ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 16-06-2015

Αριθ. Πρωτ.: Γ/ΕΞ/3456/16-06-2015

Α Π Ο Φ Α Σ Η 70/2015

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος στην έδρα της την Τετάρτη 27 Μαΐου 2015 και ώρα 10:00 μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Γιώργος Μπατζαλέξης, Αναπληρωτής Πρόεδρος, κωλυομένου του Προέδρου Πέτρου Χριστόφορου, και τα αναπληρωματικά μέλη της Αρχής Σπύρος Βλαχόπουλος, Χαράλαμπος Ανθόπουλος και Γρηγόρης Λαζαράκος ως εισηγητής, σε αντικατάσταση των τακτικών μελών Λεωνίδα Κοτσαλή, Δημητρίου Μπριόλα και Αναστάσιου-Ιωάννη Μεταξά, οι οποίοι αν και εκλήθησαν νομίμως εγγράφως, δεν παρέστησαν λόγω κωλύματος. Παρόντες χωρίς δικαίωμα ψήφου ήταν η Κυριακή Λωσταράκου, νομικός ελεγκτής-δικηγόρος, και Ανάργυρος Χρυσάνθου, ως βοηθοί εισηγητές και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικού-Οικονομικού, ως γραμματέας, μετά από εντολή του Προέδρου.

Στη συνεδρίαση της 11ης Μαρτίου 2013 και μετά από κλήση παρέστησαν α) η προσφεύγουσα Α με την πληρεξούσια δικηγόρο της Μαρία-Αλεξάνδρα Μαλάμη, και β) οι εκπρόσωποι της τράπεζας Άλκηστη Σπέντζου, δικηγόρος, και Β, Εσωτερικός Ελεγκτής της Τράπεζας, οι οποίοι και εξέθεσαν τις απόψεις τους επί της υποθέσεως και απάντησαν σε ερωτήσεις που τους τέθηκαν όπως αναφέρεται στα πρακτικά. Κατά τη συνεδρίαση της 27ης Μαΐου 2015 αναπτύχθηκε η υπόθεση από τον εισηγητή και τους βοηθούς εισηγητές και στη συνέχεια έλαβε χώρα διάσκεψη επί της υποθέσεως χωρίς την παρουσία των βοηθών Εισηγητών.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η προσφεύγουσα καταγγέλλει ότι το έτος 2012 η καθής τράπεζα Eurobank Ergasias ΑΕ δια των οργάνων της, παραβλέποντας τη λειτουργία της τραπεζικής σχέσης ως σχέσης εμπιστοσύνης μεταξύ της τράπεζας και του πελάτη, παραβίασε το απόρρητο των τραπεζικών της καταθέσεων και διενήργησε εξαντλητικό έλεγχο σε σχέση με το πρόσωπό της, προβαίνοντας σε παράνομη επεξεργασία προσωπικών της δεδομένων.

Ειδικότερα, η ανωτέρω καταγγέλλει ότι κατά το χρονικό διάστημα από 10-11-2011 έως 15-12-2011 με τη συνδρομή προστηθέντων υπαλλήλων της καταγγελλόμενης τράπεζας, τρίτοι απέκτησαν παρανόμως πρόσβαση και γνώση του υπολοίπου συγκεκριμένων τραπεζικών της λογαριασμών που τηρεί σε αυτήν, όπως διαπίστωσε σε προφορική συζήτηση που είχε με αντίδικο, αλλά και πρώην συνεργάτη της. Μετά την έντονη διαμαρτυρία της στο κατάστημα της τράπεζας στην [περιοχή] Χ, όπου η αδελφή της Γ κατείχε τη θέση της διευθύντριας, διενεργήθηκε έλεγχος από την αρμόδια υπηρεσία της τράπεζας που είχε ως αποτέλεσμα, κατά την καταγγέλλουσα**,** να εντοπιστούν οι παραβάτες, ωστόσο, η τράπεζα αρνείται ότι έλαβε χώρα η εν λόγω παράνομη επεξεργασία.

Περαιτέρω η καταγγέλλουσα καταγγέλλει ότι η τράπεζα μέσω των εσωτερικών της διευθύνσεων, παρανόμως προέβη κατά το χρονικό διάστημα 17-01-2012 έως 30-05-2012 σε προσβάσεις και ελέγχους όλων των τραπεζικών της λογαριασμών με συνδικαιούχο την αδελφή της Γ, σε βάρος της οποίας διενεργούταν εσωτερικός έλεγχος που είχε ως συνέπεια να λάβουν γνώση κινήσεων των λογαριασμών μέχρι και χαμηλόβαθμοι υπάλληλοι του ως άνω καταστήματος, όπως διαπίστωσε η καταγγέλλουσα από τα σχετικά σχόλιά τους.

Με τα με αρ. πρωτ. Γ/ΕΞ/3047/29-04-2013, Γ/ΕΞ/2650/29-04-2014 και Α/ΕΞ/68/12-06-2014 έγγραφα η Αρχή ζήτησε τις απόψεις της καθής επί των καταγγελλομένων, ιδίως ζήτησε να αποσταλεί αντίγραφο τυχόν πορίσματος του ελέγχου που διενεργήθηκε για το πρώτο σκέλος της καταγγελίας ή άλλα στοιχεία που να τεκμηριώνουν ότι δεν υπήρξαν παράνομες προσβάσεις ή διαβιβάσεις, καθώς και τα αρχεία καταγραφής των προσβάσεων υπαλλήλων της τράπεζας στους λογαριασμούς της προσφεύγουσας κατά το επίμαχο χρονικό διάστημα.

Η καθής απέστειλε με τα με αρ. πρωτ. Γ/ΕΙΣ/3707/30-05-2013, Γ/ΕΙΣ/3511/3-06-2014, Γ/ΕΙΣ/5533/18-09-2014 και Γ/ΕΙΣ/7827/11-12-2014 έγγραφά της τις απόψεις της. Η καθής υπέβαλε επίσης, σε συνέχεια της συνεδρίασης της 11ης Μαρτίου 2015, το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1761/19-03-2015 υπόμνημα, στο οποίο, συμπληρωματικά στα προηγουμένως έγγραφα, εξέθεσε τις απόψεις της, ως αυτές εκφράστηκαν στη συνεδρίαση. Ως προς το πρώτο σκέλος ενημέρωσε για το εσωτερικό κανονιστικό πλαίσιο για την τήρηση τραπεζικού απορρήτου και επαγγελματικής εχεμύθειας (Κώδικα Δεοντολογίας, Εγκυκλίους και Υπηρεσιακά Σημειώματα) και ανέφερε ότι από τη διερεύνηση που έκανε για την υπόθεση δεν προέκυψαν στοιχεία που να επιβεβαιώνουν τις καταγγελίες της προσφεύγουσας περί παραβίασης τραπεζικού απορρήτου και παράνομης επεξεργασίας τραπεζικών της λογαριασμών, κατόπιν τούτου δεν συντάχθηκε πόρισμα ελέγχου. Απέστειλε ακόμα αντίγραφα των αρχείων της από το μηχανογραφικό της σύστημα όπου περιλαμβάνονται οι καταγεγραμμένες προσβάσεις υπαλλήλων της στους επίμαχους λογαριασμούς της προσφεύγουσας με επεξήγηση του είδους των δεδομένων και των κωδικών που αναγράφονται στις στήλες των αρχείων καταγραφής. Σημείωσε ακόμα ότι δεν μπορεί να τεκμηριωθεί παράνομη επεξεργασία δεδομένου ότι οι χρήστες που εμφανίζονται στα εν λόγω αρχεία είτε εργάζονταν στο κατάστημα τήρησης του λογαριασμού ή σε άλλα καταστήματα στα οποία η προσφεύγουσα διενεργούσε κατά καιρούς συναλλαγές, από τα δε λοιπά στοιχεία συνάγεται ότι οι προσβάσεις έγιναν στο πλαίσιο τραπεζικών εργασιών και εξυπηρέτησης συναλλαγών της ανωτέρω.

Ως προς το δεύτερο σκέλος της προσφυγής, η καθής αναφέρει ότι ενήργησε σύμφωνα με τις βασικές ρυθμίσεις που αφορούν τον εσωτερικό έλεγχο των τραπεζών και ειδικότερα (α) την υπ'αρ. 281/17-03-2009 απόφαση της Επιτροπής Τραπεζικών και Πιστωτικών Θεμάτων της Τραπέζης της Ελλάδος, (β) την υπ' αρ. 2577/9-03-2006 πράξη του Διοικητή της Τραπέζης της Ελλάδος και (γ) την υπ' αρ. 285/9-07-2009 απόφαση της Επιτροπής Τραπεζικών και Πιστωτικών Θεμάτων της Τραπέζης της Ελλάδος. Η καθής αναφέρει ότι προέβη στον εσωτερικό έλεγχο που αφορούσε τους λογαριασμούς της προσφεύγουσας αφότου πληροφορήθηκε τη σύλληψη και ποινική δίωξη του Δ, γαμπρού της προσφεύγουσας και συζύγου της αδελφής της, η οποία ετύγχανε υπάλληλος της καθής και συνδικαιούχος στους επίμαχους λογαριασμούς. Το ως άνω γεγονός πληροφορήθηκε η καθής, καθόσον έλαβε μεγάλη δημοσιότητα από τα ΜΜΕ καθώς αφορούσε υπόθεση τοκογλυφικού κυκλώματος που δρούσε στην

[περιοχή] ΧΧ και συνεπώς η πληροφορία αυτή είχε δημοσιευτεί στον Τύπο και είχε δημοσιοποιηθεί από τα ΜΜΕ έχοντας καταστεί γεγονός κοινώς γνωστό. Η έρευνα διενεργήθηκε από τα αρμόδια όργανα της τράπεζας με τήρηση του καθήκοντος εχεμύθειας χωρίς τη δυνατότητα πρόσβασης τρίτων προσώπων που δεν σχετίζονται με την έρευνα, η δε αναφορά της προσφεύγουσας περί γνώσης χαμηλόβαθμων υπαλλήλων των κινήσεων λογαριασμών, η οποία δεν επιβεβαιώνεται από κάποιο αποδεικτικό στοιχείο, είναι αναληθής.

Η καθής ενημέρωσε ότι διαθέτει Κώδικα Δεοντολογίας ο οποίος αποτελεί το εσωτερικό κανονιστικό της πλαίσιο και θεσπίζει μεταξύ άλλων την υποχρέωση συμμόρφωσης του προσωπικού με το τραπεζικό απόρρητο, την επαγγελματική εχεμύθεια και τη διαφύλαξη εμπιστευτικών πληροφοριών. Επιπλέον οι υπάλληλοι ενημερώνονται σε τακτική βάση μέσω εσωτερικών εγκυκλίων και υπηρεσιακών σημειωμάτων για την υποχρέωση τήρησης των ανωτέρω υποχρεώσεων με υπενθύμιση των κυρώσεων της τράπεζας σε περίπτωση αντιδεοντολογικής συμπεριφοράς εκ μέρους τους. Σε όλα τα παραπάνω έγγραφα υπάρχει σαφής αναφορά στους όρους με τους οποίους γίνεται η εκτέλεση αναζητήσεων σε λογαριασμούς και στοιχεία πελατών, εφιστώντας την προσοχή στην απαγόρευση διενέργειας αναζητήσεων όταν δεν υπάρχει υπηρεσιακή ανάγκη και υπενθυμίζοντας ότι παραβίαση των εν λόγω υποχρεώσεων επιφέρει κυρώσεις. Οι δε αναζητήσεις στους λογαριασμούς της προσφεύγουσας που πραγματοποιήθηκαν κατά το χρονικό διάστημα 1-11-2011 έως 22-12-2011 εμπίπτουν σε τρείς κατηγορίες (α) αναζητήσεις λογαριασμών από την ίδια την προσφεύγουσα μέσω web banking, (β) αναζητήσεις από το κατάστημα στην [περιοχή] ΧΧ όπου ήταν διευθύντρια η αδελφή της και για τις οποίες η ίδια είχε ζητήσει να εξαιρεθεί από τον έλεγχο και γ) αναζητήσεις από τα στελέχη της Δ/νσης Εσωτερικού Ελέγχου (Β, Ε), τους οποίους συνέδραμε στέλεχος που μόλις είχε μετατεθεί στη Δ/νση Κανονιστικής Συμμόρφωσης (Ζ), στο πλαίσιο του διενεργηθέντος ελέγχου. Αναφορικά με τον Η, ο οποίος εμφανίζεται στα αρχεία καταγραφής της καρτέλας πελάτη της [εταιρίας… ΑΕ] να αντιστοιχίζεται στον κωδικό … (2 προσβάσεις στις 23/11/2011), κωδικό που με βάση τόσο τα υπόλοιπα στοιχεία των αρχείων καταγραφής όσο και με βάση την προσφεύγουσα, ανήκει στην Γ, η καθής ανέφερε πως πρόκειται για μεμονωμένο τυπογραφικό σφάλμα.

Η προσφεύγουσα υπέβαλε, σε συνέχεια της συνεδρίασης της 11ης Μαρτίου 2015, το υπ’ αριθμ. πρωτ. Γ/ΕΙΣ/1802/20-03-2015 υπόμνημα, στο οποίο εξέθεσε τις απόψεις της, ως αυτές εκφράστηκαν στη συνεδρίαση. Η τράπεζα δεν προσκόμισε τα

αρχεία καταγραφής των αριθμών λογαριασμών της (στην καρτέλα πελάτη της αντιστοιχούσαν πλέον του ενός λογαριασμού), προσκόμισε δε αντ' αυτού τα αρχεία καταγραφής της καρτέλας πελάτη, προβάλλοντας ότι κάτι τέτοιο θα επιβάρυνε το σύστημά της και καθιστώντας κατ' αυτό τον τρόπο την ενημέρωσή της ελλιπή. Ισχυριζόμενη δε ότι κατά την ακρόαση της υπόθεσης η Αρχή ζήτησε να προσκομιστούν τα ονόματα που αντιστοιχούν στους κωδικούς χρηστών που εμφανίζονται στις λίστες, η τράπεζα προσέθεσε μια στήλη στο εν λόγω αρχείο και καταχώρησε χειρόγραφα τα ονόματα των χρηστών.

Ειδικότερα :

(α) Τα αρχεία καταγραφής που προσκομίστηκαν στην Αρχή δεν έχουν χρονοσήμανση, ήτοι δεν υπάρχει σε κανένα σημείο της εκτύπωσης η ημερομηνία και η ώρα παραγωγής της λίστας.

(β) Στα αρχεία καταγραφής που προσκομίστηκαν στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5533/18-09-2014 έγγραφο σε κάποιες από τις περιπτώσεις δίπλα από τον κωδικό χρήστη … που ανήκει στην Γ εμφανίζεται το όνομα Η (πχ. στις 23/11/2011). Ο Η, όπως αναφέρθηκε και στην ακροαματική διαδικασία, δεν είναι ούτε υπάλληλος του καταστήματος της [οδού…] ούτε της Δ/νσης που καταχώρησε την εντολή παραγωγής των αρχείων καταγραφής που η Τράπεζα προσκόμισε στην Αρχή.

γ) Οι λογαριασμοί της προσφεύγουσας έτυχαν επεξεργασίας από υπαλλήλους όχι μόνον της Δ/νσης Καταστολής και Πρόληψης Απάτης, στην οποία υπηρετεί ο Β, αλλά και του γραφείου Κανονιστικής Συμμόρφωσης (Ζ). Η Ζ ενεπλάκη στην εξέταση της καταγγελίας λόγω της εξοικείωσής της με το μηχανογραφικό σύστημα της τράπεζας. Γενικότερα οι αλλαγές του επιπέδου πρόσβασης των χρηστών του Μηχανογραφικού Συστήματος της Τράπεζας πραγματοποιούνται με τη συμπλήρωση του εντύπου Ε-009, στο οποίο μεταξύ άλλων απαιτούνται αξιολόγηση της ενέργειας και δύο υπογραφές Ανωτέρων Στελεχών για να επιτραπεί. Δεν υπάρχει εγγράφως η εντολή από κάποιον Προϊστάμενο του Β και των υπολοίπων υπαλλήλων της Δ/νσης για την επεξεργασία των λογαριασμών της.

δ) Οι υπάλληλοι της Δ/νσης του Β έχουν πρόσβαση στα αρχεία των πελατών της Τράπεζας χωρίς να υπάρχει καταγεγραμμένη διαδικασία και έλεγχος ανωτέρου επιπέδου, ενώ ταυτόχρονα όλες οι ενέργειες πραγματοποιούνται κατόπιν προφορικής συνεννόησης.

ε) Με βάση έγγραφο εσωτερικής χρήσης της Διαχείρισης Κινδύνου Απάτης (Πολιτική και Διακυβέρνηση), «*Η Διεύθυνση Πρόληψης και Καταστολής Απάτης μπορεί να εξουσιοδοτήσει στέλεχός της να διεξάγει την έρευνα ή συνεντεύξεις. Τα αποτελέσματα της έρευνας δεν θα συζητηθούν με κανέναν άλλο πέραν αυτών που οφείλουν να γνωρίζουν… Όλες οι έρευνες διεξάγονται εντός των ορίων των ισχυόντων νόμων και κανονισμών (πχ. Νόμος Προστασίας Προσωπικών Δεδομένων*». Στο Παράρτημα Α τίθενται κανόνες αναφορικά με τη γνωστοποίηση πιθανού περιστατικού απάτης από υπάλληλο της τράπεζας στην αρμόδια Δ/νση (Δ/νση Πρόληψης και Καταστολής Απάτης). Οι κανόνες αυτοί περιλαμβάνουν: (1) τη γνωστοποίηση στοιχείων του υπόπτου, της πράξης που έχει τελέσει και άλλες σχετικών λεπτομερειών, (2) τον ορθό χειρισμό αποδεικτικών στοιχείων (διασφάλιση αποδεικτικών στοιχείων, μη παρέμβαση σε αυτά, καμία απόπειρα ιδίας διαλεύκανσης της πιθανής απάτης, μη κοινοποίηση αυτής σε οιονδήποτε τρίτο) και (3) την ενδεδειγμένη στάση απέναντι στον ύποπτο (μη επικοινωνία με αυτόν προς προδιορισμό γεγονότων ή προς αποκατάσταση, μη απευθείας αντιμετώπιση αυτού προς αποφυγή προϊδεασμού αυτού και καταστροφής πιθανών αποδεικτικών στοιχείων). Στο ίδιο κείμενο αναφέρεται ότι «*αμέσως μόλις ολοκληρωθεί η έρευνα θα ενημερωθεί η αρμόδια διοικητική ιεραρχία για τα ευρήματα της έρευνας, αποφεύγοντας εικασίες ή κάθε δήλωση η οποία δεν υποστηρίζεται και τεκμηριώνεται από γεγονότα*» (σελ. 20).

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Από τις διατάξεις του άρθρου 10 παρ.1, 2 και 3 του ν. 2472/1997 συνάγεται σαφώς ότι ο υπεύθυνος επεξεργασίας ενός αρχείου έχει την ευθύνη για την τήρηση του απορρήτου κατά τη διεξαγωγή της επεξεργασίας που εκτελείται από υπαλλήλους του, ανεξαρτήτως αν αυτοί ενήργησαν στο πλαίσιο των καθηκόντων τους ή αυτοβούλως. Η επεξεργασία από τον εκτελούντα υπάλληλο δεν απαλλάσσει τον υπεύθυνο από το καθήκον του να ελέγχει και να εξασφαλίζει ότι τα μέτρα ασφάλειας που απαιτεί ο νόμος εφαρμόζονται. Στο πλαίσιο αυτό η τράπεζα πρέπει να λαμβάνει όλα τα οργανωτικά μέτρα για την αποφυγή αθέμιτης επεξεργασίας των δεδομένων, όπως π.χ. να έχει εκπονήσει πολιτική ασφάλειας

της επεξεργασίας, να ακολουθεί κώδικα δεοντολογίας και διαδικασίες ελέγχου για την πρόσβαση εξουσιοδοτημένων προς τούτο υπαλλήλων στο σύστημα, κλπ.

2. Με βάση την παρ. 4 του κώδικα δεοντολογίας της τράπεζας (βλ. Γ/ΕΙΣ/5533/18-09-2014 έγγραφο προς την Αρχή) «*η εκτέλεση αναζητήσεων σε λογαριασμούς και στοιχεία πελατών χωρίς να συντρέχει υπηρεσιακή ανάγκη, μέσω των κεντρικών και περιφερειακών συστημάτων της Τράπεζας, στα οποία έχει πρόσβαση το προσωπικό, είναι αντιδεοντολογική και εκλαμβάνεται ως παραβίαση του Κώδικα*». Σε περίπτωση καταγγελιών, όπως αυτή της προσφεύγουσας, το τμήμα που αναλαμβάνει να διερευνήσει την τυχόν καταγγελία είναι η Διεύθυνση Ελέγχων Λειτουργικών Κινδύνων Καταστημάτων. Σε περίπτωση δε που διαπιστωθεί κάποια παράβαση, την περαιτέρω διερεύνηση αναλαμβάνει το Τμήμα Αποτροπής Απάτης (Fraud Prevention). Η Τράπεζα δεν προσκόμισε, παρότι της ζητήθηκε (Βλ. Γ/ΕΞ/68/12-06-2014 έγγραφο της Αρχής), στοιχεία από τα οποία να προκύπτει ότι τηρήθηκε η ως άνω διαδικασία διερεύνησης περιστατικών παραβίασης προσωπικών δεδομένων, όπως αθέμιτες προσβάσεις σε λογαριασμούς πελατών.

3. Από τα στοιχεία του φακέλου της υπόθεσης, συμπεριλαμβανομένων των υπομνημάτων, και των διεμειφθέντων κατά τη συνεδρίαση της 11-03-2015, προκύπτουν τα ακόλουθα:

α) Από τα προσκομισθέντα αντίγραφα των αρχείων της καθής από το μηχανογραφικό της σύστημα, όπου περιλαμβάνονται οι καταγεγραμμένες προσβάσεις υπαλλήλων της στους επίμαχους λογαριασμούς της προσφεύγουσας, προκύπτουν προσβάσεις το χρονικό διάστημα από 1/11/2011 έως 12/1/2012 στους εταιρικούς λογαριασμούς της [εταιρείας… ΑΕ] (εταιρεία της προσφεύγουσας) (α) μέσω web banking, (β) από το κατάστημα της [οδού…] στην [περιοχή] Χ, κατάστημα με το οποίο συνεργαζόταν, από τους υπαλλήλους Η, Θ, Ι, Κ, Λ, Μ και Ν, (γ) μέσω της υπηρεσίας "xxx", (δ) από το κατάστημα [περιοχής…] από την υπάλληλο Ξ, (ε) από το κατάστημα Δημαρχείου [περιοχής…] από τον υπάλληλο Ο, (στ) από το κατάστημα [περιοχής…] από την υπάλληλο Π, (ζ) από το κατάστημα [περιοχής…] από τις υπαλλήλους Ρ και Σ, (η) από την [υπηρεσία] "zzz" στην [περιοχή] ΧΧ από τους υπαλλήλους Τ και Υ (1 και 5/12/2011, 10/1/2012), (θ) από το κατάστημα [περιοχής…] από την υπάλληλο Φ, (ι) από την υπηρεσία Ελέγχου Λειτουργικών Κινδύνων-Καταστημάτων από τον

υπάλληλο Ψ (27/12/2011) και (κ) από την υπηρεσία Fraud Prevention από τον υπάλληλο Β (12/1/2012). Σημειώνεται ότι στις 23/11/2011 3 διαφορετικοί υπάλληλοι του καταστήματος της [οδού…] (Η, Θ και Κ) εμφανίζονται να αποκτούν πρόσβαση στους λογαριασμούς της εταιρείας… ΑΕ.

β) Αντιστοίχως για το ίδιο χρονικό διάστημα προκύπτουν προσβάσεις στους λογαριασμούς που τηρούσε η Α ως φυσικό πρόσωπο (α) μέσω web banking, (β) από το κατάστημα της [οδού…] από τους υπαλλήλους Γ, Μ, Θ, Ν, Κ και Λ, (γ) μέσω της υπηρεσίας " xxx", (δ) από την ERB EUROLIFE μέσω web banking (14/12/2011), (ε) από το INTERNAL AUDIT DIVISION από τον υπάλληλο Ε (20, 21 και 22/12/2011) και (στ) από τη Δ/ΝΣΗ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ από την υπάλληλο Ζ (22/12/2011). Σημειώνεται ότι στις 18/11/2011 τρεις διαφορετικοί υπάλληλοι του καταστήματος της [οδού…] (Μ, Θ, Ν) εμφανίζονται να αποκτούν πρόσβαση στους λογαριασμούς της Α.
Για τους λόγους που αναφέρθηκαν ανωτέρω, ο έλεγχος της νομιμότητας των επίδικων προσβάσεων περιορίζεται στις αναζητήσεις από τα στελέχη της Δ/νσης Εσωτερικού Ελέγχου στους λογαριασμούς που κατείχε η προσφεύγουσα ως φυσικό πρόσωπο, αφού στα νομικά πρόσωπα δεν παρέχει ο νόμος 2472/1997 έννομη προστασία (βλ. άρθρο 2 του ν. 2472/1997).

γ) Με βάση τα προσκομισθέντα από την τράπεζα αρχεία καταγραφής, στην εξέταση της καταγγελίας της Α αναμείχθηκαν 4 υπάλληλοι της τράπεζας, οι (α) Ζ (Δ/ΝΣΗ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ), (β) Ε (τμήμα INTERNAL AUDIT DIVISION), (γ) Ψ (υπηρεσία Ελέγχου Λειτουργικών Κινδύνων-Καταστημάτων) και (δ) Β (υπηρεσία Fraud Prevention). Η συνδρομή της Ζ ζητήθηκε χωρίς απολύτως καμία διατύπωση λόγω των γνώσεών της, η εν λόγω δε υπάλληλος δεν θα έπρεπε, υπό κανονικές συνθήκες, να έχει πρόσβαση σε αρχεία λογαριασμών πελατών σύμφωνα με την πολιτική Διαχείρισης Κινδύνου και Απάτης (Πολιτική και Διακυβέρνηση). Κατά τους ισχυρισμούς της τράπεζας δεν συντάχθηκε έκθεση ελέγχου αναφορικά με την καταγγελία της Α λόγω μη ύπαρξης ευρημάτων. Σημειώνεται πως δεν προσκομίστηκε από την τράπεζα κανένα σχετικό τεκμήριο (πχ. εσωτερικό έγγραφο εντολής ανάθεσης της έρευνας, σχετικά μηνύματα ηλ. αλληλογραφίας) από το οποίο να προκύπτει ο τρόπος διεξαγωγής της έρευνας και ενδεχομένως και το αποτέλεσμα αυτής. Συνεπώς δεν προκύπτει η διενέργεια τέτοιου

ελέγχου για το οποιοδήποτε πόρισμα του οποίου έστω και αρνητικό θα έπρεπε να συνταχθεί η οικεία έκθεση.

δ) Για τη διερεύνηση της καταγγελίας της Α (βλ. και προηγούμενο σημείο), δε συντάχθηκε όμως σχετική έκθεση ελέγχου, η οποία θα περιέγραφε τουλάχιστον τη διαδικασία που ακολουθήθηκε, τα πειστήρια που συλλέχθηκαν, τον τρόπο συλλογής τους, τη διαδικασία ανάλυσής τους, τα συμπεράσματα της έρευνας, κ.ο.κ. Τα εν λόγω αρχεία καταγραφής του μηχανογραφικού συστήματος της τράπεζας ονόματι …, ως προσκομίστηκαν στην Αρχή, δεν έφεραν καμία χρονοσήμανση αναφορικά με το χρόνο άντλησής τους από το σύστημα. Επιπλέον είχαν αλλοιωθεί, στο βαθμό που εμφανίζονται σε αυτά οι προσβάσεις των υπαλλήλων (Ζ, Ε, Ψ και Β), οι οποίοι διερεύνησαν την καταγγελία.
Σημειώνεται πως με βάση τα διαμειφθέντα κατά την ακρόαση της υπόθεσης, δεν τηρήθηκε από την τράπεζα κανένα αντίγραφο των αρχείων καταγραφής, τα οποία εξετάστηκαν στα πλαίσια διερεύνησης της καταγγελίας.

4. Λαμβάνοντας υπόψη όλα τα ανωτέρω, αποδεικνύονται τα ακόλουθα:

Ως προς το πρώτο σκέλος της προσφυγής, η τράπεζα δεν αιτιολόγησε επαρκώς κατά την ακρόαση και μέσω του υπομνήματός της, τις προσβάσεις στους λογαριασμούς της προσφεύγουσας Α. Ειδικότερα:

- δεν υπάρχουν επίσημα έγγραφα ανάθεσης της διερεύνησης σε αρμόδιους υπαλλήλους της τράπεζας.
- τα αρχεία καταγραφής φαίνεται να έχουν αλλοιωθεί, στο βαθμό που εμφανίζονται σε αυτά οι προσβάσεις των υπαλλήλων (Ζ, Ε, Ψ και Β), οι οποίοι διερεύνησαν την καταγγελία, γεγονός που κλονίζει την αξιοπιστία των αρχείων καταγραφής που προσκομίστηκαν. Εφόσον η Τράπεζα μπορεί να παρεμβαίνει σε μια τέτοια λίστα προσθέτοντας μια στήλη, εύλογα μπορεί να σκεφθεί κάποιος ότι είναι δυνατόν αντίστοιχα να αφαιρέσει μια στήλη ή γραμμή ή ακόμα και να επηρεάσει το περιεχόμενο της. Δεν τεκμηριώθηκε δε για ποιο λόγο οι εν λόγω υπάλληλοι αντί να εξάγουν, όπως ήταν ορθό, τα αρχεία καταγραφής των προσβάσεων στο λογαριασμούς της προσφεύγουσας,

απέκτησαν πρόσβαση στους λογαριασμούς της προσφεύγουσας, προκειμένου να εξετάσουν την καταγγελία της. Οι ισχυρισμοί της τράπεζας που εκτέθηκαν κατά τη συνεδρίαση της Αρχής ότι «μπήκαν» στους λογαριασμούς της προσφεύγουσας αρχικά για να αναζητήσουν τον αριθμό μητρώου του πελάτη και στη συνέχεια για να «προσομοιώσουν» τον τρόπο χρήσης των λογαριασμών δεν μπορούν να γίνουν αποδεκτοί και δεν νομιμοποιούν τις δεκαεπτά (17) προσβάσεις στους προσωπικούς λογαριασμούς της προσφεύγουσας από τους υπαλλήλους Ζ και Ε, στις 20/12/2011 22/12/2011. Αντιστοίχως δεν θα μπορούσαν να αιτιολογηθούν και οι επτά (7) προσβάσεις των Β και Ψ στον εταιρικό λογαριασμό της προσφεύγουσας (εταιρεία… ΑΕ) στις 27/12/2011 και 12/1/2012.

- ουδεμία διαδικασία τεκμηρίωσης σε χρονολογική σειρά (chain of custody) ακολουθήθηκε προκειμένου να μπορεί να αποδειχθεί κατά τρόπο αδιαμφισβήτητο η διαδικασία συλλογής και παρακολουθήσης των πειστηρίων ώστε συνεπακόλουθα να αποδεικνύεται πέραν πάσης αμφιβολίας η εγκυρότητα αυτών (δεν καταγράφηκε ποια είναι τα πειστήρια, πώς, πότε, πού και από ποιον συλλέχτηκαν, ποιος απέκτησε πρόσβαση σε αυτά και γιατί, πού αποθηκεύτηκαν τελικώς, κ.ο.κ. – στην προκειμένη περίπτωση δεν κρατήθηκε κανένα αντίγραφο των εξετασθέντων πειστηρίων).
- δεν υπήρξε έκθεση ελέγχου, η οποία χρησιμοποιώντας επιστημονικά αποδεκτούς κανόνες ψηφιακής εγκληματολογίας (computer forensics), σε συνάρτηση με τους κανόνες λειτουργίας της τράπεζας, να αποδεικνύει ή να απορρίπτει τους ισχυρισμούς της προσφεύγουσας περί αθέμιτης πρόσβασης στους λογαριασμούς της.

Από τα ανωτέρω προκύπτει ότι η τράπεζα Eurobank Ergasias ΑΕ, ως υπεύθυνος επεξεργασίας, δεν ακολούθησε, στην περίπτωση της προσφεύγουσας, τη διαδικασία διερεύνησης των με το ανωτέρω περιεχόμενο καταγγελιών της, καθώς στη διερεύνηση ενεπλάκη και υπάλληλος τμήματος (Δ/ΝΣΗ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ), το οποίο δεν έχει, από όσον γνωστοποιήθηκε στην Αρχή, σχετικές αρμοδιότητες. Δεν τήρησε περαιτέρω τους κανόνες χειρισμού αποδεικτικών στοιχείων που η ίδια αναφέρει σε δικό της εσωτερικό έγγραφο και που η ίδια καλεί τους υπαλλήλους της να τηρήσουν κατά τη γνωστοποίηση

πιθανής απάτης στην αρμόδια Δ/νση, με συνέπεια να μην είναι σε θέση να ελέγξει εάν οι αναζητήσεις στο σύστημά της από τους υπαλλήλους της έχουν γίνει νόμιμα ή όχι. Επιπρόσθετα, αν και έχει λάβει οργανωτικά μέτρα, σύμφωνα με το άρθρο 10 του ν. 2472/1997, (κώδικας δεοντολογίας, πολιτικής προστασίας της πληροφορίας, κ.ο.κ.), τα οποία, μεταξύ άλλων, αφορούν και τις αναζητήσεις υπαλλήλων σε λογαριασμούς πελατών, πραγματοποιήθηκαν προσβάσεις στους λογαριασμούς της προσφεύγουσας χωρίς σχετική εξουσιοδότηση από την Τράπεζα. Η δε Τράπεζα δεν ασκούσε τον δέοντα έλεγχο αν οι υπάλληλοί της ενεργούσαν σύμφωνα με τον νόμο και τις εγκυκλίους και εντολές των αρμοδίων οργάνων της. Ως εκ τούτου, διαπιστώνεται πλημμελής τήρηση οργανωτικών και τεχνικών μέτρων για την ασφάλεια των δεδομένων και την προστασία τους από παράνομη ή αθέμιτη επεξεργασία σύμφωνα με το άρθρο 10 σε συνδυασμό με τα άρθρα 4 και 5 παρ.1 του ν. 2472/1997 που οδήγησαν σε μη νόμιμες πράξεις επεξεργασίας (πρόσβαση και άντληση) στις οποίες υποβλήθηκαν τα δεδομένα της προσφεύγουσας από υπαλλήλους της τράπεζας.

5. Ως προς το δεύτερο σκέλος της προσφυγής, η καθής προέβη σε επεξεργασία προσωπικών δεδομένων της προσφεύγουσας Α, ήτοι σε έλεγχο των λογαριασμών που η καταγγέλλουσα τηρούσε στην καθής Τράπεζα, βάσει του άρθρου 5 παρ. 2 περ. β' του ν. 2472/1997, σύμφωνα με το οποίο η επεξεργασία είναι νόμιμη και δεν απαιτείται προηγούμενη συγκατάθεση του υποκειμένου των δεδομένων, όταν είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από τον νόμο, δηλαδή τις ειδικότερες διατάξεις των ν. 3691/2008 *(Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας και άλλες διατάξεις*) και ν. 3601/2007 *(Ανάληψη και άσκηση δραστηριοτήτων από τα πιστωτικά ιδρύματα, επάρκεια ιδίων κεφαλαίων των πιστωτικών ιδρυμάτων και των επιχειρήσεων παροχής επενδυτικών υπηρεσιών),* οι οποίες εξειδικεύονται με σχετικές πράξεις και αποφάσεις της Τράπεζας της Ελλάδος. Η επεξεργασία αυτή συνίστατο στον έλεγχο των λογαριασμών που η προσφεύγουσα τηρούσε στην καθής Τράπεζα, από κοινού με την αδελφή της Γ, σύζυγο του συλληφθέντος Δ. Οι πληροφορίες για τη συμμετοχή του γαμπρού της προσφεύγουσας και συζύγου της αδελφής της, η οποία ετύγχανε υπάλληλος της καθής και συνδικαιούχος στους επίμαχους λογαριασμούς, στο κύκλωμα τοκογλυφίας υπήρξαν η αφορμή για τη διενέργεια του ελέγχου, βάσει της

υποχρέωσης της καθής που απορρέει, όπως προαναφέρθηκε, από τις ειδικότερες διατάξεις των ν. 3691/2008 και ν. 3601/2007. Περαιτέρω δε η αντιμετώπιση της αιτούσας, ως διατηρούσας κοινό λογαριασμό με την αδελφή της Γ, ήταν δυνατόν να επηρεασθεί ελεγκτικά από το γεγονός ότι ο σύζυγος της συνδικαιούχου της στους κοινούς λογαριασμούς είχε κατηγορηθεί για συμμετοχή στο τοκογλυφικό κύκλωμα και νομιμοποίηση εσόδων από εγκληματικές πράξεις, σύμφωνα με τις ανωτέρω υποχρεώσεις ειδικού ελέγχου της Τράπεζας ως υπευθύνου επεξεργασίας που επιβάλλονται στα τραπεζικά ιδρύματα. Ως εκ τούτου, η επεξεργασία πρέπει να θεωρηθεί νόμιμη (βλ. και αποφάσεις 91/2014 και 116/2014 της Αρχής).

Η, κατά τους ισχυρισμούς της προσφεύγουσας, παράνομη διαρροή προσωπικών της δεδομένων σε τρίτους, μη υπαλλήλους, δεν αποδείχθηκε.

Ενόψει της βαρύτητας των πράξεων που αποδείχθηκαν και της προσβολής που επήλθε στην καταγγέλλουσα από τις παράνομες προσβάσεις στους τραπεζικούς λογαριασμούς της που κατείχε ως φυσικό πρόσωπο, η Αρχή κρίνει ομόφωνα ότι πρέπει να επιβληθούν στον υπεύθυνο της επεξεργασίας οι προβλεπόμενες στο άρθρο 21 παρ.1 εδαφ**.** α’ και β’ του ν. 2472/1997 κυρώσεις που αναφέρονται στο διατακτικό και οι οποίες κρίνονται ανάλογες με τη βαρύτητα των παραβάσεων

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

1. Επιβάλλει στην τράπεζα Eurobank Ergasias ΑΕ, ως υπεύθυνο επεξεργασίας, α) πρόστιμο ύψους πέντε χιλιάδων (5.000) ευρώ για παράνομη επεξεργασία δεδομένων της προσφεύγουσας και β) πρόστιμο ύψους πέντε χιλιάδων (5.000) ευρώ για μη τήρηση κατάλληλων οργανωτικών και τεχνικών μέτρων ασφάλειας, η οποία οδήγησε σε μη εξουσιοδοτημένες προσβάσεις υπαλλήλων της στα προσωπικά δεδομένα της προσφεύγουσας.

2. Απευθύνει σύσταση στην τράπεζα Eurobank Ergasias ΑΕ, ως υπεύθυνο επεξεργασίας, να λάβει κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από παράνομη ή αθέμιτη επεξεργασία, ώστε να τεκμηριώνονται επαρκώς οι προσβάσεις που πραγματοποιούν οι εξουσιοδοτημένοι προς τούτο υπάλληλοί της στους λογαριασμούς των πελατών της (π.χ. ενεργοποίηση μηχανισμών που να μην

επιτρέπουν προσβάσεις σε λογαριασμούς πελατών από μη εξουσιοδοτημένους χρήστες, διενέργεια σε τακτά χρονικά διαστήματα δειγματοληπτικών ελέγχων προς διαπίστωση συμμόρφωσης των υπαλλήλων της με τις σχετικές οδηγίες της τράπεζας). Στην ειδική περίπτωση, όπου υπάρχει καταγγελία για αθέμιτη πρόσβαση σε λογαριασμό πελάτη, συστήνεται στην τράπεζα:

Να ακολουθεί, ορθές διαδικασίες, οργανωτικά άλλα και τεχνικά, προκειμένου να διασφαλίσει ότι η διερεύνηση της καταγγελίας διεξάγεται κατά τρόπο που να συνάδει με τις αρχές της ψηφιακής εγκληματολογίας, στο βαθμό που ακολουθούνται διεθνώς αποδεκτές πρακτικές συλλογής και ανάλυσης ψηφιακών πειστηρίων, όπως αυτές της ACPO[1]. Με βάση τις αρχές αυτές: (1) καμία ενέργεια, η οποία πραγματοποιείται από το άτομο που ερευνά υπόθεση, όπου εμπλέκονται ψηφιακά πειστήρια, δεν θα πρέπει να αλλοιώνει δεδομένα (ψηφιακά πειστήρια), τα οποία αργότερα μπορεί να χρησιμοποιηθούν σε δικαστήριο (αρχή υπ' αριθμ. 1), (2) στην περίπτωση που παραστεί ανάγκη πρόσβασης σε δεδομένα στην «αυθεντική» τους μορφή θα πρέπει η όποια πρόσβαση να πραγματοποιείται από άτομο καταρτισμένο για αυτό και ικανό να εξηγήσει τόσο τη συνάφεια όσο και τις συνέπειες της πρόσβασης αυτής (αρχή υπ' αριθμ. 2), (3) Θα πρέπει να τηρείται ένα αρχείο καταγραφής (audit trail) όλων των ενεργειών που αφορούν τα ψηφιακά πειστήρια. Ένας ανεξάρτητος τρίτος θα πρέπει να μπορεί να εξετάσει αυτές τις ενέργειες καταλήγοντας στο ίδιο συμπέρασμα (αρχή υπ' αριθμ. 3), (4) Το άτομο που είναι υπεύθυνο για την έρευνα είναι υπεύθυνο τόσο για την τήρηση του νόμου όσο και για την τήρηση των προαναφερθέντων αρχών (αρχή υπ' αριθμ. 4).

Ο Αναπληρωτής Πρόεδρος **Η γραμματέας**

Γεώργιος Μπατζαλέξης **Ειρήνη Παπαγεωργοπούλου**

[1] http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf