ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 21-06-2011

Αριθ. Πρωτ.: Γ/ΕΞ/4323/21-06-2011

Α Π Ο Φ Α Σ Η ΑΡ. 87/2011

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος στην έδρα της τη 10-05-2011 και ώρα 10:00 μετά από πρόσκληση του Αναπληρωτή Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Χρήστος Παληοκώστας, Αναπληρωτής Πρόεδρος και Δημήτριος Λιάππης, Πέτρος Τσαντίλας, και Γρηγόριος Λαζαράκος, ως εισηγητής, αναπληρωματικά μέλη σε αντικατάσταση των τακτικών μελών Λεωνίδα Κοτσαλή, Αναστάσιου Πράσσου και Αναστάσιου – Ιωάννη Μεταξά, οι οποίοι αν και εκλήθησαν νομίμως εγγράφως δεν παρέστησαν λόγω κωλύματος. Παρόντες χωρίς δικαίωμα ψήφου ήταν ο Λεωνίδας Ρούσσος και η Γεωργία Παναγοπούλου, πληροφορικοί ελεγκτές, ως βοηθοί εισηγητές και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Στην Αρχή υποβλήθηκε καταγγελία σχετικά με περιστατικό παραβίασης προσωπικών δεδομένων από το ΕΤΑΑ – Τομέας Υγειονομικών (πρώην «Ταμείο Συντάξεων και Αυτασφάλισης Υγειονομικών» - ΤΣΑΥ, εφεξής «υπεύθυνος επεξεργασίας»). Με την υπ' αριθμ. πρωτ. Γ/ΕΞ/4858-1/31-08-2010 εντολή του Προέδρου της Αρχής διατάχθηκε η διενέργεια ελέγχου στον υπεύθυνο επεξεργασίας. Ο έλεγχος πραγματοποιήθηκε την 1-9-2010 και την 6-9-2010 στα γραφεία του υπεύθυνου επεξεργασίας που βρίσκονται στην οδό Αχαρνών 27, στην Αθήνα.

Κατόπιν της διενέργειας του ελέγχου συντάχθηκε αρχικό πόρισμα, το οποίο απεστάλη στον υπεύθυνο επεξεργασίας για παρατηρήσεις με το υπ' αριθμ. πρωτ. Γ/ΕΞ/1164/14-02-2011 έγγραφο της Αρχής. Ο υπεύθυνος επεξεργασίας κατέθεσε τις παρατηρήσεις του με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1556/02-03-2011 έγγραφο. Το πόρισμα του διοικητικού ελέγχου υποβλήθηκε από την ομάδα ελέγχου στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2837/19-04-2011 εμπιστευτικό έγγραφο.

Η Αρχή, αφού άκουσε τον εισηγητή της υπόθεσης και έλαβε υπόψη όλα τα στοιχεία του φακέλου, μετά και από διεξοδική συζήτηση,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Όπως ορίζεται στο άρθρο 4, παρ. 1, εδ. α' του Ν. 2472/1997 τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.

2. Όπως ορίζεται στο άρθρο 10, παρ. 3 του Ν. 2472/1997 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.

3. Ως περιστατικό παραβίασης προσωπικών δεδομένων θεωρείται κάθε περίπτωση παραβίασης της ασφάλειας των δεδομένων στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

4. Το συγκεκριμένο περιστατικό αφορά στη διαρροή προσωπικών δεδομένων ορισμένων χρηστών (ασφαλισμένων) της εφαρμογής ηλεκτρονικών υπηρεσιών του υπεύθυνου επεξεργασίας σε άλλους χρήστες της ίδιας εφαρμογής. Ως εκ τούτου αποτελεί περιστατικό παραβίασης των προσωπικών δεδομένων των εν λόγω χρηστών, καθώς τα προσωπικά δεδομένα τους διέρρευσαν σε μη εξουσιοδοτημένα πρόσωπα.

5. Όπως προέκυψε από τον έλεγχο της Αρχής, το περιστατικό παραβίασης προσωπικών δεδομένων οφείλεται σε τεχνικό σφάλμα της εφαρμογής ηλεκτρονικών υπηρεσιών του υπεύθυνου επεξεργασίας, το οποίο οδήγησε στην αυτόματη αποστολή ηλεκτρονικών μηνυμάτων - ειδοποιήσεων σε κάποιους εγγεγραμμένους χρήστες της εφαρμογής που περιείχαν προσωπικά δεδομένα άλλων ασφαλισμένων.

Μετά από εξέταση των ευρημάτων που αναφέρονται στο πόρισμα του διοικητικού ελέγχου, η Αρχή ενέκρινε με ορισμένες τροποποιήσεις τις περιεχόμενες σε αυτό προτάσεις της ομάδας ελέγχου αναφορικά με τα τεχνικά και οργανωτικά μέτρα που πρέπει να ληφθούν από τον υπεύθυνο επεξεργασίας για την πρόληψη παρόμοιων περιστατικών παραβίασης προσωπικών δεδομένων στο μέλλον. Η αναλυτική παρουσίαση των ευρημάτων και συστάσεων καταγράφονται στο επισυναπτόμενο εμπιστευτικό τελικό πόρισμα του ελέγχου, το οποίο κοινοποιείται στον υπεύθυνο επεξεργασίας.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων απευθύνει με βάση το άρθρο 21 παρ. 1 στοιχ. α’ του ν. 2472/1997 προειδοποίηση στον υπεύθυνο επεξεργασίας να συμμορφωθεί με τις συστάσεις που αναφέρονται στο επισυναπτόμενο τελικό πόρισμα του ελέγχου και να ενημερώσει σχετικά την Αρχή εντός τριών (3) μηνών από την κοινοποίηση της παρούσας Απόφασης.

Ο Αναπληρωτής Πρόεδρος **Η γραμματέας**

Χρήστος Παληοκώστας **Ειρήνη Παπαγεωργοπούλου**