Αριθμός πράξης 01/2013 (ΦΕΚ Β' 3433/31/12/2013)
Κοινή Πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) ως προς τις υποχρεώσεις των παροχών για την προστασία και ασφάλεια των δεδομένων σύμφωνα με τις διατάξεις του άρθρου 7 του ν. 3917/2011, όπως ισχύει («Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις», ΦΕΚ Α'22).

Η ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ (Α.Π.Δ.Π.Χ.)
ΚΑΙ
Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ
ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (Α.Δ.Α.Ε.)

Έχοντας υπόψη:

1. Τη διάταξη του άρθρου 7 παρ. 2 του ν. 3917/2011 «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις», ΦΕΚ Α' 22, όπως ισχύει,

2. Τις απαντήσεις των ενδιαφερόμενων φορέων, όπως διατυπώθηκαν στο πλαίσιο της σχετικής δημόσιας διαβούλευσης, η οποία έλαβε χώρα κατά το διάστημα από 18.10.2013 έως 11.11.2013,

3. Το Πρακτικό της συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε. της 11.12.2013,

4. Το Πρακτικό της συνεδρίασης της Ολομέλειας της Α.Π.Δ.Π.Χ. της 18.12.2013,

5. Το γεγονός ότι από τις διατάξεις της παρούσας δεν προκαλείται δαπάνη για το τρέχον και τα επόμενα οικονομικά έτη εις βάρος του Κρατικού Προϋπολογισμού, αποφασίζουν:

Την έκδοση της παρούσας Κοινής Πράξης, οι διατάξεις της οποίας έχουν ως ακολούθως:

Άρθρο 1
Σκοπός - Πεδίο Εφαρμογής

Με την παρούσα πράξη ορίζονται τα μέτρα για την προστασία και ασφάλεια των δεδομένων που οφείλουν να λαμβάνουν οι πάροχοι διαθέσιμων κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών (εφεξής «πάροχοι») σύμφωνα με τη διάταξη της παραγράφου 2 του άρθρου 7 του ν. 3917/2011, όπως ισχύει.

Άρθρο 2
Ορισμοί

Για τους σκοπούς της παρούσας πράξης εφαρμόζονται οι ορισμοί του άρθρου 2 του ν.3917/2011, επιπλέον δε νοούνται ως:

α) «Σύστημα Διατήρησης Δεδομένων (ΣΔΙΔΕ)»: η αποτελούμενη από υλικό και λογισμικό εξοπλισμό υποδομή του παρόχου που χρησιμοποιείται για τη διατήρηση των δεδομένων του άρθρου 5 του ν.3917/2011.

β) «Τόπος εγκατάστασης ΣΔΙΔΕ»: ο χώρος στον οποίο είναι εγκατεστημένο το σύστημα ΣΔΙΔΕ ή μέρος αυτού.

γ) «Περιστατικό παραβίασης ασφάλειας»: η παραβίαση της ασφάλειας που οδηγεί ή δύναται να οδηγήσει σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση των δεδομένων του άρθρου 5 του ν. 3917/2011.

δ) «Ομάδα του ΣΔΙΔΕ»: το προσωπικό του παρόχου, στο οποίο έχει ανατεθεί η λειτουργία και διαχείριση του ΣΔΙΔΕ.

Άρθρο 3
Ειδικό σχέδιο πολιτικής ασφάλειας

1. Το ειδικό σχέδιο πολιτικής ασφάλειας, όπως αυτό ορίζεται στην παρ. 2 του άρθρου 7 του ν. 3917/2011, αποτελείται από ειδική πολιτική και μέτρα ασφάλειας και διασφαλίζει την τήρηση των αρχών ασφάλειας της παρ. 1 του ίδιου άρθρου.

2. Ο πάροχος καταρτίζει το ειδικό σχέδιο πολιτικής ασφάλειας και μεριμνά για την εφαρμογή του καθ` όλη τη διάρκεια λειτουργίας του ΣΔΙΔΕ.

3. Το ειδικό σχέδιο πολιτικής ασφάλειας καταρτίζεται, εφαρμόζεται, αξιολογείται και αναθεωρείται με βάση τουλάχιστον τον προσδιορισμό και την αποτίμηση των κινδύνων, το σχεδιασμό και την υλοποίηση των μέτρων ασφάλειας και τον έλεγχο εφαρμογής τους.

Άρθρο 4
Διαχωρισμός των δεδομένων

Χωρίς να απαιτείται η υλική υποδομή του ΣΔΙΔΕ να είναι φυσικά διαχωρισμένη από τα υπόλοιπα συστήματα του παρόχου, και με την επιφύλαξη του άρθρου 6 της παρούσας πράξης, ο πάροχος εφαρμόζει σε σχέση με όλες τις λειτουργίες του ΣΔΙΔΕ λογικό διαχωρισμό επί των δεδομένων του άρθρου 5 του ν. 3917/2011 ώστε να διασφαλίζεται ότι αυτά χρησιμοποιούνται μόνον για το σκοπό του νόμου αυτού. Λογικός διαχωρισμός υπάρχει όταν το λογισμικό, όλων των επιπέδων, που χρησιμοποιείται για πρόσβαση στα δεδομένα του ΣΔΙΔΕ είναι διακριτό και λογικά απομονωμένο από το λογισμικό που χρησιμοποιείται για πρόσβαση σε δεδομένα που τηρούνται για άλλους σκοπούς.

Άρθρο 5
Μέτρα σε σχέση με το προσωπικό

5.1. Υπεύθυνος ασφάλειας των δεδομένων του ΣΔΙΔΕ

1. Ο πάροχος οφείλει να ορίσει εγγράφως υπεύθυνο ασφάλειας των δεδομένων του ΣΔΙΔΕ, στον οποίο ανατίθεται η εποπτεία του ειδικού σχεδίου πολιτικής ασφάλειας. Προς τούτο ο υπεύθυνος ασφάλειας έχει πρόσβαση σε κάθε στοιχείο του ΣΔΙΔΕ που είναι αναγκαίο για την εκτέλεση των καθηκόντων του. Τα στοιχεία του υπευθύνου ασφάλειας των δεδομένων του ΣΔΙΔΕ γνωστοποιούνται αμελλητί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) και την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.).

2. Ο υπεύθυνος ασφάλειας των δεδομένων του ΣΔΙΔΕ πρέπει να διαθέτει τα κατάλληλα επαγγελματικά προσόντα για την εκτέλεση των καθηκόντων του, ιδίως αποδεδειγμένες γνώσεις και εμπειρία σχετικά με την ασφάλεια συστημάτων πληροφορικής.

5.2. Ρόλοι και δικαιώματα πρόσβασης στα δεδομένα του ΣΔΙΔΕ

1. Με την επιφύλαξη του άρθρου 12 της παρούσας πράξης ο πάροχος διασφαλίζει ότι πρόσβαση στα δεδομένα του ΣΔΙΔΕ έχουν αποκλειστικά και μόνον ο υπεύθυνος ασφάλειας και τα μέλη της ομάδας του ΣΔΙΔΕ.

2. Ο αριθμός των μελών της ομάδας του ΣΔΙΔΕ είναι ο ελάχιστος απαιτούμενος, προκειμένου να εξασφαλίζεται η ορθή και απρόσκοπτη λειτουργία του ΣΔΙΔΕ.

3. Ο πάροχος προβλέπει τους εξής διακριτούς ρόλους για τα μέλη της ομάδας ΣΔΙΔΕ:

(α) «Διαχειριστής ΣΔΙΔΕ»: πρόσωπο, αρμόδιο για τη διαμόρφωση, συντήρηση και υποστήριξη του ΣΔΙΔΕ και την υλοποίηση των μέτρων ασφάλειας αυτού.

(β) «Χειριστής ΣΔΙΔΕ»: πρόσωπο, αρμόδιο για τη χρήση των δεδομένων του. ΣΔΙΔΕ σύμφωνα με τις διατάξεις του ν. 3917/2011.

(γ) «Διαχειριστής αρχείων καταγραφής ΣΔΙΔΕ»: πρόσωπο, αρμόδιο για τη διαμόρφωση, συντήρηση και υποστήριξη του εξυπηρετητή ηλεκτρονικής καταγραφής συμβάντων και των μέτρων ασφάλειας αυτού. Ο ρόλος του διαχειριστή αρχείων καταγραφής ΣΔΙΔΕ είναι ασυμβίβαστος με άλλους ρόλους.

4. Τα μέλη της ομάδας του ΣΔΙΔΕ έχουν πρόσβαση μόνον στα υποσυστήματα και δεδομένα που είναι απαραίτητα για την εκτέλεση ενεργειών σύμφωνα με το ρόλο τους.

5.3. Καθήκον εχεμύθειας και κατάρτιση του προσωπικού

1. Ο πάροχος διασφαλίζει ότι ο υπεύθυνος ασφάλειας των δεδομένων του ΣΔΙΔΕ και τα μέλη της ομάδας του ΣΔΙΔΕ:

(α) συνδέονται με σχέση εργασίας με τον πάροχο,

(β) ασκούν τα καθήκοντα τους βάσει έγγραφης ανάθεσης,

(γ) τηρούν ως εμπιστευτική κάθε πληροφορία σχετικά με τη λειτουργία του ΣΔΙΔΕ, καθώς και οποιαδήποτε πληροφορία ή στοιχείο υποπίπτει στην αντίληψη τους ή την κατοχή τους, ως αποτέλεσμα του ρόλου τους,

(δ) είναι κατάλληλα και επαρκώς εκπαιδευμένοι σε σχέση με τις απαιτήσεις του ρόλου τους, και γνωρίζουν τις διαδικασίες και τα μέτρα ασφάλειας που εφαρμόζει ο πάροχος για την τήρηση των δεδομένων,

(ε) είναι ενημερωμένοι ως προς τις νομικές, τεχνικές και άλλες υποχρεώσεις που απορρέουν από το ρόλο τους.

Άρθρο 6
Μέτρα φυσικής ασφάλειας

1. Ο πάροχος λαμβάνει τα κατάλληλα μέτρα για την αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης στους τόπους εγκατάστασης του ΣΔΙΔΕ. Ειδικότερα:

(α). Οι τόποι εγκατάστασης του ΣΔΙΔΕ είναι καταγεγραμμένοι και περιορίζονται στον ελάχιστο δυνατό αριθμό.

(β) Οι τόποι εγκατάστασης του ΣΔΙΔΕ προστατεύονται με σύστημα ελεγχόμενης πρόσβασης, πόρτα ασφαλείας και σύστημα άμεσης ανίχνευσης μη εξουσιοδοτημένης πρόσβασης (όπως σύστημα ανίχνευσης κίνησης και συναγερμού).

(γ) Ο πάροχος τηρεί για τα δύο προηγούμενα έτη τα στοιχεία των προσώπων που έχουν δικαίωμα φυσικής πρόσβασης στους τόπους εγκατάστασης του ΣΔΙΔΕ, καθώς και περιγραφή του είδους του δικαιώματος πρόσβασης εκάστου εξ αυτών.

2. Η πρόσβαση στο υλικό του ΣΔΙΔΕ επιτρέπεται μόνον στον υπεύθυνο ασφάλειας και στα αρμόδια μέλη της ομάδας ΣΔΙΔΕ. Κατ` εξαίρεση, επιτρέπεται η πρόσβαση σε τρίτα πρόσωπα για την εκτέλεση εργασιών συντήρησης και υποστήριξης σύμφωνα με τα αναφερόμενα στο άρθρο 12 της παρούσας πράξης.

3. Οι τόποι εγκατάστασης του ΣΔΙΔΕ διαθέτουν ενσωματωμένα συστήματα κλιματισμού, πυρανίχνευσης, πυρασφάλειας, ανιχνευτών υγρασίας και πλημμύρας.

Άρθρο 7
Μέτρα λογικής ασφάλειας

7.1. Αναγνώριση και αυθεντικοποίηση

1. Ο πάροχος λαμβάνει τα κατάλληλα μέτρα για την αναγνώριση και την αυθεντικοποίηση του υπευθύνου ασφάλειας των δεδομένων και των μελών της ομάδας του ΣΔΙΔΕ, ώστε να αποτρέπεται η μη εξουσιοδοτημένη λογική πρόσβαση στα τηρούμενα δεδομένα.

Ειδικότερα:

(α) Η πρόσβαση πραγματοποιείται με χρήση αντίστοιχου λογαριασμού, ήτοι, ζεύγους ονόματος χρήστη και κωδικού πρόσβασης. Οι λογαριασμοί των χρηστών δημιουργούνται βάσει συγκεκριμένων κανόνων που περιλαμβάνουν τουλάχιστον την πολυπλοκότητα των κωδικών πρόσβασης (ελάχιστο μήκος και επιτρεπτούς χαρακτήρες), την ιστορικότητα τους και την συχνότητα αλλαγής τους. Οι χρήστες φροντίζουν για την ορθή χρήση των λογαριασμών που τους έχουν αποδοθεί. Ο λογαριασμός κάθε χρήστη προορίζεται για αποκλειστική χρήση από τον ίδιον.

(β). Ο πάροχος διατηρεί για τη χρονική περίοδο των δύο (2) προηγούμενων ετών, ενημερωμένο αρχείο, στο οποίο περιέχονται τουλάχιστον, τα ονόματα χρήστη, η ταυτότητα χρηστών και οι σχετικές ημερομηνίες δημιουργίας και κατάργησης των λογαριασμών πρόσβασης στο ΣΔΙΔΕ.

(γ) Ο πάροχος ορίζει το μέγιστο αριθμό ανεπιτυχών προσπαθειών λογικής πρόσβασης στο ΣΔΙΔΕ, πέραν του οποίου εκκινείται η διαδικασία χειρισμού περιστατικών παραβίασης δεδομένων του ΣΔΙΔΕ, σύμφωνα με το άρθρο 13 της παρούσας πράξης.

2. Η λογική πρόσβαση στο ΣΔΙΔΕ για κάθε λειτουργία, ήτοι χρήση, διαχείριση και έλεγχο, πραγματοποιείται από προκαθορισμένους και καταγεγραμμένους τερματικούς σταθμούς.

7.2. Δικτυακή Πρόσβαση

1. Η λογική πρόσβαση στο ΣΔΙΔΕ πραγματοποιείται αποκλειστικά μέσω έμπιστου δικτύου του παρόχου για το οποίο χρησιμοποιείται κρυπτογράφηση με ασφαλές μήκος κλειδιού βάσει διεθνώς αποδεκτών προτύπων.

2. Το μέλος της ομάδας του ΣΔΙΔΕ που αποκτά λογική πρόσβαση στο έμπιστο δίκτυο του παρόχου, διακόπτει κάθε σύνδεση στο σύστημα ΣΔΙΔΕ προ της απομάκρυνσης του από τον χρησιμοποιούμενο τερματικό εξοπλισμό. Οι συνδέσεις στο ΣΔΙΔΕ διακόπτονται αυτόματα σε περίπτωση που μείνουν ανενεργές για ορισμένο χρονικό διάστημα.

3. Η λογική πρόσβαση στο ΣΔΙΔΕ πρέπει να πραγματοποιείται μέσω προκαθορισμένου τερματικού εξοπλισμού, χωρίς να είναι δυνατή η πρόσβαση στο ΣΔΙΔΕ μέσω άλλων συστημάτων του παρόχου. Επίσης, δεν επιτρέπεται η εξαγωγή δεδομένων από το σύστημα ΣΔΙΔΕ (όπως με χρήση αποσπώμενων μέσων ή μέσω προγραμμάτων ηλεκτρονικού ταχυδρομείου) για σκοπούς διαφορετικούς από αυτούς του Α` Κεφαλαίου του ν. 3917/2011, με την επιφύλαξη των οριζόμενων στο άρθρο 9 της παρούσας πράξης.

Άρθρο 8
Κρυπτογράφηση δεδομένων

Τα τηρούμενα δεδομένα προστατεύονται με τη χρήση κατάλληλων κρυπτογραφικών μηχανισμών, βάσει διεθνώς αποδεκτών προτύπων. Το μήκος του σχετικού κλειδιού κρυπτογράφησης παρέχει προστασία και ασφάλεια από επιθέσεις και απειλές. Η διαχείριση των κλειδιών κρυπτογράφησης πραγματοποιείται με ασφάλεια εντός των εγκαταστάσεων του παρόχου. Κάθε κλειδί κρυπτογράφησης χρησιμοποιείται για ορισμένο χρονικό διάστημα και τηρείται όσο απαιτείται για τη διαχείριση των δεδομένων.

Άρθρο 9
Αντίγραφα ασφαλείας

1. Ο πάροχος διαθέτει συγκεκριμένη πολιτική δημιουργίας αντιγράφων ασφαλείας, η οποία περιλαμβάνει το χρόνο δημιουργίας των αντιγράφων, μέτρα για την ασφαλή αποθήκευση τους καθώς και μέτρα για τον έλεγχο της ορθής εξαγωγής τους (περιοδικός έλεγχος ακεραιότητας/αξιοπιστίας των αντιγράφων). Τα αντίγραφα ασφαλείας περιέχουν τις μεταβολές στις
οποίες υπόκεινται τα δεδομένα ή/και αυτούσια τα δεδομένα.

2. Τα αντίγραφα ασφαλείας αποθηκεύονται σε ασφαλή τόπο, σε διαφορετική τοποθεσία από τον τόπο δημιουργίας τους και φέρουν κατάλληλη περιγραφή, η οποία, ενδεικτικά, περιλαμβάνει την ημερομηνία λήψης του αντιγράφου, την προέλευση του (εφαρμογή, λειτουργικό σύστημα, δεδομένα δικτύου κλπ), το είδος (διαφορικό, αυξητικό ή πλήρες), το χρόνο αναφοράς του αντιγράφου (ημερήσιο, εβδομαδιαίο, μηνιαίο, ετήσιο) και αρίθμηση των τυχόν επιμέρους τμημάτων.

Άρθρο 10
Καταστροφή των δεδομένων

1. Ο πάροχος καταστρέφει με ασφαλή τρόπο τα τηρούμενα δεδομένα μετά το πέρας του προβλεπόμενου χρόνου τήρησης σύμφωνα με το άρθρο 6 του ν.3917/2011. Ως ασφαλής τρόπος καταστροφής των δεδομένων θεωρείται κάθε σύνολο αυτοματοποιημένων ή μη διαδικασιών και μέτρων που μετά από την ολοκλήρωση της εφαρμογής τους δεν επιτρέπει την αναγνώριση των υποκειμένων των δεδομένων. Η καταστροφή των δεδομένων είναι μη αναστρέψιμη, δηλαδή δεν είναι δυνατή η ανάκτηση των δεδομένων με τεχνικά ή άλλα μέσα.

2. Ο πάροχος μεριμνά για το σχεδιασμό, την καταγραφή, την τήρηση και τον περιοδικό έλεγχο της εφαρμογής της διαδικασίας καταστροφής των δεδομένων.

Άρθρο 11
Καταγραφή και παρακολούθηση συμβάντων

1. Ο πάροχος διατηρεί αναλυτικό σχέδιο αρχείων καταγραφής, το οποίο περιλαμβάνει τουλάχιστον: α) την αρχιτεκτονική και τις επιμέρους μεθόδους δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, β) πλήρη περιγραφή του περιεχομένου τους και γ) τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους.

2. Ο πάροχος εξασφαλίζει ότι, κατ` ελάχιστο, καταγράφονται τα ακόλουθα συμβάντα για χρονικό διάστημα δύο (2) ετών από την πραγματοποίηση τους:

α) Οι προσπάθειες φυσικής πρόσβασης (επιτυχείς και ανεπιτυχείς) στους τόπους εγκατάστασης του ΣΔΙΔΕ.

β) Οι προσπάθειες λογικής πρόσβασης (επιτυχείς και ανεπιτυχείς) στο ΣΔΙΔΕ.

γ) Οι ενεργείες/εντολές των χρηστών και διαχειριστών του ΣΔΙΔΕ.

δ) Οι μεταβολές στη διαμόρφωση του ΣΔΙΔΕ.

ε) Τα γεγονότα που αφορούν στην ασφάλεια, και. ιδίως όταν σχετίζονται με αλλαγές στην κατάσταση και στην λειτουργία του ΣΔΙΔΕ. Ενδεικτικά αναφέρονται τα ακόλουθα παραδείγματα: αποσύνδεση/διακοπή της δικτυακής σύνδεσης του ΣΔΙΔΕ, ανίχνευση σύνδεσης συστήματος με
δικτυακή διεύθυνση του ΣΔΙΔΕ, μη προγραμματισμένη επανεκκίνηση ή βίαιη διακοπή λειτουργίας του ΣΔΙΔΕ.

3. Τα συμβάντα της περίπτωσης α της προηγούμενης παραγράφου τηρούνται εγγράφως ή ηλεκτρονικά. Τα συμβάντα των περιπτώσεων β έως και ε της προηγούμενης παραγράφου τηρούνται ηλεκτρονικά σε ειδικό εξυπηρετητή καταγραφής συμβάντων (log server), διαφορετικό
από τους εξυπηρετητές από τους οποίους προέρχονται τα συμβάντα. Ο εξυπηρετητής χρησιμοποιείται από τον πάροχο αποκλειστικά για την τήρηση και διαχείριση αρχείων καταγραφής από το ΣΔΙΔΕ ή/και από άλλα συστήματα του παρόχου.

4. Ο πάροχος εξασφαλίζει ότι οι καταγραφές είναι πλήρεις, συνεχείς και προστατεύονται από οποιαδήποτε αλλοίωση και μη εξουσιοδοτημένη πρόσβαση. Οι εγγραφές για τα συμβάντα της περίπτωσης γ της παραγράφου 2 του παρόντος άρθρου κρυπτογραφούνται σύμφωνα με τα οριζόμενα στο άρθρο 8 της παρούσας πράξης.

5. Σε περίπτωση αποτυχίας καταγραφής συμβάντων ή δυσλειτουργίας του εξυπηρετητή καταγραφής συμβάντων, ενεργοποιείται μηχανισμός άμεσης ειδοποίησης του υπευθύνου ασφάλειας των δεδομένων του ΣΔΙΔΕ και εφαρμόζονται τα προβλεπόμενα στο άρθρο 13 της παρούσας πράξης μέτρα.

6. Ο πάροχος εφαρμόζει συστήματα παρακολούθησης και ενημέρωσης για συμβάντα, τα οποία είναι πιθανόν να οδηγήσουν στην εκδήλωση περιστατικού παραβίασης ασφάλειας. Ενδεικτικά, και όχι περιοριστικά, αναφέρονται οι επανειλημμένες ανεπιτυχείς προσπάθειες πρόσβασης, οι αλλαγές στη διαμόρφωση του ΣΔΙΔΕ, οι αλλαγές στην κατάσταση και τη λειτουργία του ΣΔΙΔΕ, όπως η επανεκκίνηση ή η βίαιη διακοπή λειτουργίας του ΣΔΙΔΕ.

Άρθρο 12
Ανάπτυξη, συντήρηση και υποστήριξη του ΣΔΙΔΕ

1. Οι εργασίες ανάπτυξης, συντήρησης και υποστήριξης του ΣΔΙΔΕ πραγματοποιούνται από μέλη της ομάδας του ΣΔΙΔΕ. Κατ` εξαίρεση οι παραπάνω εργασίες δύνανται να πραγματοποιούνται και από τρίτα πρόσωπα, υπό την επίβλεψη μέλους της ομάδας του ΣΔΙΔΕ και ύστερα από ειδική έγγραφη εξουσιοδότηση (άδεια πρόσβασης) του υπευθύνου ασφάλειας των δεδομένων του ΣΔΙΔΕ. Στην άδεια πρόσβασης καταγράφονται: α) ο σκοπός για τον οποίο παρέχεται πρόσβαση, β) το ονοματεπώνυμο και η ιδιότητα του προσώπου στο οποίο επιτρέπεται η πρόσβαση, γ) το χρονικό διάστημα για το οποίο επιτρέπεται η πρόσβαση και δ) το επιβλέπον μέλος της ομάδας ΣΔΙΔΕ. Ο υπεύθυνος ασφάλειας τηρεί μητρώο με τα στοιχεία των ανωτέρω αδειών,

2. Ο πάροχος τηρεί αρχείο, στο οποίο καταγράφεται ο εξοπλισμός του ΣΔΙΔΕ (υλικό, λογισμικό και τρέχουσα έκδοση αυτών), όλες οι εργασίες που λαμβάνουν χώρα στον εξοπλισμό αυτό βάσει της παραγράφου 1 του παρόντος άρθρου, οι αιτίες μεταβολής, τα πρόσωπα που τις πραγματοποιούν και οι εξουσιοδοτήσεις της παραγράφου 1. Σχετικά με το αρχείο αυτό ισχύουν τα προβλεπόμενα στην παράγραφο 2 του άρθρου 11 της παρούσας πράξης.

3. Ο πάροχος οφείλει να ελέγχει την αυθεντικότητα και ακεραιότητα του λογισμικού του ΣΔΙΔΕ, συμπεριλαμβανομένων των εκδόσεων αναβάθμισης και διορθώσεων του κώδικα.

4. Κατά τη διαδικασία απεγκατάστασης ή απενεργοποίησης εξοπλισμού (υλικού ή λογισμικού) του ΣΔΙΔΕ, ο πάροχος οφείλει να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση στα δεδομένα που έχουν εγγραφεί στον εν λόγω εξοπλισμό και, εφόσον απαιτείται, να προβαίνει στην ασφαλή καταστροφή του εξοπλισμού, σύμφωνα με τα οριζόμενα στο άρθρο 10 της παρούσας πράξης.

5. Στις περιπτώσεις που πραγματοποιείται ανάπτυξη λογισμικού, αυτό γίνεται σε περιβάλλον δοκιμών, το οποίο είναι απομονωμένο από το σύστημα ΣΔΙΔΕ. Τόσο κατά την ανάπτυξη του λογισμικού όσο και κατά την δοκιμή του τα χρησιμοποιούμενα δεδομένα είναι μη πραγματικά (dummy data).

Άρθρο 13
Διαχείριση περιστατικών παραβίασης ασφάλειας

1. Ο πάροχος αναπτύσσει και εφαρμόζει ειδική διαδικασία για τη διαχείριση των περιστατικών παραβίασης ασφάλειας. Η διαδικασία ορίζει κατ` ελάχιστο την καταγραφή των περιστατικών, τα μέτρα για την αντιμετώπιση τους και την επικαιροποίηση ή/και την απαραίτητη προσαρμογή της διαδικασίας χειρισμού περιστατικών παραβίασης ασφάλειας.

2. Η διαχείριση των περιστατικών γίνεται από τον υπεύθυνο ασφάλειας των δεδομένων του ΣΔΙΔΕ και τα μέλη της ομάδας ΣΔΙΔΕ.

3. Ο πάροχος τηρεί αρχείο με τα περιστατικά παραβίασης ασφάλειας για πέντε έτη από την καταγραφή του περιστατικού, εκτός και εάν σε σχέση με το περιστατικό οι αρμόδιες αρχές διενεργούν έρευνα ή το θιγόμενο πρόσωπο έχει αμφισβητήσει τη νομιμότητα των ενεργειών του παρόχου. Σε αυτήν την περίπτωση τα στοιχεία διαγράφονται μετά την αμετάκλητη επίλυση της υπόθεσης.

Άρθρο 14
Σχέδιο ανάκαμψης από καταστροφές

1. Ο πάροχος οφείλει να εκπονήσει σχέδιο ανάκαμψης από καταστροφές. Το σχέδιο περιγράφει τις βασικές διαδικασίες που ακολουθούνται για την προστασία των δεδομένων του ΣΔΙΔΕ σε περιπτώσεις έκτακτων περιστατικών. Ειδικότερα, το σχέδιο ορίζει τουλάχιστον τις συνθήκες ενεργοποίησής του, τους σχετικούς ρόλους και αρμοδιότητες του προσωπικού, καθώς και τους τρόπους αντιμετώπισης των περιστατικών. Περιλαμβάνει επίσης τη σχεδίαση δοκιμών και την περιοδική εκτέλεση τους. Το σχέδιο πρέπει να αναθεωρείται μετά από κάθε σημαντική αλλαγή στο ΣΔΙΔΕ αλλά και σε τακτική βάση.

Άρθρο 15
Εσωτερικός έλεγχος

Ο πάροχος προβαίνει σε εσωτερικούς ελέγχους για την τήρηση των υποχρεώσεων της παρούσας πράξης. Ο εσωτερικός έλεγχος πραγματοποιείται κατ` ελάχιστον κάθε τετράμηνο για τις προσβάσεις στα διατηρούμενα δεδομένα και κατά τα λοιπά ετησίως. Τα αποτελέσματα του ελέγχου καταγράφονται.

Άρθρο 16
Έναρξη ισχύος

Η ισχύς της παρούσας αρχίζει μετά την πάροδο εξαμήνου από τη δημοσίευσή της στην Εφημερίδα της Κυβερνήσεως.

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 18 Δεκεμβρίου 2013

Ο Πρόεδρος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) ΠΕΤΡΟΣ ΧΡΙΣΤΟΦΟΡΟΣ	Ο Πρόεδρος της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) ΑΝΔΡΕΑΣ ΛΑΜΠΡΙΝΟΠΟΥΛΟΣ