Αθήνα, 05-08-2016

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αριθ. Πρωτ.: Γ/ΕΞ/5003/05-08-2016

Α Π Ο Φ Α Σ Η ΑΡ. 75/2016

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε στην έδρα της την Τρίτη 19-07-2016 και ώρα 10:00, μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος της Αρχής, Πέτρος Χριστόφορος και τα τακτικά μέλη της Αρχής Λεωνίδας Κοτσαλής, Αναστάσιος-Ιωάννης Μεταξάς, Δημήτριος Μπριόλας και Αντώνιος Συμβώνης. Στη συνεδρίαση παρέστη ακόμα, μετά από εντολή Προέδρου, το αναπληρωματικό μέλος της Αρχής Παναγιώτης Ροντογιάννης, ως εισηγητής με δικαίωμα ψήφου. Τα τακτικά μέλη της Αρχής Κων/νος Χριστοδούλου και Πέτρος Τσαντίλας, παρόλο που εκλήθησαν νομίμως εγγράφως, δεν παρέστησαν λόγω κωλύματος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν επίσης, με εντολή του Προέδρου, οι Γεωργία Παναγοπούλου, Γεώργιος Ρουσόπουλος, Λεωνίδας Ρούσσος ειδικοί επιστήμονες-ελεγκτές, ως βοηθοί εισηγητή. Επίσης παρέστη, με εντολή του Προέδρου, η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στο πλαίσιο της άσκησης των αρμοδιοτήτων της, σύμφωνα με το άρθρο 19 παρ. 1 στοιχ. η' του νόμου 2472/1997 αποφάσισε τη διεξαγωγή διοικητικού ελέγχου στα αρχεία της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Διοικητικής Υποστήριξης (ΓΓΠΣ&ΔΥ) και της Γενικής Γραμματείας Δημοσίων Εσόδων (ΓΓΔΕ), με

αντικείμενο την προστασία δεδομένων προσωπικού χαρακτήρα κατά την επεξεργασία που πραγματοποιείται ιδίως μέσω των εφαρμογών του υποσυστήματος Μητρώου του Taxis και του Taxisnet. Εξεδόθη σχετικά η με αρ. πρωτ. Γ/ΕΞ/5442/22-10-2015 εντολή ελέγχου, βάσει της οποίας τον έλεγχο θα πραγματοποιήσουν οι εντεταλμένοι υπάλληλοι του Τμήματος Ελεγκτών της Γραμματείας της Αρχής Γεωργία Παναγοπούλου, Γεώργιος Ρουσόπουλος και Λεωνίδας Ρούσσος (εφεξής «ομάδα ελέγχου»).

Η Αρχή με το με αρ. πρωτ. Γ/ΕΞ/5499/26-10-2015 έγγραφο ενημέρωσε τον υπεύθυνο επεξεργασίας σχετικά με το αντικείμενο και τον τρόπο διεξαγωγής του ελέγχου, ακολουθώντας τις διαδικασίες της μεθοδολογίας ελέγχων της Αρχής. Για την καλύτερη προετοιμασία του ελέγχου, ζητήθηκε να προσδιοριστεί μία διεύθυνση ηλεκτρονικού ταχυδρομείου στην οποία η ομάδα ελέγχου θα αποστέλλει ερωτηματολόγια που σχετίζονται με το αντικείμενο του συγκεκριμένου ελέγχου. Επίσης, ζητήθηκε να υποδειχθεί εκπρόσωπος για κάθε Γενική Γραμματεία που θα είναι αρμόδιος για την επικοινωνία με την Αρχή για το συγκεκριμένο θέμα. Αφού επιστραφούν ηλεκτρονικά συμπληρωμένα τα ερωτηματολόγια, η Αρχή ενημέρωσε ότι θα διεξαγάγει επιτόπιο έλεγχο, κατά τον οποίο η ομάδα ελέγχου θα ζητήσει ενδεχομένως επιπλέον διευκρινίσεις και θα προβεί σε περαιτέρω απαιτούμενες ενέργειες ελέγχου.

Ο υπεύθυνος επεξεργασίας απάντησε σχετικά με το με αρ. πρωτ. … 2015 (ΑΠΔΠΧ Γ/ΕΙΣ/6025/19-11-2015) έγγραφο με το οποίο όρισε τη διεύθυνση ηλεκτρονικού ταχυδρομείου καθώς και τα αρμόδια πρόσωπα για επικοινωνία κατά τον έλεγχο. Η ομάδα ελέγχου με το με αρ. πρωτ. Γ/ΕΞ/6377/04-12-2015 έγγραφο απέστειλε ηλεκτρονικά ερωτηματολόγιο με 41 ερωτήσεις σχετικά με το αντικείμενο του ελέγχου.

Ο υπεύθυνος επεξεργασίας απάντησε στο ερωτηματολόγιο με το με αρ. πρωτ. … 2015 έγγραφο (ΑΠΔΠΧ Γ/ΕΙΣ/216/18-01-2016). Στη συνέχεια η ομάδα ελέγχου, αφού μελέτησε τις απαντήσεις του υπευθύνου επεξεργασίας απέστειλε το με αρ. πρωτ. Γ/ΕΞ/216-1/11-03-2016 έγγραφο με συνημμένο ερωτηματολόγιο με 28 ερωτήσεις προκειμένου να παρασχεθούν περαιτέρω διευκρινίσεις.

Ο υπεύθυνος επεξεργασίας με το με αρ. πρωτ. Γ/ΕΙΣ/1655/16-03-2016 αιτήθηκε παράταση μέχρι τις 29-4-2016 για την αποστολή των απαντήσεων επί των διευκρινιστικών ερωτήσεων. Η ομάδα ελέγχου με το με αρ. πρωτ. Γ/ΕΞ/1718/18-03-2016 έγγραφο ζήτησε η αποστολή των απαντήσεων να γίνει μέχρι τις 11-4-2016. Στη

συνέχεια ο υπεύθυνος επεξεργασίας με το με αρ. πρωτ. … 2016 έγγραφο (ΑΠΔΠΧ Γ/ΕΙΣ/2363/13-04-2016) ζήτησε νέα παράταση υποβολής των ζητούμενων διευκρινήσεων έως τις 22-4-2016, η οποία έγινε δεκτή με την παράκληση να είναι η τελευταία, όπως διευκρίνισε η ομάδα ελέγχου στο με αρ. πρωτ. Γ/ΕΞ/2378/13-04-2016 έγγραφό της. Με το με αρ. πρωτ. … 2016 … έγγραφο (αρ. πρωτ. Αρχής Γ/ΕΙΣ/2634/25-04-2016) ο υπεύθυνος επεξεργασίας απέστειλε τις απαντήσεις του στα διευκρινιστικά ερωτήματα. Στη συνέχεια, κατόπιν σχετικής συνεννόησης με τον υπεύθυνο επεξεργασίας, και αφού απεστάλη σχετικά το με αρ. πρωτ. Γ/ΕΞ/3142/18-05-2016 έγγραφο, προσδιορίστηκε η 30-5-2016 ως ημερομηνία συνάντησης στις εγκαταστάσεις του υπευθύνου επεξεργασίας με σκοπό την ολοκλήρωση του ελέγχου.

Στην εν λόγω συνάντηση εκπροσωπήθηκαν αρμοδίως τόσο η ΓΓΠΣ&ΔΥ όσο και η ΓΓΔΕ. Έγινε διεξοδική διαλογική συζήτηση σχετικά με τις απαντήσεις στα ερωτηματολόγια ελέγχου, ζητήθηκαν και δόθηκαν οι αναγκαίες διευκρινίσεις. Ο υπεύθυνος επεξεργασίας με το με αρ. πρωτ. Γ/ΕΙΣ/3601/07-06-2016 έγγραφο απέστειλε συμπληρωματικές διευκρινίσεις οι οποίες ζητήθηκαν κατά τη διάρκεια της συνάντησης από την ομάδα ελέγχου.

Στη συνέχεια, η ομάδα ελέγχου μελέτησε τα στοιχεία του ελέγχου και συνέταξε Πόρισμα, το οποίο υπέβαλε στην Αρχή με το υπ. αρ. πρωτ. Γ/ΕΙΣ/4518/18-7/2016 έγγραφο (εφεξής «Πόρισμα της ομάδας ελέγχου»). Στο Πόρισμα της ομάδας ελέγχου καταγράφονται μεταξύ άλλων τα ευρήματα αναφορικά με ελλιπή μέτρα ασφάλειας ή διαδικασίες προστασίας προσωπικών δεδομένων που εντοπίστηκαν, καθώς και οι προτεινόμενες από την ομάδα ελέγχου συστάσεις για την αντιμετώπιση των κινδύνων που δημιουργούνται.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου, αφού άκουσε τον εισηγητή και τις διευκρινίσεις των βοηθών εισηγητή, οι οποίοι αποχώρησαν μετά τη συζήτηση και πριν από τη διάσκεψη και τη λήψη αποφάσεως, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

Το άρθρο 10 του ν. 2472/1997 ορίζει ότι: *«1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του. 2. Για τη διεξαγωγή της επεξεργασίας ο*

υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. 3. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 1 ι' για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας. 4. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν».

Λαμβάνοντας υπόψη το χαρακτήρα των δεδομένων, δηλαδή τον όγκο και το είδος των δεδομένων που περιλαμβάνουν δημογραφικά και οικονομικά δεδομένα όλων των πολιτών της χώρας, καθώς και τις διεθνώς αποδεκτές πρακτικές (όπως τη σειρά του προτύπου ISO/IEC 27000) ως προς τις διαδικασίες και τα οργανωτικά, φυσικά και τεχνικά μέτρα ασφάλειας, η ομάδα ελέγχου εξέτασε την επάρκεια του επιπέδου ασφαλείας των δεδομένων σε συμμόρφωση με τις απαιτήσεις του αρ. 10 του ν. 2472/1997.

Η Αρχή με την απόφαση 98/2013, με αφορμή περιστατικό παραβίασης προσωπικών δεδομένων, επέβαλε στη Γενική Γραμματεία Πληροφοριακών Συστημάτων την κύρωση του προστίμου και παράλληλα συνέστησε την εφαρμογή κατάλληλων μέτρων ασφάλειας. Η συμμόρφωση στις συστάσεις αυτές αποτέλεσε επίσης αντικείμενο του ελέγχου.

Η ομάδα ελέγχου διαπίστωσε συγκεκριμένες ελλείψεις ή/και παραλείψεις του υπευθύνου επεξεργασίας αναφορικά με τα οργανωτικά και τεχνικά μέτρα ασφάλειας και προστασίας προσωπικών δεδομένων. Οι τομείς του ελέγχου στους οποίους ιδίως προέκυψαν ευρήματα ήταν οι εξής: ορισμός υπευθύνου επεξεργασίας, πολιτική και

σχέδιο ασφάλειας, υπεύθυνος προστασίας δεδομένων, σχέδιο ανάκαμψης από καταστροφές, διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων, διαχείριση πληροφοριακών αγαθών, διαχείριση χρηστών, δικαιώματα πρόσβασης και έλεγχος πρόσβασης, αρχεία καταγραφής ενεργειών, καταστροφή δεδομένων, διαχείριση αλλαγών, διαμόρφωση περιβάλλοντος υπολογιστών. Περιλήφθηκαν στον έλεγχο επίσης και τομείς για τους οποίους δεν εντοπίστηκαν συγκεκριμένες ελλείψεις ή/και παραλείψεις, όπως οι διαδικασίες ενημέρωσης και εκπαίδευσης χρηστών-υπαλλήλων του υπευθύνου επεξεργασίας καθώς και οι σχέσεις με εκτελούντες την επεξεργασία.

Μετά από εξέταση, σύμφωνα με τα παραπάνω, των ευρημάτων που αναφέρονται στο Πόρισμα της ομάδας ελέγχου, η Αρχή εγκρίνει τα ευρήματα και τις συστάσεις που προτείνονται στο επισυναπτόμενο εμπιστευτικό Πόρισμα του ελέγχου και αποφασίζει να αναφερθεί ειδικά στην ανάγκη και τον τρόπο συμμόρφωσης σε συγκεκριμένη προτεινόμενη σύσταση του Πορίσματος ελέγχου η οποία περιλαμβάνεται σε εμπιστευτικό Παράρτημα της παρούσας.

Λαμβάνοντας υπόψη ότι η πλειοψηφία των ευρημάτων που διαπιστώθηκαν αφορά σε έλλειψη πρόβλεψης, έγκρισης, τεκμηρίωσης διαδικασιών για επιμέρους ζητήματα, η Αρχή κρίνει το επίπεδο της ασφάλειας του υπευθύνου επεξεργασίας, ως προς την επεξεργασία προσωπικών δεδομένων, σχετικά ικανοποιητικό.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή απευθύνει σύσταση στον υπεύθυνο επεξεργασίας να συμμορφωθεί με τις συστάσεις που αναφέρονται στο επισυναπτόμενο εμπιστευτικό Πόρισμα του ελέγχου και το εμπιστευτικό Παράρτημα της παρούσας και να ενημερώνει την Αρχή σχετικά με την πρόοδο υλοποίησης των συστάσεων αυτών.

Ο Πρόεδρος της Αρχής **Η Γραμματέας**

Πέτρος Χριστόφορος **Ειρήνη Παπαγεωργοπούλου**