ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 05-12-2023
Αριθ. Πρωτ.: 3108

ΑΠΟΦΑΣΗ 35/2023
(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε, μετά από πρόσκληση του Προέδρου της, σε τακτική συνεδρίαση σε σύνθεση Τμήματος στην έδρα της την 08/11/2023, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Στη συνεδρίαση μετείχε μέσω τηλεδιάσκεψης ο Γεώργιος Μπατζαλέξης, Αναπληρωτής Πρόεδρος, κωλυομένου του Προέδρου της Αρχής, Κωνσταντίνου Μενουδάκου, και παρέστησαν το αναπληρωματικό μέλος Νικόλαος Λίβος, ως εισηγητής, καθώς και τα αναπληρωματικά μέλη Δημοσθένης Βουγιούκας και Μαρία Ψάλλα, σε αντικατάσταση των τακτικών μελών Κωνσταντίνου Λαμπρινουδάκη και Γρηγόριου Τσόλια οι οποίοι δεν παρέστησαν λόγω κωλύματος αν και κλήθηκαν νομίμως εγγράφως. Στη συνεδρίαση παρέστη, με εντολή του Προέδρου χωρίς δικαίωμα ψήφου, η Χάρις Συμεωνίδου, ειδική επιστήμονας – ελέγκτρια ως βοηθός εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών υποθέσεων της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Με τη με αριθ. πρωτ. Γ/ΕΙΣ/10503/28-09-2022 καταγγελία του, ο Α (στο εξής καταγγέλλων), στρέφεται κατά της Τράπεζας Alpha Bank (στο εξής καταγγελλόμενη), της οποίας τυγχάνει πελάτης και κάτοχος πιστωτικής κάρτας για παράνομη και χωρίς προηγούμενη ενημέρωσή του χορήγηση προσωπικών δεδομένων του στην σύζυγό του. Ειδικότερα, σύμφωνα με την καταγγελία, τον … του … η καταγγελλόμενη Τράπεζα χορήγησε στη σύζυγο του καταγγέλλοντος, κατόπιν αιτήματός της, πληροφορίες σχετικά με το γεγονός ότι ο καταγγέλλων διατηρεί πιστωτική κάρτα στο

όνομά του, καθώς και εκτυπωμένες αποδείξεις όλων των συναλλαγών, τις οποίες ο καταγγέλλων είχε πραγματοποιήσει με την εν λόγω πιστωτική κάρτα τους προηγούμενους 3-4 μήνες, ήτοι πληροφορίες που εμπίπτουν στο τραπεζικό απόρρητο. Όπως υποστηρίζει ο καταγγέλλων, το γεγονός ότι η εκτύπωση είχε γίνει σε κατάστημα της Τράπεζας επιβεβαιώθηκε από υπάλληλο του Καταστήματος Alpha Bank στο Φ στον οποίο ο καταγγέλλων έδειξε τις σχετικές φωτογραφίες, ενώ από την καταγγελία προκύπτει ότι δεν προηγήθηκε ενημέρωση του καταγγέλλοντος ως υποκειμένου των δεδομένων, πριν τη διαβίβαση. Επιπλέον ο καταγγέλλων αναφέρει ότι έχει ήδη προσφύγει για τα καταγγελλόμενα πραγματικά περιστατικά στον Συνήγορο του Καταναλωτή, ενώ λάμβανε τακτικά SMS από την καταγγελλόμενη Τράπεζα με το μήνυμα ότι καταβάλλεται προσπάθεια για να βρεθεί η καλύτερη λύση για την υπόθεσή του. Ο καταγγέλλων αναφέρει επίσης ότι ο λόγος για τον οποίο είχε εκδώσει την εν λόγω πιστωτική κάρτα είναι ότι …. Τέλος, από την καταγγελία προκύπτει ότι ως συνέπεια της αθέμιτης διαρροής των πληροφοριών σχετικά με την ύπαρξη και τις κινήσεις της πιστωτικής κάρτας του καταγγέλλοντος, διαταράχθηκε σημαντικά η οικογενειακή ειρήνη και η σχέση του με τη σύζυγό του (…).

Στο πλαίσιο διερεύνησης της καταγγελίας, η Αρχή με το Γ/ΕΞΕ/3243/13-12-2022 έγγραφο κάλεσε την καταγγελλόμενη να εκθέσει τις απόψεις της επί των καταγγελλομένων, διευκρινίζοντας ιδίως, α) εάν η καταγγελλόμενη χορήγησε πληροφορίες σχετικά με τις συναλλαγές που είχαν πραγματοποιηθεί μέσω της προσωπικής πιστωτικής κάρτας του καταγγέλλοντος στη σύζυγό του, με ποια νομική βάση και διαδικασία, και για ποιο λόγο δεν ενημερώθηκε σχετικά ο καταγγέλλων ως υποκείμενο των δεδομένων, β) πότε έλαβε γνώση η καταγγελλόμενη για το καταγγελλόμενο περιστατικό εκ μέρους του καταγγέλλοντος και σε ποιες ενέργειες προέβη στη συνέχεια. Με την απάντησή της η Τράπεζα κλήθηκε να προσκομίσει τις σχετικές Πολιτικές της Τράπεζας και να διευκρινίσει εάν τα προβλεπόμενα σε αυτές τηρήθηκαν εν προκειμένω, προσδιορίζοντας ειδικότερα εάν χειρίστηκε τα καταγγελλόμενα ως περιστατικό παραβίασης προσωπικών δεδομένων σύμφωνα με τα άρθρα 33-34 ΓΚΠΔ και αιτιολογώντας την απάντησή της.

Με την υπ’ αρ. πρωτ. Γ/ΕΙΣ/125/09-01-2023 απάντησή της, η καταγγελλόμενη Τράπεζα ανέφερε τα εξής:

- Ότι ο καταγγέλλων τυγχάνει πελάτης της Alpha Bank, όπως και η σύζυγός του, και στις … υπέβαλε παράπονο για διαρροή προσωπικών του δεδομένων και συγκεκριμένα κινήσεων της πιστωτικής του κάρτας …, η οποία είχε εκδοθεί στο όνομά του χωρίς έτερο δικαιούχο (πρόσθετη κάρτα). Σύμφωνα με την Τράπεζα, η αρμόδια Υπηρεσία παρέλαβε το αίτημα αλλά τα στοιχεία που είχαν γνωστοποιηθεί από τον καταγγέλλοντα δεν ήταν επαρκή για την έναρξη σχετικής έρευνας, καθώς θα έπρεπε να εντοπιστεί ο τρόπος και η προέλευση της διαρροής τους, δεδομένου ότι δυνητικά θα μπορούσε να είναι οποιοδήποτε Κατάστημα της Τράπεζας, ενώ δεν μπορούσε να προσδιοριστεί το χρονικό διάστημα στο οποίο θα έπρεπε να εκτείνεται η έρευνα, διότι ήταν γνωστή μόνο η λήξη του εν λόγω διαστήματος (η …) και όχι η έναρξή του. Η καταγγελλόμενη πάντως αναφέρει ότι ο πελάτης – καταγγέλλων πιθανολογούσε ότι πηγή της διαρροής ήταν το Κατάστημα Χ και ότι τον ενημέρωσε όσον αφορά την παραλαβή του αιτήματος και την έναρξη επεξεργασίας του με τρία (3) μηνύματα sms (στις … και …).

- Ότι στις … ο καταγγέλλων επανήλθε με νεότερο μήνυμά του μέσω e-mail, με συνημμένη ασπρόμαυρη φωτογραφία αντιγράφου κινήσεων λογαριασμού της κάρτας του, το οποίο κατά τον ίδιο, είχε διαβιβαστεί/παραδοθεί στη σύζυγό του από άγνωστο λειτουργό της Τράπεζας «στον Ψ ή στη Χ». Κατόπιν αυτού, η Υπηρεσία της Τράπεζας διαβίβασε, σύμφωνα με την απάντηση της καταγγελλόμενης, στις … το αίτημα του καταγγέλλοντος στην αρμόδια Διεύθυνση Εσωτερικού Ελέγχου προκειμένου να εκκινήσει σχετική έρευνα, αλλά εκ παραδρομής, όπως αναφέρει, δεν διαβίβασε τα επιπλέον στοιχεία που παρέλαβε στις …, με αποτέλεσμα, λόγω έλλειψης στοιχείων που θα περιόριζαν το εύρος της έρευνας, ο Εσωτερικός Έλεγχος να ζητήσει στις … διευκρινίσεις και περαιτέρω στοιχεία από την Υπηρεσία της Τράπεζας που διαχειριζόταν την υπόθεση. Υποστηρίζει επίσης ότι για τη δυσκολία αυτή στην άμεση ανταπόκριση της Τράπεζας, ενημερώθηκε ο καταγγέλλων με τέσσερα (4) μηνύματα sms στο κινητό του με ημ/νίες (… και …).

- Ότι, στη συνέχεια, στις … παρελήφθη από την καταγγελλόμενη μέσω του Συνηγόρου του Καταναλωτή αίτημα/αναφορά του καταγγέλλοντος για το ίδιο θέμα, στο οποίο αναφερόταν ότι η σύζυγός του στις … του επέδειξε ως «αποδείξεις» αντίγραφα κινήσεων του λογαριασμού της κάρτας του, ισχυριζόμενη ότι τα έγγραφα αυτά είχαν προέλθει από την πρόσβασή της στο web banking υποκλέπτοντας τους

κωδικούς του. Στο αίτημα αυτό υπήρχε συνημμένη η ασπρόμαυρη φωτογραφία του ανωτέρω αντιγράφου λογαριασμού καθώς και νεότερα στοιχεία για την υπόθεση και έτσι, σύμφωνα με την εν λόγω απάντηση, η Υπηρεσία της Τράπεζας στις … απευθύνθηκε εκ νέου στον Εσωτερικό Έλεγχο παρέχοντας το σύνολο των στοιχείων που είχε πλέον στη διάθεσή της, ώστε να εκκινήσει η σχετική έρευνα, ενώ στις … λειτουργός της αρμόδιας Υπηρεσίας κάλεσε τον καταγγέλλοντα για την παροχή διευκρινίσεων και την επιβεβαίωση των στοιχείων που είχαν τεθεί υπόψη της.

- Ότι στις … εκδόθηκε το σχετικό πόρισμα του Εσωτερικού Ελέγχου, με το οποίο επιβεβαιώθηκε η διαρροή προσωπικών δεδομένων του καταγγέλλοντος, για την οποία καταλογίζεται ευθύνη σε Λειτουργό του Καταστήματος Ω Χ (με κωδικό …). Παρ' όλα αυτά, σύμφωνα με το πόρισμα, δεν διαγνώσθηκε δόλος εκ μέρους της Λειτουργού καθότι, όπως αναφέρει η Τράπεζα: α) τα προσωπικά δεδομένα του καταγγέλλοντος γνωστοποιήθηκαν κατόπιν αιτήματος άμεσα συγγενούς προσώπου (συζύγου), β) η σύζυγος του καταγγέλλοντα, η οποία υπήρξε εσφαλμένα αποδέκτης των δεδομένων του, τυγχάνει συνδικαιούχος του σε άλλα προϊόντα της Τράπεζας καθώς και κάτοχος πρόσθετης πιστωτικής κάρτας με κύριο δικαιούχο τον καταγγέλλοντα, γ) η διαρροή πραγματοποιήθηκε στο πλαίσιο εξυπηρέτησης / ενημέρωσης της συζύγου του καταγγέλλοντα για μια σειρά από προϊόντα, στα οποία είναι δικαιούχος ή συνδικαιούχος η ίδια, με το τελευταίο εξ αυτών να αφορά την επίμαχη πιστωτική κάρτα του καταγγέλλοντα συζύγου της και δ) η σύζυγος του καταγγέλλοντα παραπλάνησε την Λειτουργό του Καταστήματος ισχυριζόμενη ότι είχε δήθεν τη σχετική εξουσιοδότηση του κατόχου της κάρτας και συζύγου της για την παραλαβή αντιγράφου των κινήσεων της πιστωτικής κάρτας του.

Περαιτέρω, αναφορικά με τη διαχείριση του περιστατικού ως παραβίαση προσωπικών δεδομένων, με την ίδια απάντηση η καταγγελλόμενη Τράπεζα ανέφερε τα εξής:

- Ότι με την επιβεβαίωση της Παραβίασης της Εμπιστευτικότητας των δεδομένων η τράπεζα, μέσω των αρμόδιων Υπηρεσιών της προέβη σε μια σειρά από ενέργειες:

- Στις … συνεδρίασε το Συμβούλιο Διαχείρισης Γεγονότων Λειτουργικού Κινδύνου και, μεταξύ άλλων, αποφάσισε την παραπομπή της Λειτουργού για την οποία προέκυψαν ευθύνες, στο Πειθαρχικό Συμβούλιο για τη μη τήρηση των Πολιτικών της Τράπεζας.

- Στις … συνεδρίασε η Επιτροπή Αξιολογήσεως Περιστατικών Παραβιάσεως Προσωπικών Δεδομένων σύμφωνα με τη σχετική Πολιτική της Τράπεζας, η οποία εκτίμησε ότι, με βάση τις συνθήκες του περιστατικού και ιδίως του ότι οι μη εξουσιοδοτημένοι αποδέκτες των δεδομένων περιορίζονται σε ένα άτομο συγγενικό με τον καταγγέλλοντα (σύζυγος) «*δεν φαίνεται να προκύπτει κίνδυνος για τις ελευθερίες και τα δικαιώματά του ως υποκειμένου*».
- Το περιστατικό καταχωρίστηκε στο Μητρώο Περιστατικών Παραβιάσεως Δεδομένων (προσκομίζεται ως συν. 1) και συμπληρώθηκε η Φόρμα Αναλύσεως Κινδύνου Περιστατικών Παραβιάσεως Προσωπικών Δεδομένων (προσκομίζεται ως συν. 2). Σύμφωνα με την εν λόγω Φόρμα Αναλύσεως Κινδύνου, ο κίνδυνος για το υποκείμενο αξιολογείται ως «αμελητέος».
- Την … ενημέρωσε με μήνυμα μέσω ηλεκτρονικού ταχυδρομείου τον καταγγέλλοντα για το συμβάν και το αποτέλεσμα της σχετικής έρευνας και
- Στις … συνεδρίασε το Πειθαρχικό Συμβούλιο της Τράπεζας και αναμένεται σχετική απόφαση.

Με βάση τα ανωτέρω η Τράπεζα υποστηρίζει ότι εξέτασε το αίτημα του καταγγέλλοντος με τη δέουσα προσοχή, ότι «*προχώρησε στην απαιτούμενη διερεύνηση όταν είχε στη διάθεσή της τα απαραίτητα στοιχεία για να προβεί στον σχετικό έλεγχο, καθώς η πρόσκαιρη έλλειψή τους καθιστούσε ανέφικτη τη διεξαγωγή του ή θα οδηγούσε σε απασχόληση δυσανάλογα αυξημένων πόρων και θα επιμήκυνε σημαντικά τη διεξαγωγή του*». Τέλος, η Τράπεζα με το ίδιο έγγραφο προσκόμισε στην Αρχή την Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (συν. 4), το Πλαίσιο Κυβερνοασφάλειας και Ασφάλειας Πληροφοριών Ομίλου (συν. 5) και τη Διαδικασία Γνωστοποιήσεως Παραβιάσεων Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Data Breach Management) (συν. 6) και τόνισε ότι αναλαμβάνει πρωτοβουλίες συνεχούς εκπαίδευσης του προσωπικού της σε θέματα προστασίας

προσωπικών δεδομένων. Στο κείμενο αυτό, μεταξύ άλλων, προβλέπονται τα εξής: «*2.1 ΑΝΑΦΟΡΑ ΥΠΟΠΤΟΥ ΣΥΜΒΑΝΤΟΣ*

Όλα τα πιθανά περιστατικά ασφαλείας, συμπεριλαμβανομένων εκείνων που ενδέχεται να αποτελούν περιστατικά παραβιάσεως ή αποτελούν επιβεβαιωμένα περιστατικά παραβιάσεως δεδομένων προσωπικού χαρακτήρα, αναφέρονται ***άμεσα****:*

μέσω ηλεκτρονικού ταχυδρομείου:

Προς: privacy@alpha.gr

Κοινοποίηση: Διεύθυνση Κινδύνων Αγοράς και Λειτουργικών Κινδύνων

ή

τηλεφωνικώς, τηλ. 210 326 6965, τη Διεύθυνση Υποστηρικτικών Λειτουργιών, η οποία ενημερώνει ***άμεσα*** *τους κάτωθι:*

ο τον Υπεύθυνο Προστασίας Δεδομένων Ομίλου (εφεξής «ΥΠΔΟ») και

ο τη Διεύθυνση Κυβερνοασφάλειας και Ασφαλείας Πληροφοριών (εφεξής «ΔΚΑΠ»)

Τα πιθανά περιστατικά ασφαλείας δύνανται να τα αναφέρουν στην Τράπεζα, υπό την ιδιότητά της ως υπευθύνου επεξεργασίας, οι κάτωθι:

1. Μονάδες της Τραπέζης: Αναφέρουν συμβάντα τα οποία υπέπεσαν στην αντίληψή τους, τα οποία ενδεχομένως αφορούν περιστατικό ασφαλείας, και δη περιστατικό παραβιάσεως δεδομένων προσωπικού χαρακτήρα. Οι Μονάδες αυτές συμπληρώνουν αμελλητί το έντυπο «Αναγγελία Γεγονότος Λειτουργικού Κινδύνου» (Κωδ. Εντύπου 15031), κατά τα προβλεπόμενα στην Πολιτική Διαχειρίσεως Λειτουργικού Κινδύνου και το αποστέλλουν μέσω e-mail με βάση τα ανωτέρω.» […]

«2.4 ΑΞΙΟΛΟΓΗΣΗ ΠΕΡΙΣΤΑΤΙΚΟΥ ΠΑΡΑΒΙΑΣΕΩΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Είναι πολύ σημαντικό, αμέσως μόλις επιβεβαιωθεί ότι το περιστατικό αφορά παραβίαση δεδομένων προσωπικού χαρακτήρα, όχι μόνον να εκτελεστούν οι αρχικές ενέργειες προς αντιμετώπισή του, αλλά και να αξιολογηθεί ο κίνδυνος του περιστατικού παραβιάσεως, βάσει των επιπτώσεων που ενδέχεται να επιφέρει στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων».

Σε συνέχεια των ανωτέρω, η Αρχή με τις Γ/ΕΞΕ/730/22-03-2023 και Γ/ΕΞΕ/731/22-03-2023 κλήσεις αντίστοιχα, κάλεσε τον καταγγέλλοντα και την καταγγελλόμενη σε ακρόαση, μέσω τηλεδιάσκεψης, ενώπιον του Τμήματος της Αρχής στις …, προκειμένου να εκθέσουν τις απόψεις τους για την υπόθεση. Κατά τη συνεδρίαση

της …, η υπόθεση αναβλήθηκε κατόπιν αιτήματος της καταγγελλόμενης, για τη συνεδρίαση της …, οπότε και αναβλήθηκε εκ νέου, κατόπιν αιτήματος του καταγγέλλοντος, για τη συνεδρίαση της ….

Στη συνεδρίαση της … παρέστησαν, μέσω τηλεδιάσκεψης, ο καταγγέλλων και εκ μέρους της καταγγελλόμενης Τράπεζας, οι δικηγόροι Ιωάννης Μούργελας (ΑΜ ΔΣΑ …), η Αγγελική Σακοπούλου (ΑΜ ΔΣΑ …), ενώ παρέστη και ο Β, Υπεύθυνος Προστασίας Δεδομένων της Τράπεζας. Κατά την ακρόαση τα μέρη ανέπτυξαν τις απόψεις τους και έλαβαν προθεσμία για την υποβολή υπομνήματος. Στη συνέχεια η καταγγελλόμενη κατέθεσε εμπρόθεσμα το από … υπ' αριθ. πρωτ. Γ/ΕΙΣ/4899/03-07-2023 υπόμνημά της, ενώ ο καταγγέλλων δεν κατέθεσε υπόμνημα.

Κατά την ακρόαση, ο καταγγέλλων επανέλαβε τα αναφερόμενα στην καταγγελία του, τονίζοντας το γεγονός ότι η πιστωτική κάρτα ήταν αποκλειστικά στο όνομά του, ότι τόσο ο ίδιος όσο και η σύζυγός του είναι "Gold Members" της καταγγελλόμενης Τράπεζας και η σύζυγός του είναι τακτική πελάτης στο κατάστημα Χ, ότι στο πλαίσιο της εκδίκασης της αγωγής του κατά της καταγγελλόμενης Τράπεζας, υπάλληλος της τελευταίας κατέθεσε ψευδώς ότι η σύζυγός του είχε την εξουσιοδότησή του για να λάβει πληροφορίες σε σχέση με την πιστωτική του κάρτα και ότι η Τράπεζα, αφού επί 3-4 μήνες του έστελνε μηνύματα (sms) απολογούμενη για την καθυστέρηση, τελικά τον ενημέρωσε μέσω e-mail ότι καλώς έπραξε που χορήγησε τις πληροφορίες στη σύζυγό του, διότι είχε την εξουσιοδότησή του, πράγμα που, όπως υποστηρίζει ο καταγγέλλων, δεν ίσχυε. Επιπλέον, όπως διευκρίνισε ο καταγγέλλων, η σύζυγός του δεν γνώριζε τον αριθμό της κάρτας του.

Η καταγγελλόμενη, τόσο κατά την ακρόαση όσο και με το από … υπόμνημά της υποστήριξε ότι στο αρχικό από … παράπονό του, ο καταγγέλλων δεν προσδιόριζε το κατάστημα από το οποίο συνέβη η διαρροή «ούτε καν κατά περιοχή», με αποτέλεσμα να μην είναι αντικειμενικά δυνατό η διερεύνηση να οδηγήσει σε συγκεκριμένο συμπέρασμα. Ωστόσο, η καταγγελλόμενη προσκομίζει το εν λόγω αίτημα (ως συνημμένο 1), από το οποίο προκύπτει ότι ο καταγγέλλων αναφέρει ρητά ότι «υποπτεύεται το κατάστημα της Χ», ενώ και στο Γ/ΕΙΣ/125/9-1-2023 έγγραφο απόψεών της η καταγγελλόμενη αναφέρει ότι ο καταγγέλλων στο αρχικό του αίτημα «πιθανολογούσε ότι πηγή της διαρροής ήταν το Κατάστημα Χ». Περαιτέρω, η καταγγελλόμενη κατά την ακρόαση και με το υπόμνημά της υποστήριξε ότι, παρότι

με το από … δεύτερο αίτημά του ο καταγγέλλων προσκόμισε φωτογραφία εκτύπωσης (στις …) της κίνησης λογαριασμού της κάρτας του η οποία είχε δοθεί στη σύζυγό του και παρότι προσδιόρισε ότι η διαρροή έγινε μεταξύ Ψ και Χ, και πάλι η Τράπεζα δεν ήταν σε θέση να εντοπίσει την πηγή της διαρροής, δεδομένου ότι δεν προσδιορίστηκε ο ακριβής χρόνος αυτής. Ειδικότερα, η Τράπεζα αναφέρει ότι κατά μήκος του παραλιακού μετώπου μεταξύ Ψ και Χ υπάρχουν … Καταστήματά της, στα οποία υπηρετούν … λειτουργοί και σε καθένα από αυτά διενεργούνται καθημερινά κατά μ.ό. 100-120 συναλλαγές, επομένως η έρευνά της έστω και για διάστημα 35 εργασίμων ημερών (από … μέχρι …) θα έπρεπε να εκτείνεται σε πολλές χιλιάδες συναλλαγές. Ως εκ τούτου, κατά την καταγγελλόμενη Τράπεζα, «είναι προφανής η πολύ μεγάλη δυσκολία για την ολοκλήρωση ενός τέτοιου έργου ώστε να διαπιστωθεί εάν πράγματι υπήρξε διαρροή, από ποιο κατάστημα, και ποιων ακριβώς δεδομένων». Επιπλέον, η καταγγελλόμενη επανέλαβε τον ισχυρισμό ότι όταν το από … αίτημα του καταγγέλλοντος διαβιβάστηκε στις … στη Διεύθυνση Εσωτερικού Ελέγχου της Τράπεζας προκειμένου να εκκινήσει έρευνα, *εκ παραδρομής* δεν διαβιβάστηκαν και τα πρόσθετα στοιχεία, δηλαδή η προσκομισθείσα φωτογραφία της εκτύπωσης της κίνησης λογαριασμού της κάρτας του καταγγέλλοντος, προσθέτοντας ότι στην παραδρομή αυτή συνέβαλε το γεγονός ότι επρόκειτο για μια «όχι πλήρη φωτογραφία ενός μηνιαίου λογαριασμού μιας κάρτας». Επιπλέον, κατά την καταγγελλόμενη, στη φωτογραφία αυτή δεν αναφέρεται κάποιο κατάστημα αλλά μόνο η ημερομηνία έκδοσης του αντιγράφου κινήσεων του λογαριασμού (…), το όνομα του κατόχου αυτής, ο αριθμός της κάρτας, το πιστωτικό όριο αυτής και το νέο (χρεωστικό) υπόλοιπο, καθώς και τα στοιχεία των συναλλαγών που πραγματοποιήθηκαν στο χρονικό διάστημα που το αντίγραφο κάλυπτε. Κατά την Τράπεζα, η διαρροή των δεδομένων συναλλαγών που απεικονίζονται σε αυτό «*δεν φαίνεται να θέτουν ούτε κατ' ελάχιστο σε κίνδυνο τις ελευθερίες και τα δικαιώματα του κατόχου της κάρτας*», διότι «*αυτά περιορίζονται στις ημερομηνίες κατά τις οποίες οι συναλλαγές πραγματοποιήθηκαν, στις επιχειρήσεις στις οποίες αυτές πραγματοποιήθηκαν, όπως πχ …, καθώς και στο ποσό της κάθε μιας συναλλαγής, χωρίς καμία απολύτως αναφορά στα συγκεκριμένα αγαθά ή υπηρεσίες που αγοράσθηκαν, ώστε δεν ήταν αντικειμενικά εφικτός ο συσχετισμός των συναλλαγών αυτών με κάποιο πρόσωπο για το οποίο αυτές έγιναν*» και διότι είχαν χαμηλό ύψος,

ως «*καθημερινές μικρο-συναλλαγές*». Περαιτέρω, η Τράπεζα ισχυρίζεται ότι ο καταγγέλλων δεν της παρείχε όλες τις πληροφορίες που είχε στη διάθεσή του για το σκοπό της διερεύνησης του περιστατικού, καθώς ο ισχυρισμός της συζύγου του ότι είχε χρησιμοποιήσει τους κωδικούς του για το web banking έγινε γνωστός στην τράπεζα για πρώτη φορά στις …, όταν της γνωστοποιήθηκε η αναφορά που εκκρεμούσε ενώπιον του Συνηγόρου του Καταναλωτή, ενώ, όπως ο καταγγέλλων ανέφερε στο από … μήνυμά του αλλά και κατά την ακρόαση, ενώ γνώριζε το κατάστημα και τον υπάλληλο που ευθυνόταν, δεν ήθελε να τα αναφέρει στην Τράπεζα. Για το λόγο αυτό, η καταγγελλόμενη Τράπεζα υποστηρίζει ότι ο καταγγέλλων φέρει σημαντική ευθύνη για την καθυστέρηση στην έρευνα του περιστατικού. Επιπλέον, η Τράπεζα αναφέρει ότι η υπαίτια υπάλληλος κακώς δέχθηκε ως επαρκή την προφορική εξουσιοδότηση του συζύγου, παρά τις εσωτερικές διαδικασίες και οδηγίες της Τράπεζας, όμως ενήργησε καλόπιστα λόγω παραπλάνησής της, με γνώμονα την εξυπηρέτηση του πελάτη, βάσει της μακροχρόνιας σχέσης του ζεύγους με την Τράπεζα, το πλήθος των κοινών τους προϊόντων και το γεγονός ότι η σύζυγος γνώριζε την ύπαρξη αλλά και τον αριθμό της πιστωτικής κάρτας του καταγγέλλοντος. Ακολούθως, η Τράπεζα υποστηρίζει ότι το περιστατικό αντιμετωπίσθηκε ως παραβίαση προσωπικών δεδομένων, ακολουθήθηκαν όλες οι σχετικές διαδικασίες καταγραφής και χειρισμού του, η υπαίτια υπάλληλος παραπέμφθηκε στο Πειθαρχικό Συμβούλιο και τιμωρήθηκε αυστηρά με πειθαρχική ποινή παύσης ενός (1) μήνα, ενώ δεν έγινε γνωστοποίηση προς το υποκείμενο κατ' άρθρο 34 ΓΚΠΔ δεδομένου ότι το ίδιο είχε ενημερώσει την Τράπεζα για το περιστατικό, ούτε και προς την Αρχή, κατ' άρθρο 33 ΓΚΠΔ, διότι «*αφορούσε μόνο ένα υποκείμενο και δεν υπήρχε περίπτωση να επηρέαζε τα δικαιώματα και τις ελευθερίες του ίδιου του υποκειμένου ή άλλων φυσικών προσώπων*». Με το υπόμνημά της, η Τράπεζα προσκομίζει το αρχικό από … παράπονο του καταγγέλλοντος, τα ενημερωτικά sms που του απέστειλε η Τράπεζα, την ασπρόμαυρη φωτογραφία της εκτύπωσης, την καταγγελία στον Συνήγορο του Καταναλωτή, το από … αίτημα του καταγγέλλοντος, μια ένορκη βεβαίωση της διευθύντριας (κατά το χρόνο του περιστατικού) του Καταστήματος Ω Χ, καθώς και εκ νέου την Πολιτική Προστασίας Δεδομένων της Τράπεζας, την οποία είχε προσκομίσει και ως σχετ. 4 του υπ' αρ. πρωτ. Γ/ΕΙΣ/125/09-01-2023 απαντητικού της εγγράφου.

Η Αρχή, μετά από εξέταση των στοιχείων του φακέλου και αφού άκουσε τον εισηγητή και τις διευκρινίσεις από τη βοηθό εισηγητή, η οποία παρέστη χωρίς δικαίωμα ψήφου, κατόπιν διεξοδικής συζητήσεως,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Από τις διατάξεις των άρθρων 51 και 55 του Γενικού Κανονισμού Προστασίας Δεδομένων (Κανονισμού (ΕΕ) 2016/679 – εφεξής, ΓΚΠΔ) και του άρθρου 9 του νόμου 4624/2019 (ΦΕΚ Α΄ 137) προκύπτει ότι η Αρχή έχει αρμοδιότητα να εποπτεύει την εφαρμογή των διατάξεων του ΓΚΠΔ, του νόμου αυτού και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων. Ειδικότερα, από τις διατάξεις των άρθρων 57 παρ. 1 στοιχ. στ΄ του ΓΚΠΔ και 13 παρ. 1 στοιχ. ζ΄ του νόμου 4624/2019 προκύπτει ότι η Αρχή έχει αρμοδιότητα να επιληφθεί της καταγγελίας του Α κατά της Alpha Bank και να ασκήσει, αντίστοιχα, τις εξουσίες που της απονέμονται από τις διατάξεις των άρθρων 58 του ΓΚΠΔ και 15 του νόμου 4624/2019.

2. Με το άρθρο 5 παρ. 1 του Γενικού Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (εφεξής ΓΚΠΔ) τίθενται οι αρχές που πρέπει να διέπουν μια επεξεργασία. Σύμφωνα με το άρθρο 5 παρ. 1 α) και στ) ΓΚΠΔ «*1. Τα δεδομένα προσωπικού χαρακτήρα: α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»), […] στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»)*», ενώ όπως επισημαίνεται στο Προοίμιο του Κανονισμού, «*Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υφίστανται επεξεργασία κατά τρόπο που να διασφαλίζει την ενδεδειγμένη προστασία και εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων και για να αποτρέπεται κάθε ανεξουσιοδότητη πρόσβαση*

σε αυτά τα δεδομένα προσωπικού χαρακτήρα και στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία τους ή η χρήση αυτών των δεδομένων προσωπικού χαρακτήρα και του εν λόγω εξοπλισμού» (Αιτ. Σκ. 39 in fine). Περαιτέρω, σύμφωνα με την αρχή της λογοδοσίας που ορίζεται ρητώς στην δεύτερη παράγραφο του ιδίου άρθρου και συνιστά ακρογωνιαίο λίθο του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας «*φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»)*». Η αρχή αυτή συνεπάγεται την υποχρέωση του υπευθύνου επεξεργασίας να δύναται να αποδείξει συμμόρφωση με τις αρχές του άρθ. 5 παρ. 1.

3. Σύμφωνα με τη διάταξη του άρθρου 24 παρ. 1 ΓΚΠΔ: «*1. Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο*», ενώ σύμφωνα με τις διατάξεις των παρ. 1 και 2 του άρθρου 32 ΓΚΠΔ για την ασφάλεια της επεξεργασίας, «*1. Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, […] 2. Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία*».

4. Σύμφωνα με το άρθρο 4 αρ. 12 ΓΚΠΔ ως παραβίαση δεδομένων προσωπικού χαρακτήρα νοείται «*η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων*

προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία». Σύμφωνα με τις από 06-02-2018 Κατευθυντήριες Γραμμές 18/2018 της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ (νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων) για την Γνωστοποίηση παραβίασης προσωπικών δεδομένων ("*Guidelines on Personal data breach notification under Regulation 2016/679" WP 250 rev. 1*) ένας από τους τύπους παραβίασης προσωπικών δεδομένων είναι αυτός που κατηγοριοποιείται με βάση την αρχή ασφαλείας της «εμπιστευτικότητας», όταν διαπιστώνεται πρόσβαση άνευ δικαιώματος σε προσωπικά δεδομένα ("confidentiality breach"). Μια παραβίαση μπορεί δυνητικά να έχει διάφορες σημαντικές δυσμενείς συνέπειες στα πρόσωπα, οι οποίες μπορούν να οδηγήσουν σε σωματική, υλική ή ηθική βλάβη. Στον ΓΚΠΔ επεξηγείται ότι αυτή η βλάβη μπορεί να περιλαμβάνει απώλεια του ελέγχου επί των δεδομένων προσωπικού χαρακτήρα τους, περιορισμό των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, βλάβη της φήμης και απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο κλπ. (βλ. και αιτ. σκέψεις 85 και 75).

5. Τα περιστατικά παραβίασης δεδομένων πρέπει να γνωστοποιούνται στην Αρχή εντός 72 ωρών από τη στιγμή που έλαβε γνώση τους ο υπεύθυνος επεξεργασίας, σύμφωνα με το άρθρο 33 παρ. 1 ΓΚΠΔ: «*1. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση».* Σύμφωνα δε με την αιτιολογική σκέψη 85, αμέσως μόλις ο υπεύθυνος επεξεργασίας λάβει γνώση μιας παραβίασης δεδομένων προσωπικού χαρακτήρα, «*θα πρέπει αμελλητί να την γνωστοποιήσει στην αρμόδια εποπτική αρχή, εκτός εάν μπορεί να αποδείξει, σύμφωνα με την αρχή της λογοδοσίας, ότι η*

παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων». Επισημαίνεται ότι σύμφωνα με τη διατύπωση του άρθρου 33 ΓΚΠΔ και σε αντιδιαστολή με τη διατύπωση του άρθρου 34 ΓΚΠΔ, για την υποχρέωση γνωστοποίησης προς την Αρχή δεν προϋποτίθεται η ύπαρξη «*υψηλού κινδύνου*» για το υποκείμενο αλλά απλώς «*κινδύνου*» για τα δικαιώματα και τις ελευθερίες του. Σύμφωνα δε με τις ανωτέρω Κατευθυντήριες Γραμμές της ΟΕ 29 «*Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι, σε περίπτωση παραβίασης που "δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων", δεν απαιτείται γνωστοποίηση στην εποπτική αρχή. Ένα παράδειγμα μπορεί να είναι η περίπτωση όπου τα δεδομένα προσωπικού χαρακτήρα είναι ήδη διαθέσιμα στο κοινό και η κοινοποίησή τους δεν επιφέρει πιθανό κίνδυνο για το πρόσωπο*» (wp 250 rev.01, σελ.21). Εκ των ανωτέρω προκύπτει ότι με τον ΓΚΠΔ θεσπίζεται «τεκμήριο» υποχρέωσης γνωστοποίησης των περιστατικών παραβίασης στην Αρχή, με μόνη εξαίρεση την απουσία κινδύνου για τα δικαιώματα και τις ελευθερίες των θιγόμενων υποκειμένων, για την οποία ο υπεύθυνος επεξεργασίας φέρει το βάρος απόδειξης, εφόσον επιλέξει να μην προβεί σε τέτοια γνωστοποίηση. [1]

6. Η γνωστοποίηση πρέπει να έχει το ελάχιστο περιεχόμενο που αναφέρεται στην παρ. 3 του άρθρου 33 ΓΚΠΔ, ενώ σύμφωνα με την παρ. 5 του ιδίου άρθρου «*Ο*

[1] Βλ. και τις Κατευθυντήριες 09/2022 του ΕΣΠΔ για τη γνωστοποίηση περιστατικών παραβίασης (§39–40): "*Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.*

• Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.

• Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.

• Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.

• At the same time, the controller should act to contain and recover the breach. Documentation of the breach should take place as it develops.

40. Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) GDPR have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33 GDPR."

υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο». Όσον αφορά το χρόνο λήψης γνώσης του περιστατικού από τον Υπεύθυνο Επεξεργασίας, στις ως άνω ΚΓ 18/2018 της ΟΕ 29 (wp 250) αναφέρονται τα εξής: «*Όπως αναφέρεται λεπτομερώς παραπάνω, ο ΓΚΠΔ απαιτεί, σε περίπτωση παραβίασης, ο υπεύθυνος επεξεργασίας να γνωστοποιεί την παραβίαση αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος. Αυτό μπορεί να εγείρει το ερώτημα πότε ένας υπεύθυνος επεξεργασίας μπορεί να θεωρείται ότι αποκτά «γνώση» μιας παραβίασης. Η ΟΕ29 θεωρεί ότι ένας υπεύθυνος επεξεργασίας θα πρέπει να θεωρείται ότι έχει αποκτ[ήσει] «γνώση» όταν ο εν λόγω υπεύθυνος επεξεργασίας έχει εύλογο βαθμό βεβαιότητας ότι έχει προκύψει περιστατικό ασφάλειας το οποίο έχει ως αποτέλεσμα να τεθούν σε κίνδυνο τα δεδομένα προσωπικού χαρακτήρα. Ωστόσο, όπως προαναφέρθηκε, ο ΓΚΠΔ απαιτεί από τον υπεύθυνο επεξεργασίας να εφαρμόζει όλα τα κατάλληλα μέτρα τεχνικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης και την άμεση ενημέρωση της εποπτικής αρχής και των υποκειμένων των δεδομένων. Αναφέρει επίσης ότι θα πρέπει να διαπιστώνεται ότι η γνωστοποίηση πραγματοποιήθηκε χωρίς αδικαιολόγητη καθυστέρηση, λαμβανομένων υπόψη ιδίως της φύσης και της σοβαρότητας της παραβίασης δεδομένων, καθώς και των συνεπειών και των δυσμενών αποτελεσμάτων της για το υποκείμενο των δεδομένων. Κατ' αυτόν τον τρόπο, ο υπεύθυνος επεξεργασίας υπόκειται στην υποχρέωση να εξασφαλίζει ότι θα αποκτά «γνώση» οποιωνδήποτε παραβιάσεων εγκαίρως ώστε να μπορεί να προβεί στις κατάλληλες ενέργειες. Το ακριβές χρονικό σημείο όπου ένας υπεύθυνος επεξεργασίας μπορεί να θεωρείται ότι αποκτά «γνώση» μιας συγκεκριμένης παραβίασης θα εξαρτάται από τις περιστάσεις της συγκεκριμένης παραβίασης. Σε ορισμένες περιπτώσεις, θα προκύπτει με σχετική σαφήνεια από την αρχή ότι έχει διαπραχθεί παραβίαση, ενώ, σε άλλες, ενδέχεται να χρειάζεται κάποιος χρόνος για να διαπιστωθεί εάν τα δεδομένα προσωπικού χαρακτήρα έχουν τεθεί σε κίνδυνο. Ωστόσο, η έμφαση θα πρέπει να δίνεται στην έγκαιρη ανάληψη δράσης για τη*

διερεύνηση ενός περιστατικού, ώστε να διαπιστωθεί κατά πόσο τα δεδομένα προσωπικού χαρακτήρα έχουν παραβιαστεί και, σε τέτοια περίπτωση, να λαμβάνονται διορθωτικά μέτρα και να γίνεται γνωστοποίηση, εάν απαιτείται». Σύμφωνα με τα παραπάνω, από το άρθρο 33 ΓΚΠΔ δεν απορρέει μόνο η υποχρέωση υποβολής γνωστοποίησης των περιστατικών παραβίασης στην εποπτική Αρχή αλλά επιπλέον η υποχρέωση προς ενεργή διερεύνηση κάθε πιθανού περιστατικού, εφόσον ο υπεύθυνος επεξεργασίας λάβει γνώση των σχετικών ενδείξεων. Σε αντίθετη περίπτωση, ο υπεύθυνος επεξεργασίας θα μπορούσε εύκολα να παρακάμπτει κάθε φορά την υποχρέωσή του για γνωστοποίηση των περιστατικών παραβίασης προς την εποπτική Αρχή, απλώς αδιαφορώντας για τις ενδείξεις ενός πιθανού περιστατικού και αποφεύγοντας να αποκτήσει βεβαιότητα και να «λάβει γνώση» αυτού σύμφωνα με την παραπάνω διάταξη. Εξάλλου, από την παρ. 3 του άρθρου 33 ΓΚΠΔ (περιεχόμενο της γνωστοποίησης) προκύπτει η υποχρέωση του υπευθύνου επεξεργασίας να διερευνήσει άμεσα τις εκεί αναφερόμενες πληροφορίες, ώστε να είναι σε θέση να τις συμπεριλάβει στη γνωστοποίηση προς την Αρχή (φύση της παραβίασης, κατηγορίες και αριθμός επηρεαζόμενων υποκειμένων, αριθμός επηρεαζόμενων αρχείων, ενδεχόμενες συνέπειες της παραβίασης, ληφθέντα ή προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση της παραβίασης, μέτρα για την άμβλυνση των ενδεχόμενων δυσμενών συνεπειών της), καθώς και να αξιολογήσει τον κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου,[2] ώστε να αποφασίσει εάν απαιτείται γνωστοποίηση και προς αυτό κατ' άρθρο 34 ΓΚΠΔ, ενώ από την παρ. 5 του άρθρου 33 ΓΚΠΔ προκύπτει ρητά η υποχρέωση τήρησης τεκμηρίωσης για όλες τις παραπάνω διαδικασίες. Άλλωστε και βάσει της αρχής της λογοδοσίας (άρθρο 5 παρ. 2 ΓΚΠΔ), το υποκείμενο των δεδομένων που έχει ειδοποιήσει τον υπεύθυνο επεξεργασίας για μια πιθανή παραβίαση δεδομένων, δεν οφείλει να αναλάβει επιπλέον ενεργό δράση ώστε ο τελευταίος να αποκτήσει

[2] Βλ. και τις Κατευθυντήριες 09/2022 του ΕΣΠΔ για τη γνωστοποίηση περιστατικών παραβίασης (§101 – 102): "*101. This means that* ***immediately upon becoming aware of a breach, it is vitally important*** *that the controller should* ***not only seek to contain the incident but it should also assess the risk*** *that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned. 102. As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals,[…]".*

βεβαιότητα περί της ύπαρξης ή μη περιστατικού παραβίασης. Η υποχρέωση αυτή βαρύνει τον υπεύθυνο επεξεργασίας, ο οποίος φέρει την ευθύνη να αποδεικνύει τη συμμόρφωσή του.

7. Επιπλέον η παραβίαση πρέπει να ανακοινώνεται και στο υποκείμενο των δεδομένων, κατά περίπτωση και σύμφωνα με τα οριζόμενα στο άρθρο 34 παρ. 1 και 2 ΓΚΠΔ: «*1. Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων. 2. Στην ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 1 του παρόντος άρθρου περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 33 παράγραφος 3 στοιχεία β), γ) και δ)*».

8. Στην **προκειμένη περίπτωση**, δεδομένων των ανωτέρω εκτιθέμενων πραγματικών περιστατικών που προέκυψαν από τα στοιχεία του φακέλου και μετά την ακροαματική διαδικασία, διαπιστώνεται κατ' αρχάς ότι η εκ μέρους της καταγγελλόμενης Τράπεζας χορήγηση προσωπικών δεδομένων σχετικά με τη χρήση της πιστωτικής κάρτας του καταγγέλλοντος στη σύζυγό του έγινε αθέμιτα, κατά παράβαση της αρχής της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας (άρθρο 5 παρ. 1 α' ΓΚΠΔ) και κατά παράβαση της αρχής της εμπιστευτικότητας των δεδομένων (άρθρο 5 παρ. 1 στ' ΓΚΠΔ). Η εν λόγω μη εξουσιοδοτημένη επεξεργασία (κοινολόγηση με διαβίβαση) αποτελεί περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τον ορισμό του άρθρου 4 αρ. 12 ΓΚΠΔ, το οποίο αποδίδεται σε σφάλμα υπαλλήλου της Τράπεζας. Συγκεκριμένα, όπως προέκυψε από τη σχετική έρευνα της Τράπεζας και τη διενέργεια πειθαρχικού ελέγχου, στις …, κατά την επίσκεψη της συζύγου του καταγγέλλοντος στο κατάστημα Alpha Bank Ω Χ, με σκοπό να ενημερωθεί για την απόδοση κοινών επενδυτικών προϊόντων που διατηρούσε με τον καταγγέλλοντα, η σύζυγός του ζήτησε να ενημερωθεί για το υπόλοιπο και τις συναλλαγές που είχαν διενεργηθεί με πιστωτική κάρτα που διατηρούσε ο καταγγέλλων αποκλειστικά στο δικό του όνομα, διαβεβαιώνοντας την υπάλληλο ότι διαθέτει σχετική προφορική εντολή και

εξουσιοδότηση από τον καταγγέλλοντα, ως υποκείμενο των δεδομένων. Η υπάλληλος, παραπλανηθείσα ως προς την ύπαρξη εξουσιοδότησης, εκτύπωσε και χορήγησε στη σύζυγο του καταγγέλλοντος τις τρέχουσες κινήσεις της προσωπικής του πιστωτικής κάρτας, κατά παράβαση των σχετικών εσωτερικών διαδικασιών και μέτρων ασφαλείας της Τράπεζας, που απαιτούν έγγραφη εξουσιοδότηση (βλ. υπόμνημα της καταγγελλόμενης: «*Είναι προφανές ότι η συγκεκριμένη υπάλληλος κακώς δέχθηκε ως επαρκή την προφορική εξουσιοδότηση της συζύγου, παρά τις εσωτερικές οδηγίες και διαδικασίες της Τράπεζας*»). Ακολούθως, παρότι η καταγγελλόμενη Τράπεζα ενημερώθηκε για το περιστατικό αυτό στις … από τον καταγγέλλοντα, ο οποίος μάλιστα κατονόμασε ως πιθανή πηγή της διαρροής κάποιο από τα καταστήματα της Τράπεζας στην περιοχή της Χ («*υποπτεύομαι της Χ*»), και παρότι είναι δεδομένη η δυνατότητα ελέγχου των προσβάσεων που είχαν πραγματοποιηθεί το επίμαχο χρονικό διάστημα στις πληροφορίες λογαριασμού του καταγγέλλοντος από υπαλλήλους της μέσω των συστημάτων της, η Τράπεζα δεν ανέλαβε άμεσα ενεργό δράση προς διερεύνηση του περιστατικού ώστε να αποκτήσει τον απαιτούμενο βαθμό βεβαιότητας και να τηρήσει τις εκ του άρθρου 33 ΓΚΠΔ υποχρεώσεις της, θεωρώντας ότι τα στοιχεία που είχε στη διάθεσή της δεν ήταν επαρκή. Επιπλέον, παρότι ο καταγγέλλων στις … απέστειλε στην Τράπεζα σχετική φωτογραφία του αντιγράφου κινήσεων λογαριασμού που του είχε επιδείξει η σύζυγός του, η Υπηρεσία της Τράπεζας «εκ παραδρομής», όπως υποστηρίζει, δεν προώθησε το στοιχείο αυτό στη Διεύθυνση Εσωτερικού Ελέγχου, με αποτέλεσμα να μην είναι ακόμα δυνατό, κατά την άποψή της, να εκκινήσει η έρευνα. Μάλιστα το στοιχείο αυτό φαίνεται ότι δεν προωθήθηκε στη Διεύθυνση Εσωτερικού Ελέγχου ούτε στις …, όταν η τελευταία, με μήνυμά της προς την Υπηρεσία της Τράπεζας ζήτησε διευκρινίσεις και περαιτέρω στοιχεία για την υπόθεση (βλ. σχετικό Γ/ΕΙΣ/125/09-01-2023 έγγραφο απόψεων της καταγγελλόμενης). Εν τέλει η φωτογραφία της εκτύπωσης κινήσεων του λογαριασμού της πιστωτικής κάρτας του καταγγέλλοντος εστάλη στη Διεύθυνση Εσωτερικού Ελέγχου με μεγάλη καθυστέρηση στις …, ήτοι 1,5 μήνα αφότου η Τράπεζα παρέλαβε τη σχετική αναφορά του καταγγέλλοντα στον Συνήγορο του Καταναλωτή (…), με αφορμή την οποία τελικά εστάλησαν όλα τα στοιχεία στη Διεύθυνση Εσωτερικού Ελέγχου, ο οποίος εξέδωσε τελικά το από …

πόρισμα με το οποίο επιβεβαιώθηκε η διαρροή[3] και καταγράφηκε ως περιστατικό παραβίασης. Ακολούθως, η Επιτροπή Αξιολόγησης Περιστατικών Παραβίασης συνεδρίασε στις … (βλ. τη Γ/ΕΙΣ/125/09-01-2023 απάντηση της Τράπεζας), ήτοι 20 ημέρες μετά το ανωτέρω πόρισμα. Κατά τη συνεδρίαση, σύμφωνα με την ίδια απάντηση, εκτιμήθηκε ότι «*με βάση το πλήθος και το είδος των δεδομένων, που αφορούν .. συναλλαγές μέσω πιστωτικής κάρτας που διενεργήθηκαν σε χρονικό διάστημα περίπου … μηνών (… έως …) και το γεγονός ότι οι μη εξουσιοδοτημένοι αποδέκτες των ανωτέρω δεδομένων περιορίζονται σε ένα φυσικό πρόσωπο και μάλιστα συγγενικό με τον καταγγέλλοντα (σύζυγος) δεν φαίνεται να προκύπτει κίνδυνος για τις ελευθερίες και τα δικαιώματα του υποκειμένου*». Κατά συνέπεια, η Τράπεζα δεν προχώρησε σε γνωστοποίηση του περιστατικού στην Αρχή σύμφωνα με το άρθρο 33 ΓΚΠΔ, χαρακτηρίζοντας εσφαλμένα τον κίνδυνο από αυτό ως «μηδενικό» (βλ. Απόσπασμα Μητρώου Περιστατικών Παραβίασης, ως σχετ. 1 του υπομνήματος της Τράπεζας), παρά το γεγονός ότι στη Φόρμα Αναλύσεως και Αξιολογήσεως Κινδύνου του περιστατικού (σχετ. 2 του υπομνήματος της Τράπεζας) έχουν καταγραφεί ως ενδεχόμενες επιπτώσεις για το υποκείμενο η «*πρόκληση άγχους, στρες, ενόχληση και έλλειψη εμπιστοσύνης για την διαρροή των κινήσεων της πιστωτικής κάρτας του, στη σύζυγό του*». Όπως προκύπτει από την ίδια Φόρμα, η σοβαρότητα των επιπτώσεων για το υποκείμενο έχει εκτιμηθεί ως «αμελητέα», όπως επίσης «αμελητέα» χαρακτηρίζεται και η πιθανότητα να προκληθεί βλάβη στο υποκείμενο, με την εξής αιτιολογία: «*Το πλήθος και οι κατηγορίες των δεδομένων (κινήσεις μιας κάρτας για μέγιστη χρονική περίοδο … μηνών) και ο αποδέκτης τους, τα δεδομένα διέρρευσαν σε πρόσωπο του πλέον στενού οικογενειακού κύκλου του φυσικού προσώπου Β, εκτιμάται ότι μειώνουν σημαντικά την πιθανότητα επέλευσης υψηλών κινδύνων για τις ελευθερίες και τα δικαιώματα του φυσικού προσώπου Β. Κατόπιν των ανωτέρω η πιθανότητα να προκληθεί κίνδυνος για τα δικαιώματα και τις ελευθερίες του υποκειμένου ή βλάβη κρίνεται αμελητέα*». Ωστόσο η εκτίμηση αυτή της Τράπεζας είναι προδήλως εσφαλμένη, δεδομένου ότι είναι βέβαιο ότι το περιστατικό επέφερε συνέπειες στα δικαιώματα και τις ελευθερίες του

[3] *Σημειώνεται ότι στη Φόρμα Αναλύσεως Κινδύνου του περιστατικού παραβίασης, ως ημερομηνία επιβεβαίωσης του περιστατικού αναφέρεται η …, ενώ ως ημερομηνία εντοπισμού του η …, χωρίς αυτή η απόκλιση να εξηγείται από την Τράπεζα*.

καταγγέλλοντος, αφού όπως ήταν ήδη γνωστό στην Τράπεζα, διατάραξε την προσωπική και οικογενειακή του ζωή[4]. Προκύπτει εξάλλου ότι η Τράπεζα υποτιμά τις πιθανές συνέπειες της παραβίασης, υποστηρίζοντας με το υπόμνημά της ότι από την καταγραφή καθημερινών συναλλαγών, όπως είναι οι καταβολές προς το … ή το … δεν προκύπτει το είδος της παρεχόμενης υπηρεσίας, ισχυρισμός προδήλως αβάσιμος.

Περαιτέρω, στην ίδια Φόρμα Αναλύσεως και Αξιολογήσεως Κινδύνου (Σχετ. 2 του υπομνήματος) σημειώνεται ότι «*Λόγω της φύσης του περιστατικού και με δεδομένο ότι, πλέον, δεν δύνανται να αποτραπούν οι επιπτώσεις του περιστατικού, δεν υφίσταται η δυνατότητα για διορθωτικές ενέργειες εκ μέρους της Τράπεζας*», εκτίμηση επίσης εσφαλμένη, αφού η Τράπεζα θα μπορούσε σε κάθε περίπτωση να λάβει μέτρα για τον περιορισμό των επιπτώσεων του περιστατικού: Για παράδειγμα, θα μπορούσε να επικοινωνήσει με τη σύζυγο και αποδέκτη των δεδομένων του καταγγέλλοντος, να την ενημερώσει για το γεγονός ότι η διαβίβαση των συναλλακτικών πληροφοριών του προς την ίδια είχε γίνει παράνομα, κατά παράβαση των διαδικασιών της τράπεζας και του τραπεζικού απορρήτου και να την καλέσει να επιστρέψει τις σχετικές εκτυπώσεις στην Τράπεζα και να καταστρέψει τυχόν αντίγραφά τους, καθώς και να μη γνωστοποιήσει περαιτέρω τις σχετικές πληροφορίες σε τρίτους. Έτσι, παρότι η Τράπεζα αναγνωρίζει ότι εν προκειμένω έγινε παράνομη επεξεργασία και αθέμιτη διαβίβαση των δεδομένων του καταγγέλλοντος και καταχώρησε το περιστατικό στο Μητρώο Περιστατικών Παραβίασης Δεδομένων, εν τέλει δεν το γνωστοποίησε στην Αρχή κατ' άρθρο 33 ΓΚΠΔ, δεν έλαβε μέτρα για τον μετριασμό των συνεπειών του και δεν έλαβε επιπλέον μέτρα για την αποτροπή παρόμοιων περιστατικών στο μέλλον, πέρα από την επιβολή στην υπαίτια υπάλληλο της πειθαρχικής ποινής της παύσης ενός μήνα, η οποία, κατά την Τράπεζα, προορίζεται να δράσει αποτρεπτικά και για το λοιπό προσωπικό. Σημειώνεται επίσης

[4] Σύμφωνα με τις ως άνω ΓΚ 09/2022 του ΕΣΠΔ, η αξιολόγηση του κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων στο πλαίσιο περιστατικού παραβίασης διαφέρει από τη γενική αξιολόγηση του (υποθετικού) κινδύνου κατά τη διενέργεια ΕΑΠΔ και θα πρέπει να εστιάζει στην πραγματική επίδραση του περιστατικού στα υποκείμενα: "*104. It should be noted that assessing the risk to people's rights and freedoms as a result of a breach* ***has a different focus*** *to the risk considered in a DPIA). The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event.* ***With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals***."

ότι η Τράπεζα δεν εκδήλωσε οποιοδήποτε ενδιαφέρον ή μια έστω τυπική απολογία για την ηθική βλάβη που υπέστη ο καταγγέλλων εξαιτίας του περιστατικού.

9. Από τα παραπάνω εκτιθέμενα πραγματικά περιστατικά προκύπτουν μια σειρά από εσφαλμένες ενέργειες και παραλείψεις στη διαχείριση του υπό κρίση περιστατικού παραβίασης εκ μέρους της καταγγελλόμενης Τράπεζας. Συγκεκριμένα, η Τράπεζα, ως υπεύθυνος επεξεργασίας, παρότι είχε ενδείξεις για την πιθανή τέλεση περιστατικού παραβίασης, αρχικά δεν το διερεύνησε μεταθέτοντας την ευθύνη για τον εντοπισμό της πηγής της διαρροής στο υποκείμενο των δεδομένων, στη συνέχεια καθυστέρησε σημαντικά να το χειριστεί ως περιστατικό παραβίασης λόγω έλλειψης συνεννόησης μεταξύ των αρμοδίων Μονάδων της, ακολούθως υποτίμησε τις συνέπειές του για το υποκείμενο και εκτίμησε εσφαλμένα ότι δεν οφείλει να το γνωστοποιήσει στην Αρχή κατά το άρθρο 33 ΓΚΠΔ. Οι διαπιστωθείσες ελλείψεις και καθυστερήσεις κατά τον εσωτερικό χειρισμό της υπόθεσης δεν προκύπτει ότι οφείλονται σε ελλιπείς Πολιτικές και Διαδικασίες της Τράπεζας σύμφωνα με το άρθρο 24 παρ. 2 ΓΚΠΔ, αφού οι ενέργειες τις οποίες οφείλουν να ακολουθούν αμελλητί τα όργανα και οι υπηρεσίες της σε περίπτωση πιθανού περιστατικού παραβίασης προβλέπονται στα κείμενα που η Τράπεζα επικαλέστηκε και προσκόμισε (βλ. σχετ. 4-6 του υπ' αρ. πρωτ. Γ/ΕΙΣ/125/09-01-2023 απαντητικού εγγράφου της Τράπεζας) αλλά στη μη τήρηση των εν λόγω διαδικασιών στην προκειμένη περίπτωση. Κατόπιν των ανωτέρω, προκύπτει ευθύνη της Τράπεζας για το γεγονός ότι καθυστέρησε για πολλούς μήνες να διερευνήσει το συμβάν ώστε να αποκτήσει εύλογο βαθμό βεβαιότητας και να το χειριστεί ως περιστατικό παραβίασης, αλλά και για το γεγονός ότι μετά την επιβεβαίωση του περιστατικού δεν προχώρησε σε γνωστοποίησή του στην Αρχή ούτε έλαβε μέτρα για τον μετριασμό των συνεπειών του.

10. Ως εκ τούτου, η Αρχή διαπιστώνει τις εξής παραβάσεις εκ μέρους της καταγγελλόμενης Τράπεζας, ως υπευθύνου επεξεργασίας:

α) παράνομη επεξεργασία των προσωπικών δεδομένων του καταγγέλλοντος, λόγω της διαβίβασης των κινήσεων της πιστωτικής του κάρτας σε τρίτο πρόσωπο, η οποία έγινε χωρίς νομική βάση, κατά παράβαση των αρχών της νομιμότητας της επεξεργασίας και της εμπιστευτικότητας των δεδομένων (άρθρο 5 παρ. 1 α) και στ) ΓΚΠΔ) και αποτελεί περιστατικό παραβίασης (άρθρο 4 αρ. 12 ΓΚΠΔ)

β) εσφαλμένος χειρισμός του περιστατικού και μη υποβολή γνωστοποίησης στην Αρχή κατά παράβαση του άρθρου 33 ΓΚΠΔ.

11. Με βάση τα ανωτέρω, η Αρχή κρίνει ότι συντρέχει περίπτωση να ασκήσει τις κατά το άρθρο 58 παρ. 2 του ΓΚΠΔ διορθωτικές εξουσίες της σε σχέση με τις διαπιστωθείσες παραβάσεις και ότι πρέπει, με βάση τις περιστάσεις που διαπιστώθηκαν, να επιβληθεί, κατ' εφαρμογή της διάταξης του άρθρου 58 παρ. 2 εδ. θ' του ΓΚΠΔ, αποτελεσματικό, αναλογικό και αποτρεπτικό διοικητικό χρηματικό πρόστιμο κατ' άρθρο 83 του ΓΚΠΔ, τόσο προς αποκατάσταση της συμμόρφωσης, όσο και για την τιμωρία της παράνομης συμπεριφοράς. Περαιτέρω η Αρχή, έλαβε υπόψη τα κριτήρια επιμέτρησης του προστίμου που ορίζονται στο άρθρο 83 παρ. 2 του ΓΚΠΔ, την παράγραφο 5 εδ. α' του ίδιου άρθρου που έχει εφαρμογή στην παρούσα υπόθεση, τις Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του Κανονισμού 2016/679 που εκδόθηκαν στις 03-10-2017 από την Ομάδα Εργασίας του άρθρου 29 (WP 253) και τις Κατευθυντήριες γραμμές 04/2022 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων για τον υπολογισμό των διοικητικών προστίμων στο πλαίσιο του Γενικού Κανονισμού, καθώς και τα πραγματικά δεδομένα της εξεταζόμενης υπόθεσης και ιδίως τα κριτήρια που παρατίθενται στη συνέχεια, ανά παράβαση.

Α. Αναφορικά με την πρώτη ως άνω διαπιστωθείσα παράβαση (βλ. σκέψη 10 α), λαμβάνονται ιδιαιτέρως υπόψη οι εξής ειδικές περιστάσεις:

α) ότι η παράβαση της νομιμότητας της επεξεργασίας εμπίπτει στη διάταξη της παρ. 5 του άρθρου 83 ΓΚΠΔ,

β) ότι το περιστατικό φαίνεται να είναι μεμονωμένο, καθώς δεν έχει επιβληθεί από την Αρχή κύρωση στην Τράπεζα για παρόμοια παράβαση στο παρελθόν,

γ) ότι η παράβαση επηρέασε άμεσα ένα υποκείμενο δεδομένων, …,

δ) ότι η παράβαση οφείλεται σε ανθρώπινο σφάλμα υπαλλήλου που αποδίδεται σε αμέλεια, ενώ η Τράπεζα έχει θεσπίσει κατάλληλες διαδικασίες που προβλέπουν την έγγραφη εξουσιοδότηση ως προϋπόθεση για τη χορήγηση πληροφοριών σε τρίτο,

ε) ότι η Τράπεζα δεν έλαβε μέτρα για τον μετριασμό των άμεσων επιπτώσεων του περιστατικού για το υποκείμενο των δεδομένων, όπως π.χ. να επικοινωνήσει με την αποδέκτη των δεδομένων και να της ζητήσει να επιστρέψει στην Τράπεζα ή να καταστρέψει τα δεδομένα που της χορηγήθηκαν παράνομα,

στ) ότι, ωστόσο, η Τράπεζα προχώρησε τελικά σε πειθαρχικό έλεγχο της υπαλλήλου που παραβίασε τις εν λόγω διαδικασίες, και της επέβαλε πειθαρχική ποινή.

Β. Αναφορικά με τη δεύτερη ως άνω διαπιστωθείσα παράβαση (βλ. σκέψη 10 β), λαμβάνονται ιδιαιτέρως υπόψη τα εξής κριτήρια:

α) ότι η παράβαση των υποχρεώσεων του υπευθύνου επεξεργασίας εκ του άρθρου 33 ΓΚΠΔ εμπίπτει στη διάταξη της παρ. 4 του άρθρου 83 ΓΚΠΔ,

β) ο βαθμός ευθύνης της καταγγελλόμενης, η οποία παρότι έχει λάβει κατάλληλα οργανωτικά μέτρα και έχει θεσπίσει σχετικές πολιτικές για τη διαχείριση περιστατικών παραβίασης δεδομένων, προέκυψε ότι δεν τα εφάρμοσε στην πράξη στην προκειμένη περίπτωση,

γ) ότι διαπιστώθηκε πολύμηνη καθυστέρηση σε μια διαδικασία που πρέπει να διενεργείται εντός 72 ωρών, γεγονός που υποδηλώνει πιθανή προσπάθεια συγκάλυψης εκ μέρους της Τράπεζας, σε κάθε δε περίπτωση αδιαφορία ως προς την τήρηση των εκ του ΓΚΠΔ υποχρεώσεών της,

δ) ότι στο πλαίσιο ελέγχου της καταγγελίας από την Αρχή, η Τράπεζα μετέθεσε το βάρος ευθύνης για τη διερεύνηση του περιστατικού στο υποκείμενο, κατά τρόπο που αντιβαίνει στην αρχή της λογοδοσίας,

ε) ότι η Τράπεζα περαιτέρω αδιαφόρησε για τις συνέπειες του περιστατικού στο υποκείμενο των δεδομένων, των οποίων τελούσε σε γνώση και υποτίμησε τον κίνδυνο για το υποκείμενο μέχρι του σημείου να τον χαρακτηρίζει «μηδενικό»,

στ) ότι βάσει των ανωτέρω προκύπτει ότι ο συνολικά εσφαλμένος και αθέμιτος χειρισμός του περιστατικού εκ μέρους της Τράπεζας αποτελεί συστημικό πρόβλημα που δυνητικά μπορεί να επηρεάσει και άλλους πελάτες της.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η ΑΡΧΗ

Α. Επιβάλλει, στην ΑΛΦΑ ΤΡΑΠΕΖΑ Α.Ε. ως υπεύθυνο επεξεργασίας, με βάση το άρθρο 58 παρ. 2 εδ. θ) του ΓΚΠΔ, διοικητικό πρόστιμο ύψους δέκα χιλιάδων (10.000€) ευρώ, για τη διαπιστωθείσα παράβαση των αρχών της νομιμότητας της επεξεργασίας και της εμπιστευτικότητας των δεδομένων κατ' άρθρο 5 παρ. 1 α) και στ) ΓΚΠΔ.

Β. Επιβάλλει, στην ΑΛΦΑ ΤΡΑΠΕΖΑ Α.Ε., ως υπεύθυνο επεξεργασίας, με βάση το άρθρο 58 παρ. 2 εδ. θ) του ΓΚΠΔ, διοικητικό πρόστιμο ύψους πενήντα χιλιάδων (50.000€) ευρώ, για τη διαπιστωθείσα παράβαση της υποχρέωσης χειρισμού και γνωστοποίησης περιστατικού παραβίασης βάσει του άρθρου 33 ΓΚΠΔ.

Ο Πρόεδρος	**Η Γραμματέας**
Γεώργιος Μπατζαλέξης	**Ειρήνη Παπαγεωργοπούλου**