Αρ. Φακ.: Α /Π 68/2017

ΑΠΟΦΑΣΗ

΄Υστερα από αυτεπάγγελτη έρευνα με αφορμή δημοσιεύματα στον τύπο αναφορικά με διαρροή προσωπικών δεδομένων από τη CYTA (την Αστυνομία Κύπρου και τις Υπηρεσίες Κοινωνικών Ασφαλίσεων)

Με αφορμή πληθώρα δημοσιευμάτων στον ημερήσιο έντυπο και ηλεκτρονικό τύπο από τις 12/8/2017 μέχρι τις 18/8/2017 τα οποία έφεραν και /ή ενέπλεκαν την CYTA (εφεξής «η καθ'ής») σε σκάνδαλο διαρροής προσωπικών δεδομένων, το οποίο μάλιστα σύμφωνα με τα δημοσιεύματα είχε αναδειχθεί από συγκεκριμένα Μ.Μ.Ε από το 2009, χωρίς ωστόσο να διεξαχθεί ποινική διερεύνηση της υπόθεσης, αποφάσισα να διερευνήσω το εν λόγω περιστατικό.

2. Ιστορικό της υπόθεσης με βάση τα δημοσιεύματα:

Σύμφωνα με την πλειοψηφία των δημοσιευμάτων (τα οποία αποτελούν μέρος του Φακέλου της υπόθεσης) 43χρονη υπάλληλος της καθ'ής διέρρευσε σε 68χρονο πρώην αστυνομικό προσωπικά δεδομένα 249 πελατών της καθ'ής. Το συμβάν έγινε αντιληπτό ύστερα από εσωτερικό έλεγχο που διενήργησε η ίδια η καθ'ής.

3. Ενέργειες Επιτρόπου:

3.1 Λόγω των διαστάσεων που έλαβε η υπόθεση διαρροής και /ή παραβίασης προσωπικών δεδομένων αριθμού φυσικών προσώπων από τις βάσεις δεδομένων της καθ'ού, σε τρίτα, μη εξουσιοδοτούμενα πρόσωπα, και ανεξάρτητα από οποιαδήποτε άλλη παράλληλη διαδικασία που διεξήγαγε Αρχή στη Δημοκρατία και ανεξάρτητα από τη διαδικασία Γνωστοποίησης συμβάντος παραβίασης προσωπικών δεδομένων (άρθρο

98Α Νόμου 112(Ι)/2004), αποφάσισα να διερευνήσω το περιστατικό με βάση τις εξουσίες που μου απονέμουν οι διατάξεις του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001, Ν.138(Ι)/2001, όπως τροποποιήθηκε, (εφεξής «ο Νόμος»).

3.2 Με την επιστολή μου προς την καθ'ής ημερ. 18 Αυγούστου 2017, ζήτησα όπως με ενημερώσει σχετικά με τα κάτωθι:

«3.2.1 τις συνθήκες κάτω από τις οποίες επεσυνέβη το περιστατικό καθώς και τη φύση της παράβασης,

3.2.2 τα προτεινόμενα μέτρα και τις επόμενες ενέργειές σας για το μετριασμό και /ή αποκατάσταση των δυσμενών αποτελεσμάτων της παραβίασης,

3.2.3 τις συνέπειες της παραβίασης, και

3.2.4 τα μέτρα ασφάλειας (συμπεριλαμβανομένων των οργανωτικών μέτρων ασφάλειας) που λαμβάνονταν κατά την επέλευση των περιστατικών ασφαλείας και αναφορά των λόγων που κατά την άποψη της καθ'ής τα μέτρα αυτά δεν απέδωσαν τα, κατά την κρίση της, αναμενόμενα αποτελέσματα, και /ή δεν λειτούργησαν όπως θα έπρεπε, ώστε να είχαν αποφευχθεί τα περιστατικά ασφάλειας στα οποία, με βάση τα δημοσιεύματα φαίνεται να ενέχεται η καθ'ής.».

3.2.5 Με την ίδια επίσης επιστολή **<u>επισημάνθηκαν</u>** οι διατάξεις **του άρθρου 10 του Νόμου,** που αφορούν στο **απόρρητο και την ασφάλεια της επεξεργασίας**, δυνάμει των οποίων:

*«10.-(1) **Η επεξεργασία δεδομένων είναι απόρρητη**. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνο 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 ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.

……..».

3.2.6 Για τους σκοπούς υποβολής των σχολίων και απόψεών της καθ'ής ορίστηκε αποκλειστική προθεσμία δύο εβδομάδων από την ημερομηνία παραλαβής της ανωτέρω επιστολής μου.

4. Θέσεις της καθ'ής αναφορικά με το περιεχόμενο της επιστολής μου:

Η καθ'ής με την επιστολή της ημερ. 1 Σεπτεμβρίου 2017, με ενημέρωσε σχετικά με τα ακόλουθα:

4.1 Στα πλαίσια των προληπτικών και κατασταλτικών ελέγχων τηλεπικοινωνιακής απάτης που πραγματοποιούσε η μονάδα Ασφάλειας Πληροφοριών πραγματοποιήθηκε έλεγχος των προσβάσεων του προσωπικού από τον οποίο **διεφάνη** ότι η υπάλληλος της καθ'ής "Χ" (εφεξής «η υπάλληλος») **είχε μη εξουσιοδοτημένη πρόσβαση**, σε μεγάλο αριθμό προσωπικών δεδομένων πελατών της καθ'ής, στοιχείων όπως ονοματεπώνυμου και διεύθυνσης.
Διευκρινίστηκε επίσης ότι η εξυπηρέτηση πελατών και η πρόσβαση της υπαλλήλου σε στοιχεία τους ήταν δυνατή με βάση τα προηγούμενα καθήκοντα της. Με την αλλαγή των καθηκόντων της τα οποία αφορούσαν πλέον στην διαχείριση τιμολογίων για παραγγελίες, η καθ'ής **παρέλειψε να αφαιρέσει από την υπάλληλο τις σχετικές προσβάσεις** στη βάση δεδομένων που περιελάμβανε προσωπικά δεδομένα των πελατών της.

4.2 Με τον εντοπισμό του περιστατικού έγινε αμέσως καταγγελία στην Αστυνομία και αφαιρεθήκαν όλες οι προσβάσεις της υπαλλήλου σε κτίρια και συστήματα πληροφορικής της καθ'ής.

Στάληκε επίσης, εσωτερική εγκύκλιος σε όλες τις μονάδες της καθ'ής για έλεγχο των προσβάσεων όλου του προσωπικού με σκοπό τη διασφάλιση πλήρους συμμόρφωσης με την **πολιτική ασφάλειας** η οποία, όπως ανέφεραν, καθόριζε ότι κατά την αποχώρηση προσωπικού από συγκεκριμένο πόστο (π.χ αλλαγή καθηκόντων, μετάθεση κλπ) αφαιρούνται τα δικαιώματα πρόσβασης. Τα δικαιώματα αυτά δίνονται ανά εφαρμογή με γραπτή έγκριση στη βάση των καθηκόντων του προσωπικού και περιορίζονται στις απολύτως απαραίτητες πληροφορίες για της διεκπεραίωση των καθηκόντων αυτών. Όλες οι προσβάσεις καταγράφονται σε αρχεία ιχνηλασιμότητας. **Τη βάση δεδομένων των αρχείων ιχνηλασιμότητας διαχειρίζεται η μονάδα Ασφάλειας Πληροφοριών η οποία διενεργεί και τους σχετικούς ελέγχους σχετικά με τη νομιμότητα των προσβάσεων.**
Οι διαδικασίες και πολιτικές ασφαλείας είναι αναρτημένες στο ενδοδίκτυο της καθ΄ ής για εύκολη πρόσβαση και έχουν γίνει σχετικά εκπαιδευτικά σεμινάρια.

4.3 Οι συνέπειες της παραβίασης των προσωπικών δεδομένων της καθ'ής δεν είχαν μέχρι τούδε διαπιστωθεί δεδομένου ότι η υπόθεση τελούσε υπό διερεύνηση από την Αστυνομία.

4.4.1 Η καθ'ής λάμβανε μέτρα για την ασφάλεια των πληροφοριών Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) στη βάση του διεθνούς προτύπου ISO27001/2013. Έχει εξασφαλίσει επίσης τη σχετική πιστοποίηση ISO27001/2013 στα κέντρα δεδομένων της (data centers).

4.4.2 Το ΣΔΑΠ περιλαμβάνει σχετικό εγχειρίδιο το οποίο καλύπτει θέματα για την ασφάλεια δικτύων και πληροφοριών (ηλεκτρονικής πρόσβασης, διαχείρισης κωδικών πρόσβασης, διατήρησης αρχείων ιχνηλασιμότητας, ελέγχων ασφαλείας, διαδικασίες χειρισμού περιστατικών, τεχνικές και διαδικασίες για προστασία από κυβερνοπειρατές κλπ).

4.4.3 Αναφορικά με τα τεχνικά θέματα ασφάλειας δικτύων πληροφορικής, όπως ανέφεραν, έχει συσταθεί ομάδα εξειδικευμένων ατόμων οι οποίοι έχουν, μεταξύ άλλων, την ευθύνη τεχνικού σχεδιασμού της υποδομής ασφάλειας των συστημάτων πληροφορικής, τη διενέργεια τεχνικών ελέγχων ασφάλειας κλπ.
Το προσωπικό της καθ'ής το οποίο εμπλέκεται σε θέματα ασφάλειας των πληροφοριών διαθέτει όλες τις απαραίτητες γνώσεις και εμπειρίες και έχει εξασφαλίσει τις σχετικές πιστοποιήσεις π.χ CISSP, CISA, CEH, ISO27001 Lead implementer κλπ.

4.4.4 Η καθ'ής κατέληξε ότι λαμβάνει όλα τα ενδεικνυόμενα τεχνικά και διαδικαστικά μέτρα που είναι πρακτικά εφαρμόσιμα για τα θέματα ασφάλειας των πληροφοριών.

5. Νομοθετικό έρεισμα:

5.1 Άρθρο 23(1) (η) του Νόμου: Αρμοδιότητες, λειτουργία και αποφάσεις Επιτρόπου:

«23.(1) - Ο Επίτροπος έχει τις εξής αρμοδιότητες:
……..
(η) Ενεργεί αυτεπαγγέλτως ή ύστερα από καταγγελία ελέγχους σε οποιοδήποτε αρχείο. Έχει, για το σκοπό αυτό, δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας, χωρίς να δύναται να του αντιταχθεί κανενός είδους απόρρητο, εξαιρουμένου μόνο του δικηγορικού. Κατ' εξαίρεση, ο Επίτροπος δεν έχει πρόσβαση στα στοιχεία ταυτότητας συνεργατών που περιέχονται σε αρχεία που τηρούνται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.
Τον έλεγχο διενεργεί ο Επίτροπος ή λειτουργός του Γραφείου ειδικά εξουσιοδοτημένος για το σκοπό αυτό από αυτόν. Κατά τον έλεγχο αρχείων που τηρούνται για λόγους εθνικής ασφάλειας, παρίσταται αυτοπροσώπως ο Επίτροπος.».

Σχόλιο: Νοείται ότι στην ανωτέρω έννοια των ελέγχων δεν περιλαμβάνονται μόνον οι επιτόπιοι έλεγχοι αλλά και οι έλεγχοι που διεξάγονται μέσω συλλογής στοιχείων με άλλους τρόπους, όπως για παράδειγμα μέσω υποβολής γραπτών ερωτημάτων διά αλληλογραφίας.

5.2 Άρθρο 10 (1),(2),(3) Απόρρητο και ασφάλεια της επεξεργασίας:

«10.-(1) Η επεξεργασία δεδομένων είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνο 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 ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας……..».

6. Σκεπτικό Επιτρόπου και Κατάληξη:

Ύστερα από εξέταση και /ή μελέτη των θέσεων και ισχυρισμών της καθ'ής σε συσχέτιση με όλα τα ενώπιόν μου στοιχεία (δημοσιεύματα και προφορική ενημέρωση που έλαβα από την Αστυνομία) και αφού έλαβα υπόψην μου όλα τα κατωτέρω: –

6.1 **Παραδοχή της καθ'ής** ότι η υπάλληλος είχε **μη εξουσιοδοτημένη πρόσβαση** σε μεγάλο αριθμό προσωπικών δεδομένων τα οποία αφορούσαν κοινά /απλά δεδομένα των πελατών της καθ' ής όπως ονοματεπώνυμο και διεύθυνση.

6.2 **Παραδοχή της καθ'ής** ότι με την αλλαγή των καθηκόντων της υπαλλήλου και την μετακίνηση της σε άλλη θέση **παρέλειψε** να ενεργήσει σύμφωνα με την πολιτική ασφαλείας ώστε να αφαιρέσει τα δικαιώματα πρόσβασής της στα προσωπικά δεδομένα των πελατών που είχε με βάση τα προηγούμενα καθήκοντά της.

Σχόλιο: Η αναθεώρηση των ρόλων εντός ενός Οργανισμού εμπίπτει και αποτελεί μέρος των **οργανωτικών μέτρων ασφάλειας**. Η περιοδική επανεξέταση και αναθεώρηση των εξουσιοδοτήσεων και δικαιωμάτων πρόσβασης σε όλα τα στάδια της εργασιακής σχέσης των υπαλλήλων π.χ πρόσληψη, μετακίνηση, αλλαγή καθηκόντων, αποχώρηση κλπ θα πρέπει όχι μόνο να προβλέπεται ως διαδικασία στην πολιτική ασφαλείας αλλά να εφαρμόζεται και να ελέγχεται η εφαρμογή της κατά τακτά χρονικά διαστήματα.

Εισήγηση: Μπορεί ο φορέας της υποχρέωσης για το σκοπό αυτό να τηρεί κατάλογο με τα δικαιώματα πρόσβασης τον οποίο να επικαιροποιεί κατά τακτά χρονικά διαστήματα. Μπορεί να επιμεριστεί η ευθύνη αυτή σε κάθε οικείο προϊστάμενο ο οποίος να έχει υποχρέωση να ενημερώνει τον κατάλογο αυτό σε σχέση με κάθε υφιστάμενό του ο οποίος μετακινείται, αλλάζει καθήκοντα ή αποχωρεί από τον Οργανισμό και να προβαίνει σε όλες τις απαραίτητες ενέργειες για αφαίρεση των σχετικών δικαιωμάτων πρόσβασης.

Σχετικό είναι το κατωτέρω απόσπασμα από την Απόφαση της Ελληνικής Αρχής Προστασίας Δεδομένων Αρ.98/2013:

«Καταρχάς 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, αποτελούν ιδίως η μη αποποίηση της ευθύνης (ή λογοδοσία) καθώς και ο διαχωρισμός των δεδομένων ανάλογα με το σκοπό της επεξεργασίας. Κατά τα διεθνώς αποδεκτά πρότυπα ασφάλειας πληροφοριακών συστημάτων (π.χ. βλ. σειρά ISO/IEC 27000) τα κατάλληλα μέτρα κατά το άρθρο 10 παρ. 3 ν. 2472/1997 εντάσσονται σε ένα Σύστημα Ασφάλειας Πληροφοριακών Συστημάτων (ISMS). Το εν λόγω Σύστημα προϋποθέτει την εκπόνηση μελέτης επικινδυνότητας με βάση τους κινδύνους και τη φύση των δεδομένων, και μεταξύ άλλων περιλαμβάνει την κατάρτιση πολιτικής και σχεδίων ασφάλειας, όπου προσδιορίζονται συγκεκριμένα τεχνικά και οργανωτικά μέτρα. ***Τα μέτρα αυτά, εκτός του ότι πρέπει να εφαρμόζονται, επιπλέον παρακολουθούνται και αξιολογούνται*** *με σκοπό τη διαρκή προσαρμογή τους στις επιχειρησιακές ανάγκες του υπευθύνου επεξεργασίας και στις τεχνολογικές εξελίξεις, τις οποίες οφείλει να λαμβάνει υπ΄ όψιν ο υπεύθυνος επεξεργασίας (βλ. άρθρο 17 παρ. 1 Οδηγία 95/46/ΕΚ).*

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…».

6.3 Ομοίως, στην παρούσα υπόθεση η καθ'ής παρόλο που ισχυρίζεται στην υποπαράγραφο 4.4.4 της παρούσας Απόφασης ότι λάμβανε και /ή λαμβάνει όλα τα ενδεικνυόμενα τεχνικά και διαδικαστικά μέτρα που είναι πρακτικά εφαρμόσιμα για τα θέματα ασφάλειας των πληροφοριών, εντούτοις το αποτέλεσμα ήταν ότι υπάλληλός της χωρίς εξουσιοδοτημένη πρόσβαση και /ή καθ' υπέρβασή της προέβη σε απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.
Στην περίπτωση αυτή διαπιστώνεται ότι δεν λειτούργησαν κατά τον ορθό και ενδεδειγμένο τρόπο τα οργανωτικά μέτρα ασφάλειας, ως μέτρα προληπτικής φύσης, με λογικό επακόλουθο τη μη λήψη και /ή ενεργοποίηση των απαραίτητων υπό τις περιστάσεις τεχνικών μέτρων ασφάλειας π.χ Διαχείριση λογαριασμών χρηστών που πρέπει να περιλαμβάνει κατ' ελάχιστο διαδικασίες για την προσθήκη, μεταβολή ιδιοτήτων και διαγραφή λογαριασμού.

6.4 Ειδικότερα τα δεδομένα, τα οποία είχαν καταστεί αντικείμενο μη εξουσιοδοτημένης πρόσβασης και περαιτέρω επεξεργασίας συνιστούν απλά και /ή κοινά προσωπικά δεδομένα τα οποία όμως, **επιπλέον** υπόκεινται στο σύνολό τους στο απόρρητο των επικοινωνιών.

6.5 Δημοσιεύματα του 2010 στον έντυπο και ηλεκτρονικό τύπο τα οποία έφεραν την καθ'ής να εμπλέκεται σε υπόθεση παραβίασης και διαρροής προσωπικών δεδομένων σε παρόμοια υπόθεση –

Σχετικά αποσπάσματα παρατίθενται αυτούσια (πηγή Sigmalive 26/2/2010):

«Ανησυχίες για τη διαρροή τηλεπικοινωνιακών δεδομένων μετά την υποκλοπή στη ΣΥΤΑ

Ο Βοηθός Γενικός Εισαγγελέας ανησυχεί για το τι μπορεί να γίνεται στις ιδιωτικές εταιρείες κινητής τηλεφωνίας με τις υποκλοπές.

ΜΙΧΑΛΗΣ ΚΑΤΣΟΥΝΩΤΟΣ- Πιθανόν να μην αποκαλυφθεί η ταυτότητα όλων των συνδρομητών που παρακολουθούνταν.

Νέες σοβαρές διαστάσεις παίρνει το θέμα της υποκλοπής τηλεπικοινωνιακών δεδομένων στη ΣΥΤΑ, μετά από δηλώσεις του βοηθού Γενικού Εισαγγελέα Άκη Παπασάββα. Ο κ. Παπασάββας εξέφρασε τις ανησυχίες του μετά την αποκάλυψη ότι το απόρρητο των τηλεπικοινωνιακών δεδομένων των πολιτών δυνατόν να παραβιάζετο και στο παρελθόν, μετά τη σύλληψη υπαλλήλου της ΑΤΗΚ, ο οποίος φέρεται να παρακολουθούσε, να υπέκλεπτε και να πωλούσε τηλεπικοινωνιακά δεδομένα κινητής τηλεφωνίας σε ιδιωτικό ντετέκτιβ, τα οποία ο τελευταίος χρησιμοποιούσε στο πλαίσιο των υποθέσεων που αναλάμβανε.

Όπως λέχθηκε από την Αστυνομία, η υπόθεση περιήλθε για πρώτη φορά εις γνώσιν της ΚΥΤΑ, όταν ένας πελάτης, κρατώντας κατάλογο με τηλεφωνικά δεδομένα, ζήτησε εξηγήσεις από υπαλλήλους του οργανισμού.

Το γεγονός προκάλεσε υποψίες καθώς τα συγκεκριμένα προσωπικά δεδομένα είναι απόρρητα και μόνο κάποιος εκ των έσω θα μπορούσε να τα είχε εξασφαλίσει.
Σύμφωνα πάντα με την Αστυνομία, ο πελάτης της ΚΥΤΑ φέρεται να παραδέχθηκε ότι αγόρασε τα τηλεπικοινωνιακά δεδομένα.
Τότε, πολύ διακριτικά άρχισαν οι έρευνες εντός της ΚΥΤΑ για να εντοπιστεί ο υπάλληλος στο τμήμα κινητής τηλεφωνίας του οργανισμού, ο οποίος παρακολουθούσε, πραγματοποιούσε παρεμβάσεις και υπέκλεπτε στοιχεία και πληροφορίες από τηλεφωνικές κλήσεις κινητής τηλεφωνίας.

Η Αστυνομία θα προχωρήσει στην υποβολή αιτήσεων για έκδοση διαταγμάτων αποκάλυψης των τηλεπικοινωνιακών δεδομένων για τις 22 περιπτώσεις, οι οποίες φαίνεται να υπήρξαν αντικείμενο υποκλοπής.

Όπως δήλωσε ο εκπρόσωπος Τύπου της Αστυνομίας, Μιχάλης Κατσουνωτός, από την αποκάλυψη των στοιχείων, δυνατόν να διαφανούν και τα κίνητρα των δραστών.
Είπε, επίσης, ότι η Αστυνομία δεν γνωρίζει κανέναν από τους συνδρομητές, ούτε κατά πόσον μεταξύ τους περιλαμβάνονται πολιτικοί ή άλλοι αξιωματούχοι.

Η Βουλή θεωρεί το όλο θέμα πολύ σοβαρό. Και εισηγείται τη σύσταση Αρχής για την προστασία του απορρήτου των επικοινωνιών όπως εφαρμόζεται στις πλείστες χώρες της Ε.Ε. Ο πρόεδρος της επιτροπής Νομικών, Ιωνάς Νικολάου, ανέφερε ότι ο μηχανισμός ελέγχου της ΚΥΤΑ δεν είναι ικανοποιητικός και πως το περιστατικό αυτό αποκαλύφθηκε μετά από καταγγελία και όχι στα πλαίσια της άσκησης αυτού του ελέγχου.».

6.6 Ο εσωτερικός έλεγχος των αρχείων ιχνηλασιμότητας, τα οποία καταγράφουν τις προσπελάσεις των χρηστών, παρέχει τη δυνατότητα, ως τεχνικό μέτρο ασφάλειας κατασταλτικής φύσης, να εντοπίζονται, μέσω εκ των υστέρων ελέγχου, περιστατικά παραβίασης ασφάλειας προσωπικών δεδομένων.

Σχετικά με τέτοιας φύσεως περιστατικά θα πρέπει να εφαρμόζονται διαδικασίες για την αναγνώριση, αναφορά και **άμεση αντιμετώπισή τους** στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας και όχι η διαπίστωση και /ή ο εντοπισμός τους να γίνεται μέσω παρεμπίπτουσας διαδικασίας και /ή άλλων ελέγχων.

Στις διαδικασίες αυτές πρέπει να περιλαμβάνονται κατ' αρχάς οι ενέργειες που είναι αναγκαίες για τη διερεύνηση του εκάστοτε περιστατικού – τρόπος αναφοράς περιστατικού, προσωπικό που θα ενεργοποιηθεί, αρχεία-συστήματα που θα πρέπει να διερευνηθούν, τι θα περιλαμβάνει το αρχείο διαχείρισης περιστατικού, διαδικασία ενημέρωσης των θιγομένων ατόμων (υποκειμένα των δεδομένα) ανάλογα με την έκταση του περιστατικού, κ.λπ.

6.7 Η καθ'ής ως υπεύθυνος επεξεργασίας δεν θα πρέπει να παραμένει αμέτοχη στις διαδικασίες αυτές ακόμη και όταν γίνονται παράλληλες έρευνες από τις διωκτικές αρχές, θα έπρεπε να είναι σε θέση να γνωρίζει τις πιθανές συνέπειες μίας τέτοιας παραβίασης των προσωπικών δεδομένων των πελατών της, δεδομένου ότι με βάση τα δημοσιεύματα πρόκειται για αρκετά μεγάλο αριθμό, 249 άτομα.

6.8 Σημειώνεται ότι η καθ'ής δεν έχει επιβεβαιώσει και ή παρέλειψε να αναφερθεί στον αριθμό των επηρεαζόμενων συνδρομητών/πελατών της, στοιχεία των οποίων, έτυχαν μη εξουσιοδοτημένης πρόσβασης και περαιτέρω επεξεργασίας.

6.9 Η επιλογή του κατάλληλου κατά περίπτωση προσωπικού με καταβολές ήθους, εχεμύθειας και εμπιστευτικότητας από έκαστο υπεύθυνο επεξεργασίας αποτελεί πάγια υποχρέωσή του.

6.10 Η καθ'ής, σύμφωνα με τους ισχυρισμούς στην επιστολή της, λαμβάνει όλα τα κατάλληλα μέτρα ασφάλειας και έχει εξασφαλίσει για το σκοπό αυτό όλες τις απαραίτητες πιστοποιήσεις για λειτουργία του Οργανισμού της σύμφωνα με τα διεθνώς αναγνωρισμένα πρότυπα για την ασφάλεια των πληροφοριών, και έχει σε ισχύ πολιτική ασφάλειας την οποία κυκλοφόρησε στο προσωπικό της. Επίσης, έχει πραγματοποιήσει σεμινάρια για την εκπαίδευση του προσωπικού της.

6.11 Η καθ'ής, έλαβε κάποια διορθωτικά μέτρα, μεταξύ των οποίων ήταν και η απομάκρυνση της υπαλλήλου τόσο από τα πληροφοριακά συστήματα όσο και από τα κτίρια της καθ'ής.

Και αφού άκουσα την καθ'ής με βάση τις διατάξεις του άρθρου 43 του περί των Γενικών Αρχών του Διοικητικού Δικαίου Νόμου, Ν,158(Ι)/1999, ασκώντας το δικαίωμα της προηγούμενης ακρόασης, σχετικά με ενδεχόμενη παράβαση των διατάξεων του άρθρου 10(1),(2) και (3) του Νόμου –

7. Έχω καταλήξει, τηρουμένης και της παραδοχής της καθ'ής, ως οι παρ. **6.1** και **6.2** της παρούσας Απόφασης ότι η καθ'ής ευθύνεται για την παράβαση των διατάξεων του άρθρου 10(1),(2) και (3) του Νόμου μέσω των πράξεων και παραλείψεών της για μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα από την υπάλληλό της και περαιτέρω επεξεργασία, περιστατικό που ενδεχομένως να μπορούσε να αποφευχθεί εάν η καθ'ής αφαιρούσε τα δικαιώματα πρόσβασης της υπαλλήλου με την αλλαγή των καθηκόντων της.

8. Υπό το φως της ανωτέρω κατάληξής μου, **καλείται** με την παρούσα Απόφαση η καθ'ής, όπως, τηρουμένων των διατάξεων του άρθρου 43 του περί των Γενικών Αρχών του Διοικητικού Δικαίου Νόμου, Ν,158(Ι)/1999, ασκώντας το δικαίωμα της προηγούμενης ακρόασης, **υποβάλε**ι εντός **δέκα ημερών** από την ημερομηνία της παραλαβής της παρούσας Απόφασης τις θέσεις της καθώς και τους λόγους για τους οποίους πιστεύει ότι δεν θα πρέπει να της επιβληθεί οποιαδήποτε από τις προβλεπόμενες στις διατάξεις του άρθρου 25 Διοικητικές κυρώσεις και /ή να με

ενημερώσει γραπτώς σχετικά με τους λόγους και τις περιστάσεις που θα πρέπει να ληφθούν υπόψη στο πλαίσιο και για τους σκοπούς επιβολής μίας εκ των διοικητικών κυρώσεων οι οποίες διαλαμβάνονται στο άρθρο 25(1) του Νόμου –

«(β) χρηματική ποινή μέχρι τριάντα χιλιάδες ευρώ (€30,000),
(γ) προσωρινή ανάκληση άδειας,
(δ) οριστική ανάκληση άδειας,
(ε) καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή των σχετικών δεδομένων.».

Ειρήνη Λοϊζίδου Νικολαϊδου
Επίτροπος Προστασίας
Δεδομένων Προσωπικού Χαρακτήρα

ΛΕΥΚΩΣΙΑ, 20 Οκτωβρίου 2017