείς διαδικασίες που καθορίζονται στην πολιτική ασφαλείας.

3. Συντάσσονται καταστάσεις απογραφής για να εξασφαλισθεί η ύπαρξη διαθέσιμων πληροφοριών σχετικά με τα αρχεία καταχώρισης, την εφαρμοζόμενη περίοδο διατήρησης και τις άδειες πρόσβασης.

4. Όλα τα σημαντικά στοιχεία ενεργητικού της επικοινωνιακής υποδομής προσδιορίζονται, ώστε να είναι δυνατή η προστασία τους αναλόγως της σημασίας τους. Τηρείται ενημερωμένο αρχείο του σχετικού εξοπλισμού πληροφορικής.

5. Υπάρχει διαθέσιμο έγγραφο υλικό σχετικά με την επικοινωνιακή υποδομή το οποίο ενημερώνεται. Η μη εξουσιοδοτημένη πρόσβαση στο υλικό αυτό απαγορεύεται.

6. Οι παράγραφοι 1 έως 5 εφαρμόζονται, τηρουμένων των αναλογιών, στο κεντρικό SIS II. Στο βαθμό αυτό, κάθε αναφορά στην επικοινωνιακή υποδομή νοείται ως αναφορά στο κεντρικό SIS II.

Άρθρο 11

Έλεγχος της καταχώρισης σε αρχείο

1. Λαμβάνονται τα κατάλληλα μέτρα για να εξασφαλιστεί η δέουσα καταχώριση των δεδομένων σε αρχείο και η εξουσιοδοτημένη μόνο πρόσβαση σε αυτά.

2. Όλα τα στοιχεία εξοπλισμού που περιέχουν μέσα αποθήκευσης ελέγχονται πριν διατεθούν ως απορρίμματα ώστε να εξασφαλιστεί ότι τα ευαίσθητα δεδομένα έχουν αφαιρεθεί ή πλήρως επικαλυφθεί, ή καταστρέφονται κατά τρόπο ασφαλή.

Άρθρο 12

Έλεγχος κωδικού αναγνώρισης

1. Όλοι οι κωδικοί αναγνώρισης φυλάσσονται σε ασφαλές μέρος και είναι εμπιστευτικοί. Εάν υπάρχει υπόνοια ότι ένας κωδικός αναγνώρισης έχει διαρρεύσει, ο εν λόγω κωδικός τροποποιείται αμέσως ή ο σχετικός λογαριασμός ακυρώνεται. Χρησιμοποιούνται ατομικές και αποκλειστικές ταυτότητες χρήστη.

2. Στην πολιτική ασφαλείας ορίζονται οι διαδικασίες για την είσοδο στο σύστημα και την έξοδο από αυτό ώστε να αποφευχθεί το ενδεχόμενο μη εξουσιοδοτημένης πρόσβασης.

Άρθρο 13

Έλεγχος της πρόσβασης

1. Η πολιτική ασφαλείας καθορίζει μια επίσημη διαδικασία εγγραφής και διαγραφής του προσωπικού όσον αφορά τη χορήγηση και την ανάκληση πρόσβασης στο υλικό και λογισμικό του SIS II για τους σκοπούς της επιχειρησιακής διαχείρισης. Η χορήγηση και χρήση των ενδεδειγμένων στοιχείων πρόσβασης (κωδικοί αναγνώρισης ή άλλα κατάλληλα μέσα) ελέγχονται με επίσημη διαδικασία διαχείρισης, όπως καθορίζεται στην πολιτική ασφαλείας.

2. Η πρόσβαση στο υλικό και λογισμικό SIS II στο CS-SIS:

i) περιορίζεται στα εξουσιοδοτημένα πρόσωπα·

ii) περιορίζεται στις περιπτώσεις που υφίσταται θεμιτός σκοπός σύμφωνα με το άρθρο 45 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 61 της απόφασης 2007/533/ΔΕΥ, ή με το άρθρο 50 παράγραφος 2 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 66 παράγραφος 2 της απόφασης 2007/533/ΔΕΥ·

iii) δεν υπερβαίνει τη διάρκεια και το πεδίο εφαρμογής που απαιτούνται για τον σκοπό της πρόσβασης· και

iv) παραχωρείται μόνο σύμφωνα με την πολιτική ελέγχου της πρόσβασης που καθορίζεται στην πολιτική ασφαλείας.

3. Στο CS-SIS χρησιμοποιούνται μόνο οι κονσόλες και το λογισμικό που έχουν εγκριθεί από τον τοπικό υπεύθυνο ασφαλείας για το κεντρικό SIS II. Η χρήση υπηρεσιών συστήματος με τις οποίες είναι δυνατό να αποφευχθούν έλεγχοι του συστήματος και της εφαρμογής, περιορίζεται και ελέγχεται. Προβλέπονται διαδικασίες για τον έλεγχο της εγκατάστασης του λογισμικού.

Άρθρο 14

Έλεγχος της διαβίβασης

Η επικοινωνιακή υποδομή παρακολουθείται, ώστε να εξασφαλίζεται η διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των ανταλλαγών πληροφοριών. Χρησιμοποιούνται κρυπτογραφικά μέσα για την προστασία των δεδομένων που μεταβιβάζονται στην επικοινωνιακή υποδομή.

Άρθρο 15

Έλεγχος της εισαγωγής

Οι λογαριασμοί προσώπων που διαθέτουν εξουσιοδότηση πρόσβασης στο λογισμικό SIS II από το CS-SIS ελέγχονται από τον τοπικό υπεύθυνο ασφαλείας για το κεντρικό SIS II. Η χρήση των εν λόγω λογαριασμών, συμπεριλαμβανομένου του χρόνου και της ταυτότητας του χρήστη, καταχωρίζονται.

Άρθρο 16

Έλεγχος της μεταφοράς

1. Στην πολιτική ασφαλείας ορίζονται τα κατάλληλα μέτρα ώστε να αποφεύγεται η μη εξουσιοδοτημένη ανάγνωση, αντιγραφή, τροποποίηση ή διαγραφή προσωπικών δεδομένων κατά τη διαβίβασή τους στο ή από το SIS II ή κατά τη μεταφορά των μέσων αποθήκευσής τους. Στην πολιτική ασφαλείας καθορίζονται διατάξεις όσον αφορά τους επιτρεπτούς τρόπους αποστολής ή μεταφοράς, καθώς και όσον αφορά τις διαδικασίες λογοδοσίας για τη μεταφορά στοιχείων και την άφιξή τους στον τόπο προορισμού. Τα μέσα αποθήκευσης δεδομένων δεν περιέχουν άλλα δεδομένα εκτός από αυτά που πρέπει να αποσταλούν.

2. Υπηρεσίες που παρέχονται από τρίτους και αφορούν την πρόσβαση, επεξεργασία, διαβίβαση ή διαχείριση εγκαταστάσεων επεξεργασίας δεδομένων ή προϊόντα ή υπηρεσίες που προστίθενται σε εγκαταστάσεις επεξεργασίας δεδομένων, υποβάλλονται σε κατάλληλα ολοκληρωμένους ελέγχους ασφαλείας.

Άρθρο 17

Ασφάλεια της επικοινωνιακής υποδομής

1. Ο έλεγχος και η διαχείριση της επικοινωνιακής υποδομής πραγματοποιούνται κατά τον ενδεδειγμένο τρόπο ώστε η επικοινωνιακή υποδομή να προστατεύεται από απειλές και να εξασφαλίζεται η ασφάλεια τόσο της ίδιας όσο και του κεντρικού SIS II, συμπεριλαμβανομένης της ανταλλαγής δεδομένων μέσω αυτού.

2. Τα χαρακτηριστικά ασφαλείας, τα επίπεδα εξυπηρέτησης και οι απαιτήσεις διαχείρισης όλων των υπηρεσιών δικτύου προσδιορίζονται στη συμφωνία παροχής υπηρεσιών δικτύου με τον πάροχο υπηρεσιών.

3. Εκτός από την προστασία των σημείων πρόσβασης SIS II, προστατεύεται και κάθε πρόσθετη υπηρεσία που χρησιμοποιείται από την επικοινωνιακή υποδομή. Στην πολιτική ασφαλείας ορίζονται τα κατάλληλα μέτρα.

Άρθρο 18

Παρακολούθηση

1. Ημερολόγια για την καταγραφή των πληροφοριών που αναφέρονται στο άρθρο 18 παράγραφος 1 του κανονισμού (ΕΚ) αριθ. 1987/2006 και στο άρθρο 18 παράγραφος 1 της απόφασης 2007/533/ΔΕΥ σχετικά με κάθε πρόσβαση σε προσωπικά δεδομένα και κάθε ανταλλαγή τους στο πλαίσιο του CS-SIS παραμένουν ασφαλώς αποθηκευμένα και προσβάσιμα από τους χώρους εγκατάστασης του κύριου και εφεδρικού CS-SIS για το ανώτατο χρονικό διάστημα που αναφέρεται στο άρθρο 18 παράγραφος 3 του κανονισμού (ΕΚ) αριθ. 1987/2006 και στο άρθρο 18 παράγραφος 3 της απόφασης 2007/533/ΔΕΥ.

2. Στην πολιτική ασφαλείας καθορίζονται οι διαδικασίες για την παρακολούθηση της χρήσης ή των σφαλμάτων στις εγκαταστάσεις επεξεργασίας δεδομένων και τα αποτελέσματα των δραστηριοτήτων παρακολούθησης αναθεωρούνται τακτικά. Εφόσον κριθεί απαραίτητο, λαμβάνονται κατάλληλα μέτρα.

3. Τα ημερολόγια και οι σχετικές υποδομές προστατεύονται κατά κάθε παραποίησης και μη εξουσιοδοτημένης πρόσβασης ώστε να τηρούνται οι απαιτήσεις συγκέντρωσης και διατήρησης αποδεικτικών στοιχείων κατά την περίοδο διατήρησης.

Άρθρο 19

Κρυπτογραφικά μέτρα

Όταν αυτό κριθεί απαραίτητο, χρησιμοποιούνται κρυπτογραφικά μέτρα για την προστασία των πληροφοριών. Η χρήση τους, καθώς και οι σκοποί και οι όροι αυτής, πρέπει να εγκριθούν εκ των προτέρων από τον υπεύθυνο ασφαλείας του συστήματος.

ΚΕΦΑΛΑΙΟ IV

ΑΣΦΆΛΕΙΑ ΑΝΘΡΏΠΙΝΩΝ ΠΌΡΩΝ

Άρθρο 20

Χαρακτηριστικά του προσωπικού

1. Η πολιτική ασφαλείας ορίζει τα καθήκοντα και τις αρμοδιότητες των προσώπων που διαθέτουν εξουσιοδοτημένη πρόσβαση στο κεντρικό SIS II.

2. Η πολιτική ασφαλείας ορίζει τα καθήκοντα και τις αρμοδιότητες των προσώπων που διαθέτουν εξουσιοδοτημένη πρόσβαση στην επικοινωνιακή υποδομή.

3. Οι ρόλοι και οι αρμοδιότητες ασφαλείας του προσωπικού της Επιτροπής, των εργοληπτών και του προσωπικού που συμμετέχουν στην επιχειρησιακή διαχείριση ορίζονται, επισημοποιούνται και ανακοινώνονται στους ενδιαφερόμενους. Για το προσωπικό της Επιτροπής, οι εν λόγω ρόλοι και αρμοδιότητες αναφέρονται στην περιγραφή των καθηκόντων και στους στόχους, ενώ για τους εργολήπτες αναφέρονται στις συμβάσεις ή στις συμφωνίες όσον αφορά τα επίπεδα εξυπηρέτησης.

4. Συμφωνίες εμπιστευτικότητας και διαφύλαξης του απορρήτου συνάπτονται με όλα τα πρόσωπα τα οποία δεν υπόκεινται στους κανόνες της Ευρωπαϊκής Ένωσης ή των κρατών μελών για τις δημόσιες υπηρεσίες. Το προσωπικό που πρόκειται να εργαστεί με δεδομένα SIS II εφοδιάζεται με τις απαραίτητες άδειες ή πιστοποιητικά σύμφωνα με τις λεπτομερείς διαδικασίες που καθορίζονται στην πολιτική ασφαλείας.

Άρθρο 21

Παροχή πληροφοριών στο προσωπικό

1. Όλα τα μέλη του προσωπικού και οι εργολήπτες παρακολουθούν κατάλληλη κατάρτιση σχετικά με τα θέματα ασφαλείας, τις νομικές απαιτήσεις, τις πολιτικές και τις διαδικασίες, στο βαθμό που απαιτούν τα καθήκοντά τους.

2. Μετά τη λύση της μίσθωσης εργασίας ή της σύμβασης, η πολιτική ασφαλείας ορίζει τις υποχρεώσεις του προσωπικού και των εργοληπτών που σχετίζονται με την αλλαγή εργασίας ή τη λύση της μίσθωσης εργασίας, και θεσπίζει τις διαδικασίες για τη διαχείριση της επιστροφής των στοιχείων ενεργητικού και την αφαίρεση των δικαιωμάτων πρόσβασης.

ΚΕΦΑΛΑΙΟ V

ΤΕΛΙΚΗ ΔΙΑΤΑΞΗ

Άρθρο 22

Εφαρμογή

1. Η παρούσα απόφαση τίθεται σε εφαρμογή την ημερομηνία που θα καθορίσει το Συμβούλιο σύμφωνα με το άρθρο 55 παράγραφος 2 του κανονισμού (ΕΚ) αριθ. 1987/2006 και το άρθρο 71 παράγραφος 2 της απόφασης 2007/533/ΔΕΥ.

2. Τα άρθρα 1 παράγραφος 1, 2 παράγραφος 1, 2 παράγραφος 3 στοιχεία β), δ), στ) και θ), 3, 6 παράγραφος 5, 7 παράγραφος 5, 9 παράγραφος 6, 10 παράγραφος 6, 13 παράγραφοι 2 και 3, 15, 18 και 20 παράγραφος 1 λήγουν όταν η διαχειριστική αρχή αναλάβει τα καθήκοντά της.

Βρυξέλλες, 4 Μαΐου 2010.

Για την Επιτροπή

Ο Πρόεδρος

José Manuel BARROSO