Αθήνα, 31-10-2014

Αριθ. Πρωτ.: Γ/ΕΞ/6617/31-10-2014

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Α Π Ο Φ Α Σ Η ΑΡ. 164/2014

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την 2-07-2014, σε συνέχεια της από 18-6-2014 τακτικής συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Π. Χριστόφορος, Πρόεδρος της Αρχής, τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Α.Ι. Μεταξάς, Δ. Μπριόλας, Α. Συμβώνης, Κ. Χριστοδούλου, Π. Τσαντίλας και το αναπληρωματικό μέλος της Αρχής Π. Ροντογιάννης, ως εισηγητής. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, η Γ. Παναγοπούλου ειδική επιστήμονας-ελέγκτρια, ως βοηθός εισηγητή και η Ε. Παπαγεωργοπούλου, υπάλληλος του Διοικητικού – Οικονομικού Τμήματος της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Με το με αρ. πρωτ. Γ/ΕΙΣ/1505/06-03-2014 έγγραφο ο Α (εφεξής «προσφεύγων») κατήγγειλε στην Αρχή ότι αποτελέσματα εξετάσεων αίματος που είχε πραγματοποιήσει στην «Βιοϊατρική ΑΕ» (στην διεύθυνση …) (εφεξής «υπεύθυνος επεξεργασίας») ενδέχεται να εστάλησαν μέσω ηλεκτρονικού ταχυδρομείο σε τρίτο πρόσωπο.

Συγκεκριμένα, ο προσφεύγων αναφέρει ότι πραγματοποίησε εξετάσεις αίματος και ζήτησε να σταλούν τα αποτελέσματα στη διεύθυνση ηλεκτρονικού ταχυδρομείου του. Σε τηλεφωνική επικοινωνία με τον υπεύθυνο επεξεργασίας ενημερώθηκε ότι τα αποτελέσματα είχαν μεν αποσταλεί, αλλά ο ίδιος δεν τα είχε λάβει. Ο προσφεύγων θεώρησε ότι ενδέχεται

τρίτος να είχε λάβει γνώση των αποτελεσμάτων.

Η Αρχή με το με αρ. πρωτ. Γ/ΕΞ/1505-1/27-03-2014 έγγραφό της ζήτησε τις ακόλουθες διευκρινίσεις από τον υπεύθυνο επεξεργασίας: σχετικά με:

1. Τον τρόπο και τον χρόνο κατά τον οποίο πληροφορήθηκε το περιστατικό και τις ενέργειες στις οποίες προέβη αμέσως μετά.

2. Τους λόγους που οδήγησαν στο περιστατικό.

3. Τη διαδικασία και τα μέτρα ασφάλειας που εφαρμόζει στην περίπτωση χρήσης του ηλεκτρονικού ταχυδρομείου ως μέσου για την αποστολή αποτελεσμάτων ιατρικών εξετάσεων.

4. Τα μέτρα που σκοπεύει να λάβει για την αποφυγή παρόμοιων περιστατικών στο μέλλον.

5. Εάν έχει ήδη αντιμετωπίσει παρόμοιο περιστατικό στο παρελθόν και σε ποιες ενέργειες προέβη.

Ο υπεύθυνος επεξεργασίας απάντησε με το με αρ. πρωτ. Γ/ΕΙΣ/2703/30-04-2014 έγγραφο στο οποίο αναφέρει συνοπτικά τα παρακάτω:

Η διαδικασία και τα μέτρα ασφάλειας στην περίπτωση αποστολής ιατρικών αποτελεσμάτων μέσω ηλεκτρονικού ταχυδρομείου, είναι η εξής:

Πρέπει να την έχει ζητήσει ο ίδιος ο πελάτης και μάλιστα γραπτώς, ήτοι με τη συμπλήρωση σχετικού εντύπου, το οποίο θα φέρει επίσης τον αριθμό της ταυτότητάς του και την υπογραφή του. Η αίτηση αυτή αρχειοθετείται σε ειδικό φάκελο.

Η αποστολή του σχετικού μηνύματος ηλεκτρονικού ταχυδρομείου γίνεται μόνο από τον ηλεκτρονικό υπολογιστή του υπεύθυνου της Μονάδας και στη συνέχεια εκτυπώνεται από τα απεσταλμένα και επισυνάπτεται στο φάκελο απαντήσεων του πελάτη. Το αρχείο απεσταλμένων δε σβήνεται, ενώ μια δεύτερη εκτύπωση αρχειοθετείται στον ειδικό φάκελο αρχειοθέτησης.

Για τη συγκεκριμένη, περίπτωση, ο υπεύθυνος επεξεργασίας αναφέρει τα εξής:

Ο προσφεύγων συμπλήρωσε χειρόγραφα τα στοιχεία του στο έντυπο της αίτησης. Τα αποτελέσματα των εξετάσεων εστάλησαν στην ηλεκτρονική διεύθυνση που ο ίδιος είχε αναγράψει στο έντυπο της αίτησής του, όμως ο κεντρικός διακομιστής ενημέρωσε με απαντητικό μήνυμα ότι δεν παραδόθηκε το μήνυμα ηλεκτρονικού ταχυδρομείου. Στη συνέχεια, κατόπιν τηλεφωνικής επικοινωνίας με τον ίδιο, προς επιβεβαίωση, απεστάλησαν πάλι τα αποτελέσματα στην ίδια ηλεκτρονική διεύθυνση, όμως για δεύτερη φορά ήρθε απαντητικό μήνυμα από τον κεντρικό διακομιστή ότι απέτυχε η αποστολή και το μήνυμα

ηλεκτρονικού ταχυδρομείου δεν παραδόθηκε.

Όταν ο προσφεύγων διαμαρτυρήθηκε τηλεφωνικά ότι τα αποτελέσματα εστάλησαν σε άλλη, λάθος διεύθυνση ηλεκτρονικού ταχυδρομείου αναζητήθηκαν όλα τα σχετικά στοιχεία και διαπιστώθηκε ότι τηρήθηκε η όλη διαδικασία σωστά.

Ο υπεύθυνος επεξεργασίας αναφέρει ότι δεν υπήρξε καμία διαρροή σε τρίτους των προσωπικών δεδομένων του προσφεύγοντος, δεδομένου ότι από το ιστορικό των απεσταλμένων μηνυμάτων (το οποίο και επισυνάπτεται στο απαντητικό έγγραφο) προκύπτει ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου που απεστάλησαν δεν παρελήφθησαν από κανέναν, ούτε από τον ίδιο τον προσφεύγοντα ούτε από οιονδήποτε τρίτο, καθώς απερρίφθησαν κατά την αποστολή διότι ο κεντρικός διακομιστής δεν κατάφερε να εντοπίσει την εν λόγω ηλεκτρονική διεύθυνση. Τέλος, επισημαίνεται ότι δεν έχει συμβεί ποτέ στο παρελθόν παρόμοιο περιστατικό.

Η Αρχή κάλεσε με το με αρ. πρωτ. Γ/ΕΞ/3559/03-06-2014 έγγραφο τον υπεύθυνο επεξεργασίας στη συνεδρίαση της Αρχής στις 18-6-2014. Η εταιρεία παρέστη δια του νομικού εκπροσώπου Β. Επίσης παρέστη και η Γ, μόνον ως ακροάτρια.

Ο υπεύθυνος επεξεργασίας έλαβε προθεσμία και κατέθεσε το με αρ. πρωτ. Γ/ΕΙΣ/4008/25-06-2014 υπόμνημα, στο οποίο αναφέρει συνοπτικά ότι ο προσφεύγων δεν υπέστη καμία βλάβη καθώς δεν διέρρευσαν προσωπικά του δεδομένα σε κανέναν τρίτο. Ενημερώνει ότι έλαβε πρόσθετα μέτρα προκειμένου να αποφευχθούν παρόμοια περιστατικά στο μέλλον. Συγκεκριμένα, πραγματοποιείται πλέον επαλήθευση από τον ασθενή της διεύθυνσης ηλεκτρονικού ταχυδρομείου, όπως έχει καταχωρηθεί ηλεκτρονικά από τη γραμματεία, καθώς και εκτύπωση και υπογραφή των στοιχείων του, όπως αυτά εμφανίζονται στο ηλεκτρονικό σύστημα.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων, αφού έγινε μνεία στα διαμειφθέντα κατά τη συνεδρίαση της 18-06-2014, άκουσε τον εισηγητή και τους βοηθούς εισηγητή, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Το άρθρο 10 του ν.2472/1997 καθιερώνει δύο θεμελιώδεις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων και καθορίζουν τη νομιμότητά της: την αρχή του απορρήτου και της ασφάλειας της επεξεργασίας. Βάσει των αρχών αυτών, ο υπεύθυνος επεξεργασίας βαρύνεται, μεταξύ άλλων, με την λήψη των κατάλληλων οργανωτικών και

τεχνικών μέτρων για την προστασία των προσωπικών δεδομένων από κάθε αθέμιτη επεξεργασία. 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.

Στη συγκεκριμένη περίπτωση:

Το αντικείμενο της επεξεργασίας περιλαμβάνει δεδομένα υγείας, δηλαδή ευαίσθητα προσωπικά δεδομένα, σύμφωνα με το άρθρο 2, εδ. β) του ν. 2472/1997, τα οποία από τη φύση τους χρήζουν υψηλού επιπέδου προστασίας.

Από την αίτηση του προσφεύγοντος για την αποστολή των αποτελεσμάτων των ιατρικών του εξετάσεων (προσκομίστηκε από τον υπεύθυνο επεξεργασίας, συνημμένο στο με αρ. πρωτ. Γ/ΕΙΣ/2703/30-04-2014 έγγραφο), προκύπτει ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου που συμπλήρωσε ο προσφεύγων μπορεί να αναγνωστεί με δύο τρόπους, διότι περιέχει ψηφίο το οποίο μπορεί να αναγνωστεί ως «0» (μηδέν) αλλά και ως «ο» (όμικρον) από το χειρόγραφό του.

Η σωστή ηλεκτρονική διεύθυνση, όπως αναφέρει ο προσφεύγων, είναι διαφορετική από εκείνη στην οποία ο υπεύθυνος επεξεργασίας απέστειλε, ανεπιτυχώς, τα αποτελέσματα, δύο φορές, με αποτέλεσμα ο διακομιστής να στείλει μήνυμα ανεπιτυχούς παράδοσης λόγω μη ύπαρξης της διεύθυνσης ηλεκτρονικού ταχυδρομείου. Η διαφορά ήταν ένα ψηφίο το οποίο καταχωρήθηκε λανθασμένα ως «ο» (όμικρον) ενώ ήταν «0» (μηδέν). Από το απορριπτικό μήνυμα που εστάλη από το διακομιστή ηλεκτρονικού ταχυδρομείου (συνημμένο στο με αρ. πρωτ. Γ/ΕΙΣ/2703/30-04-2014 έγγραφο), προκύπτει ότι η αποστολή των αποτελεσμάτων απέτυχε δύο φορές διότι ο διακομιστής ηλεκτρονικού ταχυδρομείου δεν βρήκε τη συγκεκριμένη ηλεκτρονική διεύθυνση. Δεν έχει προσκομιστεί κάποιο στοιχείο, για παράδοση του μηνύματος σε λάθος παραλήπτη, και σε συνδυασμό με το απορριπτικό μήνυμα προκύπτει ότι το μήνυμα δεν παραδόθηκε τελικά σε τρίτο.

Βεβαίως, η αποστολή σε λάθος διεύθυνση ηλεκτρονικού ταχυδρομείου (έστω και εάν ήταν όντως λάθος το ένα ψηφίο) θα μπορούσε να είχε οδηγήσει σε πρόσβαση τρίτου στα ευαίσθητα δεδομένα υγείας του προσφεύγοντος, εάν η διεύθυνση αυτή ήταν υπαρκτή και άνηκε σε τρίτο πρόσωπο.

Η διαδικασία που ακολουθεί ο υπεύθυνος επεξεργασίας, ήτοι γραπτή αίτηση για την αποστολή των μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου, και η τήρηση των αναγκαίων για την απόδειξη της αποστολής εγγράφων, δεν επαρκεί στην περίπτωση ανθρωπίνου λάθους κατά την πληκτρολόγηση της ηλεκτρονικής διεύθυνσης του παραλήπτη, κάτι που δεν μπορεί να αποκλειστεί ειδικά για παρόμοιους οπτικά χαρακτήρες. Για αυτό και θα πρέπει να

προστεθεί στα τηρούμενα μέτρα ασφάλειας η εξασφάλιση της εμπιστευτικότητας, των αποτελεσμάτων των ιατρικών εξετάσεων. Ειδικότερα, θα πρέπει να εξασφαλίζεται ότι, ακόμα κι αν συμβεί ανθρώπινο λάθος, τα ευαίσθητα δεδομένα προσωπικού χαρακτήρα θα είναι δυνατό να αναγνωστούν μόνο από τον πραγματικό αποδέκτη της επικοινωνίας.

Πρέπει εδώ να σημειωθεί ότι ένα μήνυμα ηλεκτρονικού ταχυδρομείου διέρχεται από διάφορους ενδιάμεσους κόμβους (διακομιστές ηλεκτρονικού ταχυδρομείου) και εν τέλει αποθηκεύεται στην προσωπική θυρίδα ηλεκτρονικού ταχυδρομείου, στο διακομιστή εισερχόμενης αλληλογραφίας του αποδέκτη. Αν και, τυπικά, η πρόσβαση σε αυτά τα σημεία δεν επιτρέπεται σε κανένα, δεν μπορεί να αποκλειστεί η δυνατότητα ανάγνωσης του μηνύματος από όσους έχουν τα κατάλληλα δικαιώματα (π.χ. διαχειριστές συστημάτων) ή σε περίπτωση περιστατικού παραβίασης δεδομένων. Συνεπώς, είναι σκόπιμο να διασφαλίζεται περαιτέρω ένα μήνυμα που περιέχει ευαίσθητα δεδομένα π.χ. με χρήση μεθόδων κρυπτογράφησης.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή απευθύνει αυστηρή προειδοποίηση στην «Βιοϊατρική ΑΕ» για τήρηση των επιταγών του άρθρου 10 του ν. 2472/1997 για το απόρρητο και την ασφάλεια της επεξεργασίας. Ειδικότερα, η αποστολή των αποτελεσμάτων των εξετάσεων ενδείκνυται να πραγματοποιείται με ασφαλή τρόπο, ιδίως σε κρυπτογραφημένη μορφή, σε αρχείο επισυναπτόμενο στο μήνυμα, με χρήση διεθνώς αποδεκτών προτύπων αλγορίθμων κρυπτογράφησης που μόνο ο παραλήπτης να μπορεί να αποκρυπτογραφήσει. Ο ασθενής μπορεί να λαμβάνει ισχυρό συνθηματικό αποκρυπτογράφησης με μέσο διαφορετικό του μηνύματος ηλεκτρονικού ταχυδρομείου (π.χ SMS, έγγραφο). Επίσης, ενδείκνυται να πραγματοποιείται επαλήθευση της καταχωρηθείσας στο πληροφοριακό σύστημα διεύθυνσης ηλεκτρονικού ταχυδρομείου από τον ίδιο τον ασθενή.

Ο Πρόεδρος **Η γραμματέας**

Πέτρος Χριστόφορος **Ειρήνη Παπαγεωργοπούλου**