ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 16/06/2011

Αριθ. Πρωτ.: Γ/ΕΞ/4220/16.06.2011

Α Π Ο Φ Α Σ Η ΑΡ. 60/2011

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος στην έδρα της την 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 τα αναπληρωματικά μέλη, Δημήτριος Λιάππης, ως εισηγητής, και Γρηγόριος Λαζαράκος, σε αντικατάσταση των τακτικών μελών Λεωνίδα Κοτσαλή και Αναστάσιου – Ιωάννη Μεταξά, οι οποίοι αν και εκλήθησαν νομίμως εγγράφως δεν παρέστησαν λόγω κωλύματος. Παρόντες χωρίς δικαίωμα ψήφου ήταν οι Ιωάννης Λυκοτραφίτης και Ανάργυρος Χρυσάνθου, 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:

Το Ινστιτούτο Υγείας του Παιδιού (εφεξής ΙΥΠ) ενημέρωσε την Αρχή, με το υπ' αριθμ. πρωτ. ……/2009 έγγραφό του (αριθμ. πρωτ. ΑΠΔΠΧ Γ/ΕΙΣ/2623/27-04-2009), σχετικά με παραβίαση προσωπικών δεδομένων, λόγω κλοπής, στις 8-04-2009, τεσσάρων (4) ηλεκτρονικών υπολογιστών από τη μονάδα του ΙΥΠ στην ……, στους οποίους ήταν καταχωρημένα ευαίσθητα προσωπικά δεδομένα υγείας των εξεταζόμενων παιδιών. Η κλοπή των εν λόγω υπολογιστών αναφέρθηκε και στο Τμήμα Ασφάλειας …… την ημέρα του συμβάντος (8-04-2009). Σε συνέχεια του

ως άνω εγγράφου, η Αρχή ζήτησε από το ΙΥΠ, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/2623-1/02-06-2009 έγγραφό της, να παράσχει περαιτέρω διευκρινίσεις αναφορικά με το συγκεκριμένο περιστατικό διαρροής προσωπικών δεδομένων. Ειδικότερα, το ΙΥΠ κλήθηκε να διευκρινίσει: *«α) τις κατηγορίες δεδο ένων που τηρούσε στους ηλεκτρονικούς υπολογιστές για τα παιδιά ή άλλα πρόσωπα (π.χ. ονο ατεπώνυ ο, η ερο ηνία γέννησης, εθνικότητα, η ερο ηνία εξέτασης, πάθηση, κτλ.), β) τον αριθ ό παιδιών, ή και άλλων προσώπων, των οποίων τα δεδο ένα ήταν καταχωρη ένα, γ) τα έτρα φυσικής και λογικής ασφάλειας που είχε λάβει και που ίσχυαν την η ερο ηνία του συ βάντος, δ) αν υπάρχει δυνατότητα αποκατάστασης των δεδο ένων που περιέχονταν στους κλε ένους υπολογιστές, είτε από το φυσικό αρχείο είτε από αντίγραφα ασφαλείας, ε) τυχόν έτρα που ελήφθησαν ύστερα από το συ βάν (π.χ. επιπλέον έτρα ασφαλείας) και στ) τυχόν άλλες ενέργειες στις οποίες προέβη το ΙΥΠ (π.χ. πιθανή ενη έρωση των γονιών των εν λόγω παιδιών)»*.

Το ΙΥΠ απάντησε στο ως άνω έγγραφο της Αρχής, με το υπ' αριθμ. πρωτ. ……../2009 έγγραφό του (αριθμ. πρωτ. ΑΠΔΠΧ Γ/ΕΙΣ/3940/23-6-2009), δηλώνοντας ότι:

1. Η κλοπή αφορούσε μόνον ηλεκτρονικά αρχεία της μονάδας του στην ……., ως ακολούθως:

- «*το ηλεκτρονικό αρχείο του πρωτοβάθ ιου παιδιατρικού ιατρείου, το οποίο περιέχει το ονο ατεπώνυ ο του παιδιού, την η ερο ηνία γέννησης, την εθνικότητα, τον ασφαλιστικό φορέα, αριθ ούς τηλεφώνων και την αιτία επίσκεψης στο Κέντρο Υγείας*
- *το ηλεκτρονικό αρχείο της κοινωνικής λειτουργού, το οποίο περιέχει το ονο ατεπώνυ ο του παιδιού, την η ερο ηνία γέννησης, την εθνικότητα, τον ασφαλιστικό φορέα, αριθ ούς τηλεφώνων, την αιτία επίσκεψης στο Κέντρο Υγείας και τις εκθέσεις της οικογενειακής κατάστασης των περιπτώσεων που κατατίθενται σε υπηρεσίες ή άλλους φορείς (πχ. σύλλογοι ή σω ατεία, κλπ.) για τη χορήγηση επιδο άτων*
- *το ηλεκτρονικό αρχείο του αναπτυξιακού ιατρείου, το οποίο περιέχει κυρίως τις βεβαιώσεις ε την εκτί ηση των αναγκών του παιδιού σε θεραπείες»*

2. Στα παραπάνω ηλεκτρονικά αρχεία τηρούνταν προσωπικά δεδομένα 2050 παιδιών.

3. Το ΙΥΠ είχε λάβει ορισμένα μέτρα φυσικής (συναγερμός) και λογικής ασφάλειας (λήξη εβδομαδιαίων αντιγράφων ασφαλείας, χρήση προσωπικών συνθηματικών ανά υπολογιστή, αντιϊκό πρόγραμμα) για την προστασία τόσο των τηρούμενων δεδομένων όσο και του πληροφοριακού εξοπλισμού του. Παρά ταύτα, ο συναγερμός δε λειτούργησε την ημέρα του περιστατικού.

4. Το ΙΥΠ ανέκτησε τα δεδομένα που περιέχονταν στους κλεμμένους υπολογιστές από τα αντίγραφα ασφάλειας, τα οποία τηρούσε, και προέβη σε ενημέρωση των γονέων των παιδιών αναφορικά με το περιστατικό. Επίσης, έλαβε επιπλέον μέτρα λογικής ασφάλειας (χρήση συνθηματικών σε ηλεκτρονικά αρχεία ασθενών, προφύλαξη οθόνης με συνθηματικό, λήψη τριμηνιαίων αντιγράφων ασφαλείας) και φυσικής ασφάλειας (φύλαξη των αντιγράφων ασφαλείας σε ειδικό χώρο) για την προστασία των προσωπικών δεδομένων, τα οποία τηρούνται στην μονάδα του στην ……..

Η Αρχή έχει χορηγήσει στο ΙΥΠ με το υπ' αριθμ. πρωτ. ΓΝ/ΕΞ/2794/28-11-2003 έγγραφό της άδεια ίδρυσης και λειτουργίας αρχείου με ευαίσθητα δεδομένα για το σκοπό της παροχής των υπηρεσιών του εργαστηριακού ελέγχου και θεραπείας σπάνιων νοσημάτων νεογνών και παιδιών. Η Αρχή έχει επίσης χορηγήσει στο ΙΥΠ με το ΓΝ/ΕΞ/2795/28-11-2003 έγγραφό άδεια ίδρυσης και λειτουργίας αρχείου με ευαίσθητα δεδομένα για το σκοπό της παροχής των υπηρεσιών της κοινωνικής και αναπτυξιακής παιδιατρικής, ψυχικής υγείας, πρωτοβάθμιας φροντίδας, προαγωγής της υγείας και της ποιότητας ζωής του κακοποιούμενο παιδιού και της οικογένειας του. Και ο δύο χορηγηθείσες άδειες περιέχουν συγκεκριμένους όρους που αφορούν το απόρρητο και την ασφάλεια της επεξεργασίας, οι οποίοι περιλαμβάνουν και την εκπόνηση και εφαρμογή πολιτικής και σχεδίου ασφαλείας από το ΙΥΠ. Οι άδειες αυτές ανανεώθηκαν με το ΓΝ/ΕΞ/1370/26-11-2010 έγγραφο της Αρχής μέχρι τις 20-11-2015.

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. Το άρθρο 4, παρ. 1, στοιχ. α' του ν. 2472/1997 ορίζει ότι 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. Το άρθρο 10, παρ. 3 του ν. 2472/1997 ορίζει ότι 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 που ανέφερε το ΙΥΠ στην Αρχή αποτελεί περιστατικό παραβίασης των προσωπικών δεδομένων των παιδιών που είχαν επισκεφτεί το κέντρο, καθώς τα εν λόγω δεδομένα διέρρευσαν –λόγω της κλοπής των μέσων επεξεργασίας – σε μη εξουσιοδοτημένα πρόσωπα. Η βαρύτητα του περιστατικού αυξάνεται από το γεγονός ότι α) τα δεδομένα που διέρρευσαν περιέχουν και δεδομένα υγείας, δηλαδή ευαίσθητα προσωπικά δεδομένα κατά την έννοια του αρ. 2 στοιχ. β ν. 2472/1997, β) το περιστατικό αφορά μεγάλο αριθμό ατόμων (2050 παιδιά που ήταν καταχωρημένα στα αρχεία του κέντρου).

5. Σύμφωνα με τα στοιχεία του περιστατικού που αναφέρθηκαν στην Αρχή, προκύπτει ότι το περιστατικό οφείλεται στην ανεπάρκεια των μέτρων φυσικής και λογικής ασφάλειας του ΙΥΠ. Πιο συγκεκριμένα, ως προς τη φυσική ασφάλεια, το υπάρχον σύστημα συναγερμού δεν λειτούργησε κατά τη χρονική στιγμή του περιστατικού, ενώ δεν υπήρχε επαρκής έλεγχος της φυσικής πρόσβασης στους χώρους επεξεργασίας των ευαίσθητων προσωπικών δεδομένων. Ως προς τη λογική ασφάλεια, όπως δήλωσε το ΙΥΠ, οι χρήστες του χρησιμοποιούσαν προσωπικά συνθηματικά για το άνοιγμα του σταθμού εργασίας τους, λαμβανόταν αντίγραφο ασφαλείας σε εβδομαδιαία βάση και χρησιμοποιούταν αντιϊκό πρόγραμμα σε όλους τους υπολογιστές. Παρόλα αυτά, από τα στοιχεία που γνωστοποιήθηκαν στην Αρχή, δεν φαίνεται να υπήρχε επαρκής διαδικασία διαχείρισης των χρηστών και των συνθηματικών των συστημάτων επεξεργασίας, με αποτέλεσμα να μην είναι ασφαλής

η διαδικασία αυθεντικοποίησης των χρηστών στα αρχεία των προσωπικών δεδομένων. Περαιτέρω, το ΙΥΠ δεν είχε λάβει ειδικότερα μέτρα ασφαλείας, όπως κρυπτογράφηση των σκληρών δίσκων των υπολογιστών, οι οποίοι χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων, ώστε να καθίστανται τα δεδομένα ακατάληπτα σε μη εξουσιοδοτημένους χρήστες. Τα ανωτέρω διευκολύνουν την μη εξουσιοδοτημένη πρόσβαση στα παραπάνω δεδομένα.

6. Παρά τις ανωτέρω ελλείψεις, το ΙΥΠ έλαβε αμέσως μέτρα για την αντιμετώπιση του περιστατικού. Ειδικότερα, μετά τη διαπίστωση του περιστατικού το γνωστοποίησε στην Αρχή. Περαιτέρω, το ΙΥΠ προέβη στη λήψη επανορθωτικών/διορθωτικών μέτρων (αναφορά στην αστυνομία, ανάκτηση δεδομένων από αντίγραφα ασφάλειας και ενημέρωση των γονέων των παιδιών, τα οποία αφορούσαν τα δεδομένα), ενώ παράλληλα έλαβε νέα μέτρα για την ενίσχυση της λογικής ασφάλειας των ηλεκτρονικών αρχείων που τηρεί.

7. Λαμβάνοντας υπόψη όλα τα παραπάνω καθώς και ότι δεν είχε συμβεί παρόμοιο περιστατικό παραβίασης προσωπικών δεδομένων στις εγκαταστάσεις του ΙΥΠ στο παρελθόν, προκύπτει ότι το ΙΥΠ, αν και παραβίασε το άρθρο 10 παρ. 3 ν. 2472/1997, περιόρισε κατά το δυνατόν την έκταση της διαρροής των δεδομένων και έλαβε μέτρα για την αντιμετώπιση παρόμοιων προβλημάτων στο μέλλον.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα απευθύνει στο ΙΥΠ με βάση το άρθρο 21 παρ. 1 στοιχ. α’ του Ν. 2472/1997 προειδοποίηση να λάβει κατ’ ελάχιστο τα οργανωτικά και τεχνικά μέτρα ασφάλειας, τα οποία περιλαμβάνονται στο επισυναπτόμενο εμπιστευτικό Παράρτημα της παρούσας Απόφασης, 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**