ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ Ε ΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 08-01-2015

Αριθ. Πρωτ.: Γ/ΕΞ/51/08-01-2015

Α Π Ο Φ Α Σ Η ΑΡ. 1 / 2015

Η Αρχή Προστασίας εδομένων Προσωπικού Χαρακτήρα συνήλθε, μετά από πρόσκληση του Προέδρου της, σε τακτική συνεδρίαση στην έδρα της την 16-12-2014, σε συνέχεια της από 07-10-2014 συνεδρίασης, προκειμένου να εξετάσει την υπόθεση του αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος, Π. Χριστόφορος και τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Α.-Ι. Μεταξάς, . Μπριόλας, Α. Συμβώνης, ως εισηγητής, Κ. Χριστοδούλου και Π. Τσαντίλας. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν επίσης, με εντολή του Προέδρου, ο Γ. Ρουσόπουλος, ειδικός επιστήμονας–ελεγκτής, ως βοηθός εισηγητή, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/62/07-01-2013 έγγραφό της η Υποδιεύθυνση ίωξης Ηλεκτρονικού Εγκλήματος (ΗΕ) ζήτησε τη συνδρομή της Αρχής σε έρευνά της στην εταιρεία «InfoCredit A.E.». Μετά τη διενέργεια του ελέγχου τα συλλεχθέντα ψηφιακά πειστήρια ζητήθηκαν από την ΗΕ με τα υπ' αριθμ. πρωτ. Γ/ΕΞ/914/11-02-2013 και Γ/ΕΞ/1750/08-03-2013 έγγραφα της Αρχής και χορηγήθηκαν στην Αρχή με τα υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2712/17-04-2013 και Γ/ΕΙΣ/2856/22-04-2013 έγγραφα της ιεύθυνσης Εγκ/κων Ερευνών της Ελληνικής Αστυνομίας, κατόπιν έγκρισης των αρμόδιων εισαγγελικών και ανακριτικών αρχών.

Από την εξέταση των ψηφιακών πειστηρίων διαπιστώθηκε ότι σε αυτά περιέχονταν προσωπικά δεδομένα μεγάλου αριθμού συνδρομητών της «Οργανισμός Τηλεπικοινωνιών της Ελλάδος Α.Ε.» (εφεξής ΟΤΕ και υπεύθυνος επεξεργασίας).

Συγκεκριμένα βρέθηκαν πίνακες βάσης δεδομένων με ονόματα και λοιπά προσωπικά δεδομένα συνδρομητών του ΟΤΕ, ως εξής:

α. Πίνακες «ote08_subscriptions», «ote09_subscriptions», «ote10a_subscriptions» και «ote10_subscriptions» με 5.434.349, 4.671.389, 4.620.797 και 4.563.422 στοιχεία συνδρομών αντίστοιχα. Τα στοιχεία αυτά περιλαμβάνουν κωδικούς συνδρομής και συνδρομητή, αριθμό τηλεφώνου, κωδικούς προσφερόμενης υπηρεσίας, διεύθυνση, την πληροφορία για το αν η συνδρομή είναι ενεργή ή όχι και την πληροφορία για το αν ο αριθμός τηλεφώνου είναι ανακοινώσιμος σε καταλόγους ή όχι (απόρρητος).

β. Πίνακας «ote_customers» με 8.453.783 εγγραφές όπου περιέχονται προσωπικά δεδομένα συνδρομητών του ΟΤΕ (κωδικός συνδρομητή, ονοματεπώνυμο, όνομα πατρός, ημερομηνία γέννησης, Α.Φ.Μ., στοιχεία δελτίου ταυτότητας, διεύθυνση και έτος.

γ. Πίνακας «ote_epagelma» με 3.969.568 εγγραφές, όπου τηρείται η αντιστοιχία Α.Φ.Μ. και επαγγέλματος.

δ. Πίνακας «ote_products» με 601 εγγραφές όπου τηρούνται πληροφορίες για τα προϊόντα ή τις υπηρεσίες στις οποίες αφορά η κάθε συνδρομή.

Η Αρχή απέστειλε με το υπ' αριθμ. πρωτ. Γ/ΕΞ/5522/28-08-2013 έγγραφο αντίγραφο των σχετικών ψηφιακών πειστηρίων μαζί με συνοπτική περιγραφή τους στον ΟΤΕ ζητώντας τις απόψεις της εταιρείας. Ο ΟΤΕ απάντησε με το υπ' αριθμ. πρωτ. …/…-…-2013 έγγραφό του (αρ. πρωτ. Αρχής Γ/ΕΙΣ/7599/27-11-2013) επισημαίνοντας τα εξής: α) ότι από την ανάλυση των στοιχείων εκτιμούν ότι τα δεδομένα που περιέχονται στους πίνακες «ote_subscriptions», «ote_customers», «ote_epaggelma» και «ote_products» αφορούν την περίοδο 2008 έως και Μάιο 2010, β) ότι δεν αποτελούν ακριβές αντίγραφο βάσης δεδομένων του ΟΤΕ, και γ) ότι κατά το χρονικό διάστημα αυτό ο ΟΤΕ ελάμβανε τα κατάλληλα και απαιτούμενα για την ασφαλή διαχείριση των βάσεων δεδομένων και συστημάτων του οργανωτικά και τεχνικά μέτρα με σκοπό την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Για το τελευταίο αναφέρει ειδικότερα ότι στις βάσεις δεδομένων και στα συστήματά του εφαρμοζόταν περιορισμένη και προσωποποιημένη πρόσβαση για την εξυπηρέτηση συγκεκριμένων σκοπών (π.χ. έκδοση λογαριασμών). Όλες οι προσβάσεις παρέχονταν από ένα κεντρικό πληροφοριακό σύστημα (Κεντρικό Σύστημα ιαχείρισης Πρόσβασης) το οποίο κατόπιν αντικαταστάθηκε από σύστημα διαχείρισης

ταυτότητας (Identity Management). Με τον τρόπο αυτό καταγράφεται ποιος ζητούσε πρόσβαση, ποιος την ενέκρινε και πότε. Σε επίπεδο βάσης δεδομένων γινόταν καταγραφή των προσβάσεων των χρηστών (συνδέσεις/αποσυνδέσεις και αποτυχημένες προσπάθειες σύνδεσης). Τα αρχεία καταγραφής διατηρούνται για δύο (2) έτη, σύμφωνα με τον Κανονισμό της Α ΑΕ για τη ιασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών. Καθώς το περιστατικό αφορούσε σε χρόνο μεγαλύτερο των δύο ετών, δεν κατέστη δυνατός ο έλεγχος των αρχείων καταγραφής. Επιπλέον αναφέρει ότι υπήρχε διαχωρισμός δικτύων σε λογικό επίπεδο και ελεγχόμενη φυσική πρόσβαση στα κτήρια του ΟΤΕ και στα Κέντρα εδομένων που βρίσκονται οι εξυπηρετητές του. Τέλος, ο ΟΤΕ ανέφερε ότι η διαδικασία διασφάλισης των δεδομένων των πελατών είναι μια διαρκώς εξελισσόμενη και αναβαθμιζόμενη διαδικασία και περιγράφει τις ενέργειές του προς το σκοπό αυτό.

Μετά την εξέταση της ανωτέρω απάντησης η Αρχή απέστειλε νεώτερη επιστολή (υπ' αριθμ. πρωτ. Γ/ΕΞ/1034/17-02-2014), ζητώντας περαιτέρω διευκρινίσεις. Ο ΟΤΕ απάντησε εκ νέου με το υπ' αριθμ. πρωτ. …/…-…-2014 έγγραφό του (αρ. πρωτ. Αρχής Γ/ΕΙΣ/2085/01-04-2014) επισημαίνοντας τα εξής: α) Ότι πέραν της καταγραφής του συνόλου των προσβάσεων εφαρμόζει κανόνες περιορισμένης και προσωποποιημένης πρόσβασης σε βάσεις δεδομένων για την εξυπηρέτηση συγκεκριμένων σκοπών από περιορισμένο αριθμό ειδικά εξουσιοδοτημένων ατόμων. Κατά το χρόνο απάντησης είναι σε εξέλιξη διαδικασία εγκατάστασης συστήματος αποφυγής μαζικής μεταφόρτωσης δεδομένων (DLP). β) Ότι έγινε η πλέον επιστάμενη και εκτεταμένη εσωτερική έρευνα, αλλά δεδομένης της μη ύπαρξης αρχείων καταγραφής δεν ήταν δυνατή η εξαγωγή ασφαλών συμπερασμάτων. γ) Ότι οι κατηγορίες δεδομένων (πεδία) customer, account_num, product_id και product_seq περιέχουν στοιχεία που υπάρχουν σε βάσεις δεδομένων του ΟΤΕ ενώ το πεδίο subs-id δεν υπάρχει με τη μορφή που βρέθηκε στα ψηφιακά πειστήρια. Αντίθετα οι πίνακες ote_subscriptions δεν υφίστανται στις βάσεις του ΟΤΕ με αυτή τη μορφή και αποτελούν προϊόν συνδυαστικής αναζήτησης (ερωτήματα - queries) δεδομένων από διαφορετικούς πίνακες ενώ αφορούν σε συγκεκριμένα προϊόντα τηλεφωνίας της εταιρείας. δ) Ότι σε στοιχεία όπως αυτά του περιστατικού δύναται να έχουν πρόσβαση οι αρμόδιοι υπάλληλοι του ΟΤΕ ή/και εξωτερικοί συνεργάτες με τους οποίους συνάπτονται συμβάσεις εμπιστευτικότητας. Ωστόσο, πρόσβαση στο σύνολο των δεδομένων που χορηγήθηκαν είχαν μόνο οι εργαζόμενοι του ΟΤΕ που απασχολούνται ως διαχειριστές βάσεων δεδομένων και καθώς και

περιορισμένος αριθμός προσωπικού συνεργαζόμενων εταιρειών. Ο ΟΤΕ επισημαίνει ότι η συνδρομή εξωτερικών συνεργατών είναι απαραίτητη τόσο για την επίλυση τεχνικών προβλημάτων όσο και για την ανάπτυξη νέων εφαρμογών. ε) Ότι προχώρησε σε λεπτομερή έρευνα και ανάλυση για το συγκεκριμένο περιστατικό για πάνω από δύο μήνες. Ελέγχθηκαν εφαρμογές, βάσεις και διασυνδέσεις συστημάτων. ημιουργήθηκε δοκιμαστικό περιβάλλον εφαρμογών και δεδομένων για το έτος 2010. Επιπλέον υλοποιήθηκε διαδικασία αναπαραγωγής του περιβάλλοντος του περιστατικού για να εκτιμηθεί ο χρόνος και ο τρόπος που απαιτείται για να παραχθούν πίνακες με στοιχεία παρόμοια με αυτά των ευρεθέντων αρχείων. Η έλλειψη αρχείων καταγραφής, λόγω της παρόδου του χρόνου τήρησης τους, είχε ως επακόλουθο την αδυναμία απόδειξης ή ασφαλούς ένδειξης για τη συνδρομή γεγονότων και την ύπαρξη εμπλεκομένων προσώπων.

Εν όψει της συνεδρίασης της 7/10/2014 κατατέθηκαν από τον ΟΤΕ (με το υπ' αριθμ' πρωτ. Γ/ΕΙΣ/5733/26-09-2014 έγγραφό του) αντίγραφα της πολιτικής ασφάλειας και λοιπών συναφών κειμένων, τόσο στη μορφή που ήταν εν ισχύ κατά το διάστημα που εκτιμάται ότι συνέβη το περιστατικό παραβίασης προσωπικών δεδομένων, όσο και στην ισχύουσα κατά το χρόνο της ακρόασης. Με το έγγραφό αυτό μάλιστα, ο ΟΤΕ επισημαίνει ότι βελτιώνει συνεχώς τα μέτρα ασφάλειας που εφαρμόζει και τις σχετικές με αυτά διαδικασίες λαμβάνοντας τα πλέον σύγχρονα τεχνικά μέτρα ενίσχυσης της ασφάλειας και της προστασίας των δεδομένων των πελατών του. Τα μέτρα αυτά περιγράφονται αναλυτικά.

Κατά τη διενέργεια διοικητικού ελέγχου της Αρχής στον ΟΤΕ κατά το έτος 2009, στο πλαίσιο της κοινής δράσης έρευνας για την εφαρμογή των Οδηγιών της Ε.Κ. για την τήρηση δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών (2006/24/ΕΚ) και την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών (2002/58/ΕΚ) ο ΟΤΕ χορήγησε στην Αρχή αντίγραφο της τότε ισχύουσας πολιτικής ασφάλειας (υπ' αριθμ. πρωτ. Γ/ΕΙΣ/7428/10-12-2009). Σε αυτό περιέχεται η έκδοση 1.1/21-11-2006 της Πολιτικής Πρόσβασης όπου αναφέρονται στην παρ. 3.4.2 «*Διαδικασίες ελέγχου διαδικασιών διαχείρισης πρόσβασης*» αναφέρεται μεταξύ άλλων ότι «*…Ο έλεγχος των διαδικασιών βασίζεται και στα αρχεία καταγραφής συμβάντων που προέρχονται από τα κρίσιμα συστήματα του Οργανισμού. Όλα τα συστήματα και οι εφαρμογές που διαχειρίζονται ευαίσθητα δεδομένα δημιουργούν αρχεία καταγραφής συμβάντων που καταγράφουν κάθε ενέργεια εισαγωγής, τροποποίησης και διαγραφής των δεδομένων αυτών ή δικαιωμάτων*

χρηστών, τις συνδέσεις των χρηστών και την ταυτότητά τους, την ώρα και την ημερομηνία σύνδεσης και αποσύνδεσης από το σύστημα καθώς και τις εφαρμογές που χρησιμοποιήθηκαν, την εκκίνηση και τον τερματισμό των συστημάτων….» Επίσης, στην υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/1495/23-12-2010 γνωστοποίησή του ο ΟΤΕ επισύναψε αντίγραφο της ιαδικασίας Ελέγχου ικαιωμάτων Πρόσβασης (συγκεκριμένα: έκδοση 1.4/12-11-2010). Σε αυτή προβλέπεται διαδικασία συστηματικού ελέγχου της εξουσιοδοτημένης πρόσβασης η οποία πρέπει να εκτελείται τουλάχιστον κάθε 6 μήνες. Παρόμοιες κατάλληλες προβλέψεις για τους ελέγχους ασφάλειας και πρόσβασης υπάρχουν και στις νεώτερες πολιτικές του ΟΤΕ[1]. Κατόπιν της συνεδρίασης της 07-11-2014 ο ΟΤΕ κατέθεσε το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6463/27-10-2014 υπόμνημα. Σε αυτό υποστηρίζει συνοπτικά τα εξής: α) Ότι ουδέποτε διαβίβασαν μαζικά δεδομένα σε τρίτους. β) Ότι το συγκεκριμένο περιστατικό διερευνήθηκε διεξοδικά (όπως ήδη περιγράφηκε στο προηγούμενό του υπόμνημα). γ) Ότι το σύνολο των δεδομένων ήταν καταχωρημένα μόνο στη κεντρική βάση δεδομένων τιμολόγησης του ΟΤΕ για την οποία γινόταν επιβεβαίωση των δικαιωμάτων πρόσβασης σε εξαμηνιαία βάση σε εφαρμογή και της νομοθεσίας Sarbannes-Oxley των Η.Π.Α., αλλά τα στοιχεία επιβεβαίωσης των ελέγχων δεν έχουν τηρηθεί, καθώς έχουν διαγραφεί τα ηλεκτρονικά αρχεία καταγραφής. δ) Ότι ο ακριβής χρόνος του περιστατικού αλλά και το πλήθος των συμβάντων παραγωγής των δεδομένων δεν είναι δυνατό να διαπιστωθεί, καθώς ανάγονται σε χρόνο πέραν της διετίας, ενώ από τα τηρούμενα αρχεία καταγραφής δεν διαπιστώθηκε περιστατικό ασφάλειας ούτε ένδειξη για μη αιτιολογημένη μαζική εξαγωγή δεδομένων τα έτη 2012 και 2013. ε) Ότι η πληροφορία που περιέχεται στα δεδομένα του περιστατικού αποτελεί μεν εσωτερική πληροφορία του ΟΤΕ, αλλά δεν είναι σε καμία περίπτωση κρίσιμη ή ευαίσθητη. Επισημάνει μάλιστα ότι τα δεδομένα αυτά διαβιβάζονται και στη ΓΓΠΣ στο πλαίσιο της υφιστάμενης νομοθεσίας ενώ το πεδίο customer_ref αποτελεί εσωτερικής χρησιμότητας πληροφορία που δεν μπορεί να προκαλέσει βλάβη στα υποκείμενα των δεδομένων. στ) Ότι το εν λόγω περιστατικό μπορεί να είναι μόνο αποτέλεσμα κακόβουλης ενέργειας. Επίσης αναφέρει ότι το γεγονός ότι δεν έχουν καταγραφεί περιστατικά παραβίασης υποδεικνύει ότι τα μέτρα που λαμβάνονται είναι επαρκή και αποτελεσματικά. ζ) Ότι έχει ληφθεί πλήθος πρόσθετων μέτρων για τη

[1] Βλ. ειδικότερα: α) Έλεγχοι Ασφάλειας Πληροφοριών (έκδοση PR.ERM.02.16 - 10/05/2013), β) Έλεγχος Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης (Έκδοση PR.ERM.02.07 -15/4/2013)

διασφάλιση των δεδομένων των πελατών του. Τέλος, υποστηρίζει ότι τα δεδομένα που περιελάμβανε το περιστατικό παραβίασης δεν ήταν κρίσιμα ή ευαίσθητα.

Στο πλαίσιο εξέτασης της ως άνω υπόθεσης, ο ΟΤΕ κλήθηκε νομίμως σε ακρόαση κατά τη συζήτηση της υπόθεσης ενώπιον της Αρχής στις 07-10-2014 με την υπ' αριθμ. πρωτ. ΓΝ/ΕΞ/5515/17-09-2014 κλήση και παρέστη. Κατά τη συνεδρίαση, η κληθείσα εξέθεσε προφορικά τις απόψεις της, τις οποίες ανέπτυξε κατόπιν διεξοδικώς με σχετικό υπόμνημά της (υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/6463/27-10-2014).

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου και αναφορά στα διαμειφθέντα της συνεδρίασης της 07-10-2014, αφού άκουσε τον εισηγητή και το βοηθό εισηγητή, ο οποίος στη συνέχεια αποχώρησε, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦ ΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Κατά το 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...». Επίσης, στο άρ. 12 παρ. 1 του ν. 3471/2006 ορίζεται ότι «ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του, καθώς και η ασφάλεια του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών. Τα μέτρα αυτά, εφόσον είναι αναγκαίο, λαμβάνονται από κοινού με τον φορέα παροχής του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών, πρέπει δε να εγγυώνται επίπεδο ασφαλείας ανάλογο προς τον υπάρχοντα κίνδυνο, λαμβανομένων υπόψη αφ' ενός των πλέον προσφάτων τεχνικών δυνατοτήτων αφ' ετέρου δε του κόστους εφαρμογής τους.»

Από τα ανωτέρω προκύπτει ότι ο υπεύθυνος επεξεργασίας, οφείλει ο ίδιος, να προσδιορίζει την καταλληλότητα των μέτρων με κριτήρια α) τη φύση των δεδομένων, όπως καταρχήν απλά ή ευαίσθητα, και τα προστατευόμενα από ειδικά απόρρητα δεδομένα, β) την επικινδυνότητα της επεξεργασίας, δηλαδή ιδίως τις επιπτώσεις που ενδέχεται να επιφέρουν στα φυσικά πρόσωπα περιστατικά παραβίασης των δεδομένων και επιπλέον λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις και το κόστος.

Όπως έχει ήδη επισημάνει η Αρχή με την απόφαση 98/2013, η ασφάλεια εξειδικεύεται σε τρεις βασικούς στόχους, ήτοι την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, ενώ συμπληρωματικοί στόχοι, ιδίως από τη σκοπιά της προστασίας των προσωπικών δεδομένων, αποτελεί μεταξύ άλλων και η μη αποποίηση της ευθύνης (ή λογοδοσία). Από το γράμμα και το σκοπό της διάταξης είναι σαφές ότι η υποχρέωση αυτή του υπευθύνου επεξεργασίας έχει προληπτικό και κατασταλτικό χαρακτήρα. Προληπτικό ώστε τα εφαρμοστέα μέτρα να αποτρέψουν περιστατικά παραβίασης προσωπικών δεδομένων, κατασταλτικό ώστε τυχόν περιστατικό να μπορεί να ανιχνευθεί και να διερευνηθεί.

2. Από τα στοιχεία του φακέλου της υπόθεσης προκύπτει περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα μεγάλου αριθμού συνδρομητών του ΟΤΕ. Το περιστατικό αφορά σε δεδομένα μεταξύ των ετών 2008 και 2010. εν κατέστη δυνατό να διαπιστωθεί με ποιο τρόπο πραγματοποιήθηκε το περιστατικό, αλλά η ύπαρξη πινάκων συνδρομητών για τέσσερις διαφορετικές περιόδους οδηγεί στο συμπέρασμα ότι συνέβη τουλάχιστον μία φορά, κατά πάσα πιθανότητα σε τέσσερις διαφορετικές περιόδους. Τα δεδομένα αφορούν σε πάνω από 8.000.000 παλιούς ή υφιστάμενους συνδρομητές (στους οποίους περιλαμβάνονται φυσικά όσο και νομικά πρόσωπα), που έχουν διατελέσει συνδρομητές του ΟΤΕ (συνολικά). Η αρχική προέλευση των δεδομένων είναι πέραν αμφιβολίας ο ΟΤΕ, καθώς στα δεδομένα περιλαμβάνονται πεδία που είναι εσωτερικά του οργανισμού, ιδίως τα customer, account_num, product_id και product_seq. Στα δεδομένα περιλαμβάνονται τόσο στοιχεία συνδρομητών που είναι ανακοινώσιμα σε καταλόγους (και άρα μπορεί να βρεθούν από δημόσια προσβάσιμη πηγή) αλλά και στοιχεία μη ανακοινώσιμα σε καταλόγους (π.χ. ΑΦΜ), που δεν μπορεί να βρεθούν σε δημόσια προσβάσιμη πηγή. Επίσης, σε πάνω από 350.000 περιπτώσεις συνδρομητών το υποκείμενο των δεδομένων έχει ρητά ζητήσει από τον πάροχο να μην περιλαμβάνονται τα στοιχεία του σε καταλόγους. Είναι βέβαιο ότι δεδομένα των πινάκων (ιδίως του πίνακα

πελατών) έχουν συνδυαστεί με άλλα δεδομένα, είτε εντός του οργανισμού, είτε με διασταύρωση με άλλα δεδομένα (π.χ. με αυτά που κατείχε παράνομα η InfoCredit). Το γεγονός αυτό αποδεικνύει ότι υπήρξε επίπτωση από την επεξεργασία των προσωπικών δεδομένων των συνδρομητών του οργανισμού, ιδιαίτερα μάλιστα και σε όσους είχαν δηλώσει ότι δεν επιθυμούν να είναι τα στοιχεία τους ανακοινώσιμα σε καταλόγους.

Όσον αφορά τα μέτρα ασφάλειας που εφαρμόζει ο ΟΤΕ, ως πάροχος υπηρεσιών ηλεκτρονικής επικοινωνίας υπόκειται σε αυστηρούς κανόνες ως προς την ασφάλεια των ηλεκτρονικών υπηρεσιών που παρέχει και των συναφών δεδομένων (στα οποία περιλαμβάνονται και τα δεδομένα συνδρομητών). ιαθέτει μεν πολιτική ασφάλειας (σύμφωνη με τους κανονισμούς της Α ΑΕ) αλλά τα λαμβανόμενα μέτρα ασφάλειας αποδείχθηκαν στην πράξη ανεπαρκή. Και τούτο γιατί δεν κατάφεραν να αποτρέψουν «μαζική» διαρροή δεδομένων για έως τέσσερις διαφορετικές χρονικές περιόδους, γεγονός που υποδεικνύει ότι το περιστατικό δεν ήταν ένα μεμονωμένο ή τυχαίο γεγονός.

Η Αρχή δέχεται ότι ο ΟΤΕ δεν έχει πλέον τη δυνατότητα να διερευνήσει πλήρως το περιστατικό, καθώς έχουν περάσει πλέον των δύο ετών και τα αρχεία καταγραφής έχουν καταστραφεί. Τούτο όμως δεν σημαίνει ότι ο οργανισμός απαλλάσσεται των ευθυνών του. Αντίθετα, θα έπρεπε να έχει εφαρμόσει μέτρα ασφάλειας που να εξασφαλίζουν ότι δεν είναι δυνατή η μαζική μεταφόρτωση ή/και η εξαγωγή δεδομένων από τα συστήματά του συμπεριλαμβανομένων και των διαχειριστών ή ειδικών εξωτερικών συνεργατών του. Σε κάθε περίπτωση, θα έπρεπε ένα τέτοιας έκτασης και επαναλαμβανόμενο περιστατικό να έχει προληφθεί, ή στη χειρότερη περίπτωση ανιχνευθεί, από τα εφαρμοζόμενα μέτρα ασφάλειας. Η πρόληψη ή, στη χειρότερη περίπτωση, η ανίχνευση ενός τέτοιου περιστατικού δεν μπορεί να θεωρηθεί ως αδύνατη. Άλλωστε, η διαδικασία εξαμηνιαίου ελέγχου των δικαιωμάτων πρόσβασης σε συνδυασμό με την καταγραφή των ενεργειών των χρηστών, μέτρα που ήδη περιγράφονται στις διαδικασίες που υφίσταντο κατά το χρονικό διάστημα 2008 έως 2010, αποτελεί καταρχήν επαρκές μέτρο. Το γεγονός, όμως ότι συνέβη το περιστατικό αποδεικνύει ότι είτε η καταγραφή ενεργειών δεν διενεργήθηκε σωστά, ώστε μη εξουσιοδοτημένος χρήστης απέκτησε το σύνολο των δεδομένων, είτε ότι ο (τουλάχιστον ανά εξάμηνο) έλεγχος των προσβάσεων δεν έγινε αποτελεσματικά. Αν τα ανωτέρω είχαν εφαρμοστεί το περιστατικό θα είχε αντιμετωπιστεί, έστω και κατασταλτικά, εντός του προβλεπόμενου χρονικού

διαστήματος. Αποδεικνύεται επομένως ότι τα λαμβανόμενα μέτρα ασφάλειας δεν ήταν ικανά να αποτρέψουν το περιστατικό.

Από το υπόμνημα του Οργανισμού που κατατέθηκε προ της ακρόασής του προκύπτει επίσης ότι προβαίνει σε διαρκή βελτίωση των μέτρων ασφάλειας, όπως οφείλει. Η πιθανότητα επανάληψης παρόμοιου περιστατικού μειώνεται πλέον, από την εγκατάσταση των συστημάτων DAM (Database Activity Monitor) και IDM (Identity Management) και το διαχωρισμό των δικτύων.

Η Αρχή, λαμβάνοντας υπόψη το μεγάλο αριθμό προσωπικών δεδομένων συνδρομητών φυσικών προσώπων (παλαιών και υφισταμένων) του ΟΤΕ που διέρρευσαν, το γεγονός ότι στα δεδομένα περιλαμβάνονται μη δημόσια προσβάσιμα απλά προσωπικά δεδομένα για μεγάλο αριθμό συνδρομητών, την προσβολή που επήλθε στα υποκείμενα των δεδομένων, όπως αυτή εκτέθηκε αναλυτικά ανωτέρω, τη διαπίστωση ότι δεν τηρήθηκαν τα κατάλληλα μέτρα ασφάλειας, συνεκτιμώντας το γεγονός ότι ο ΟΤΕ ενισχύει τα λαμβανόμενα μέτρα ασφάλειας και ότι μετά τη ανακοίνωση του περαστικού σε αυτόν προχώρησε σε ενέργειες –έστω και ατελέσφορες– για τη διερεύνησή του, κρίνει ότι πρέπει να επιβληθεί στον υπεύθυνο επεξεργασίας η προβλεπόμενη στο άρθρο 21 παρ. 1 στοιχ. β΄ του ν. 2472/1997 κύρωση που αναφέρεται στο διατακτικό της παρούσας και η οποία κρίνεται ανάλογη με τη βαρύτητα της παράβασης.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή επιβάλλει, με βάση τα άρθρα 19 παρ. 1 στοιχ. στ΄ και 21 του ν. 2472/1997, στην «Οργανισμός Τηλεπικοινωνιών της Ελλάδος Α.Ε.» πρόστιμο εξήντα χιλιάδων (60.000) Ευρώ για την ως άνω διαπιστωθείσα παραβίαση των διατάξεων του άρθρου 10 του ν. 2472/1997 και το άρθρου 12 του ν. 3471/2006.

Ο Πρόεδρος της Αρχής **Η Γραμματέας**

Πέτρος Χριστόφορος **Ειρήνη Παπαγεωργοπούλου**