ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 02-02-2023
Αριθ. Πρωτ.: 267

ΑΠΟΦΑΣΗ 4/2023
(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε, μετά από πρόσκληση του Προέδρου της, σε τακτική συνεδρίαση σε σύνθεση Τμήματος στην έδρα της την 18/01/2023, 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 Γεώργιος Κόντης, 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/5802/15-09-2021 καταγγελία του, ο Α (στο εξής καταγγέλλων), στρέφεται κατά της Τράπεζας Πειραιώς (στο εξής καταγγελλόμενη), της οποίας τυγχάνει πελάτης και δικαιούχος τραπεζικού λογαριασμού παραπονούμενος για παράνομη και χωρίς προηγούμενη ενημέρωσή του χορήγηση προσωπικών δεδομένων του στην αντίδικό του, Β. Ειδικότερα, σύμφωνα με την καταγγελία, στο πλαίσιο αγωγής που εκκρεμεί εναντίον του καταγγέλλοντος από την ως άνω αντίδικο ενώπιον του Μονομελούς Πρωτοδικείου Χ, η αντίδικός του επικαλέστηκε και προσκόμισε με τις από … προτάσεις της, τις αναλυτικές κινήσεις δύο τραπεζικών λογαριασμών (με αριθμούς … και …) της καταγγελλόμενης Τράπεζας,

στους οποίους ο καταγγέλλων ήταν αρχικά συνδικαιούχος με πρώτη δικαιούχο τη θεία του, Γ το γένος Β, και από τον θάνατό της στις … και εφεξής, μοναδικός δικαιούχος. Σύμφωνα με την καταγγελία, οι προσκομισθείσες αναλυτικές κινήσεις των ως άνω λογαριασμών αφορούσαν και το χρονικό διάστημα μετά το θάνατο της θείας του, μέχρι και τον … . Περαιτέρω, ο καταγγέλλων αναφέρει ότι αμέσως μόλις έλαβε γνώση των παραπάνω μετέβη στο Υποκατάστημα Ψ, όπου ο διευθυντής Δ επικαλέστηκε το τραπεζικό απόρρητο και ισχυρίστηκε ότι η Τράπεζα ουδέποτε θα χορηγούσε τα εν λόγω στοιχεία. Στη συνέχεια, με το Γ/ΕΙΣ/7545/18-11-2021 έγγραφό του ο καταγγέλλων κοινοποίησε στην Αρχή το αίτημα που υπέβαλε στην Τράπεζα (με αριθμό πρωτοκόλλου …) διά του πληρεξουσίου δικηγόρου του, Στέφανου Τοπάλη, και με τα Γ/ΕΙΣ/1103/27-01-2022 και Γ/ΕΙΣ/6617/03-05-2022 έγγραφά του κοινοποίησε στην Αρχή τις απαντήσεις που είχε λάβει αρχικά μέσω sms για την εξέλιξη του αιτήματός του και την τελική από … έγγραφη απάντηση της Τράπεζας, σύμφωνα με την οποία η Τράπεζα έχει λάβει όλα τα απαραίτητα μέτρα προκειμένου να διαφυλάσσεται το τραπεζικό απόρρητο των πελατών της σύμφωνα με το ισχύον θεσμικό πλαίσιο, καθώς και ότι επιλαμβάνεται αρμοδίως σε περιπτώσεις όπως η υπό κρίση υπόθεση που της γνωστοποιήθηκε, κατ’ εφαρμογή των εσωτερικών της διαδικασιών.

Στο πλαίσιο διερεύνησης της καταγγελίας, η Αρχή με το ως Γ/ΕΞΕ/1219/20-05-2022 έγγραφο κάλεσε την καταγγελλόμενη να εκθέσει τις απόψεις της επί των καταγγελλομένων. Από την καταγγελλόμενη ζητήθηκε να διευκρινίσει, ιδίως, α) εάν χορήγησε τις εν λόγω καταστάσεις αναλυτικής κίνησης των λογαριασμών του καταγγέλλοντος στην αντίδικό του, Β, με ποια νομική βάση και διαδικασία, β) στην περίπτωση που η ανωτέρω επεξεργασία βασίσθηκε στο άρθρο 6 παρ. 1 στοιχείο στ΄ ΓΚΠΔ, ποια ήταν εν προκειμένω τα έννομα συμφέροντα που επιδιώκονται, προσδιορίζοντας τη διαδικασία της στάθμισης που ακολουθήθηκε, ώστε να κριθεί εάν υπερτερούν έναντι των συμφερόντων, των θεμελιωδών δικαιωμάτων και των ελευθεριών του καταγγέλλοντος, ως υποκειμένου, και γ) εάν ενημερώθηκε ο καταγγέλλων ως υποκείμενο για την ανωτέρω επεξεργασία κατά τα άρθρα 13 και 14 ΓΚΠΔ, και, σε περίπτωση αρνητικής απάντησης, με ποια αιτιολογία.

Με την υπ' αρ. πρωτ. Γ/ΕΙΣ/7717/06-06-2022 απάντησή της, η καταγγελλόμενη Τράπεζα κατ' αρχάς αναφέρει ότι ο καταγγέλλων τηρούσε κοινούς τραπεζικούς λογαριασμούς με την αποθανούσα Γ και ότι η Β, επίσης πελάτης της Τράπεζας, επικαλούμενη την ιδιότητα της μίας εκ των νομίμων κληρονόμων της ως άνω αποβιωσάσης θείας της Γ, ιδιότητα που προέκυπτε και από τη σχετική νομιμοποίησή της ως κληρονόμου που τηρούνταν στην Τράπεζα - υπέβαλε αίτημα χορήγησης στην ίδια στοιχείων και κινήσεων των τραπεζικών λογαριασμών, στους οποίους η θεία της ήταν δικαιούχος εν ζωή. Εν συνεχεία, «εκ προφανούς παραδρομής και λόγω εσφαλμένης εκτίμησης των πραγματικών περιστατικών και των επιμέρους δεδομένων και παραμέτρων εκ μέρους του υπαλλήλου στον οποίο απευθύνθηκε η Β» όπως αναφέρει η καταγγελλόμενη, δόθηκαν από τον εν λόγω υπάλληλο, μετά την παραλαβή του σχετικού αιτήματος, τα αιτηθέντα στοιχεία και κινήσεις τραπεζικών λογαριασμών. Ο υπάλληλος, δηλαδή, βασιζόμενος στα έγγραφα περί νομιμοποίησης της αιτούσας, ως νόμιμης κληρονόμου της συνδικαιούχου του καταγγέλλοντος, θεώρησε «*εκ προφανούς παραδρομής και από δική του εσφαλμένη εκτίμηση*», ότι η αιτούσα είχε κληρονομικά δικαιώματα και κληρονομικές αξιώσεις και ως προς αυτούς τους τραπεζικούς λογαριασμούς και εσφαλμένα θεώρησε ότι είχε και το δικαίωμα να λάβει γνώση και των αιτηθέντων στοιχείων που αφορούσαν τους συγκεκριμένους λογαριασμούς, οπότε ικανοποίησε το αίτημά της «*λόγω ανθρώπινου λάθους και απροσεξίας, αλλά χωρίς πρόθεση και δόλο*». Σύμφωνα με την απάντηση της καταγγελλόμενης, η Τράπεζα επιλήφθηκε άμεσα του θέματος, υπήρξε άμεση κινητοποίηση των αρμοδίων Μονάδων της για την ενδελεχή διερεύνηση της υπόθεσης και τη διεξαγωγή όλων των σχετικών εσωτερικών της διαδικασιών. Αναφέρει δε ότι, όπως προέκυψε από την εξέταση του υπαλλήλου, ο ίδιος δεν γνώριζε την αιτούσα, εκ παραδρομής δεν είδε ποιοι ήταν οι συνδικαιούχοι των συγκεκριμένων λογαριασμών, παραπλανήθηκε και της έδωσε τις κινήσεις των λογαριασμών, ενώ βασιζόμενος στην ιδιότητά της ως νομίμου κληρονόμου, έκρινε ότι δεν χρειαζόταν να ζητήσει ούτε τη γνωμοδότηση της Νομικής Υπηρεσίας της Τράπεζας. Με την ίδια απάντησή της, η Τράπεζα υποστηρίζει: α) ότι προέβη σε όλες τις ενδεδειγμένες ενέργειες για τη διερεύνηση και αντιμετώπιση της υπό κρίση υπόθεσης, β) ότι γενικά μέσω των διαδικασιών, πολιτικών, εσωτερικών κανονισμών που έχει εκπονήσει, εκπαιδευτικών σεμιναρίων που διεξάγει, της άσκησης διαρκούς

εποπτείας, εκπαίδευσης και καθοδήγησης του προσωπικού, μεριμνά για τη διαφύλαξη, προστασία και σύννομη επεξεργασία των προσωπικών δεδομένων καθώς και την περιφρούρηση του τραπεζικού απορρήτου, γ) ότι είχε ενημερώσει και εκπαιδεύσει και τον συγκεκριμένο υπάλληλο – όπως όλους τους υπαλλήλους, ώστε να εκπληρώνει τα καθήκοντά του σε συμμόρφωση με τις νομικές και κανονιστικές απαιτήσεις της Τράπεζας, συμπεριλαμβανομένης της ανάγκης να ζητηθεί γνωμοδότηση της Νομικής της Υπηρεσίας, ωστόσο, από ανθρώπινο λάθος, εκ προφανούς παραδρομής και λόγω βεβιασμένης και απερίσκεπτης ενέργειας, βασιζόμενος στην ιδιότητα της αιτούσας ως νομίμου κληρονόμου, δεν τήρησε την ως άνω διαδικασία και έσπευσε να χορηγήσει τα αιτηθέντα στοιχεία, δ) ότι η Τράπεζα έχει εκκινήσει και τις σχετικές πειθαρχικές διαδικασίες, ε) ότι, συμπερασματικά, η υπό εξέταση περίπτωση δεν ανάγεται στο πεδίο ευθύνης της Τράπεζας, η οποιαδήποτε παράβαση δεν θα μπορούσε να καταλογιστεί στην Τράπεζα και τέλος, στ) ότι σύμφωνα με απόφαση της Βελγικής Αρχής Προστασίας Δεδομένων σε υπόθεση αναφορικά με την εκ λάθους αποστολή ηλεκτρονικής αλληλογραφίας σε υποκείμενα διαφορετικά από τους στοχευόμενους αποδέκτες (Beslissing ten gronde 07/2021 van 29 januari 2021) και παρά το γεγονός ότι και η εκ παραδρομής επεξεργασία δεδομένων συνιστά αντικειμενικό γεγονός και επεξεργασία, η συγκεκριμένη εκ λάθους επεξεργασία δεν συνιστά παραβίαση δεδομένων προσωπικού χαρακτήρα, αφού η χωρίς πρόθεση περιγραφόμενη στην ως άνω απόφαση επεξεργασία, δεν οφείλονταν σε μη επαρκή τεχνικά και οργανωτικά μέτρα εκ μέρους του υπευθύνου επεξεργασίας, δεδομένου ότι το άρθρο 33 ΓΚΠΔ θα πρέπει να εφαρμόζεται συνδυαστικά με το άρθρο 32 ΓΚΠΔ, και επομένως η παραβίαση δεδομένων προσωπικού χαρακτήρα του άρθρου 33 προϋποθέτει παραβίαση των διατάξεων του άρθρου 32 ΓΚΠΔ. Ως εκ τούτου, εφόσον το ανθρώπινο λάθος δεν δύναται σε καμία περίπτωση να αποκλειστεί, η Βελγική Αρχή κατέληξε στην άποψη ότι δεν συντελέστηκε παραβίαση των διατάξεων των άρθρων 32 και 33 ΓΚΠΔ.

Συμπερασματικά, παρότι η καταγγελλόμενη Τράπεζα αναγνωρίζει ότι εν προκειμένω έγινε παράνομη επεξεργασία και αθέμιτη διαβίβαση των δεδομένων του καταγγέλλοντος, επειδή αυτή οφείλεται σε ανθρώπινο σφάλμα, εσφαλμένη εκτίμηση και παραδρομή του υπαλλήλου και όχι σε μη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων του άρθρου 32 ΓΚΠΔ, θεωρεί ότι η ίδια έχει τηρήσει τις σχετικές

υποχρεώσεις της διερευνώντας το περιστατικό και κινώντας σχετική πειθαρχική διαδικασία, χωρίς να γνωστοποιήσει το περιστατικό στην Αρχή κατ' άρθρο 33 ΓΚΠΔ, εφαρμόζοντας την ανωτέρω ερμηνεία του άρθρου αυτού από την αντίστοιχη Βελγική Αρχή.

Δεδομένων των ανωτέρω, η Αρχή, με σχετικές κλήσεις κάλεσε τους εμπλεκόμενους στο συμβούλιο του Τμήματος της Αρχής στις 09-11-2022, προκειμένου να εκθέσουν τις απόψεις τους για την υπόθεση. Κατά τη συνεδρίαση παρέστησαν ο καταγγέλλων μαζί με τον πληρεξούσιο δικηγόρο του, Στέφανο Τοπάλη (…) και για λογαριασμό της καταγγελλόμενης Τράπεζας, η πληρεξούσια δικηγόρος Βασιλική – Μαρία Σαλδάρη (…), η Ε, ο ΣΤ, Περιφερειακός Διευθυντής, υπεύθυνος για το εμπλεκόμενο κατάστημα και ο Ζ, ΥΠΔ της Τράπεζας, ο οποίος δεν έλαβε το λόγο. Ακολούθως τα μέρη έλαβαν προθεσμία και προσκόμισαν εμπροθέσμως, ο μεν καταγγέλλων το Γ/ΕΙΣ/12002/23-11-2022 έγγραφο υπόμνημά του, η δε καταγγελλόμενη το Γ/ΕΙΣ/12098/28-11-2022 έγγραφο υπόμνημά της.

Κατά τη συνεδρίαση και με το υπόμνημά του, ο καταγγέλλων επανέλαβε τα αναφερόμενα στην καταγγελία του και επεσήμανε ότι η παραβίαση του δικαιώματος πρόσβασης με τη μορφή διαρροής – χορήγησης στοιχείων σε τρίτο, μη δικαιούμενο πρόσωπο, όπως και η παραβίαση του τραπεζικού του απορρήτου και η παράλειψη οποιασδήποτε επίσημης ενημέρωσής του, ως υποκειμένου των δεδομένων, έστω και μεταγενέστερα, συνομολογήθηκε από την καταγγελλόμενη Τράπεζα. Ο καταγγέλλων τόνισε ότι τα προσωπικά δεδομένα του που χορηγήθηκαν σε τρίτο αποτέλεσαν τη βάση και χρησιμοποιήθηκαν εναντίον του στο πλαίσιο αγωγής ενώπιον του Μονομελούς Πρωτοδικείου Χ και επεσήμανε ότι η Τράπεζα δεν έδωσε πληροφορίες σχετικά με το υποκατάστημα, τον εμπλεκόμενο υπάλληλο και τις ειδικότερες συνθήκες (τρόπος υποβολής της αίτησης, συνοδευτικά έγγραφα, πληροφορίες σχετικά με τη «νομιμοποίηση κληρονόμων» που επικαλείται η Τράπεζα) ούτε σχετικά με τις διαπιστώσεις της πειθαρχικής διαδικασίας που κατέληξε σε επίπληξη, ώστε να κριθεί εάν η διαρροή των δεδομένων του, που αφορούσε δύο λογαριασμούς σε διάστημα αρκετών ετών, οφείλεται πράγματι σε ανθρώπινο λάθος του εν λόγω υπαλλήλου. Καταλήγοντας υποστήριξε ότι η παραβίαση των δεδομένων του έγινε με

πρόθεση, πιθανώς στο πλαίσιο γνωριμίας με τον συγκεκριμένο υπάλληλο, χωρίς να λάβει χώρα οποιαδήποτε στάθμιση και ότι τελικά δεν επρόκειτο για ένα μεμονωμένο περιστατικό οφειλόμενο σε παραδρομή, αλλά για συστημική αστοχία της Τράπεζας, η οποία, παραβλέποντας τη δυναμική μικρών κοινωνιών όπως αυτή των Ψ επιτρέπει αντίστοιχες συμπεριφορές. Ο καταγγέλλων ουδέν όμως στοιχείο προσκόμισε, από το οποίο να αποδεικνύεται ο εν λόγω ισχυρισμός.

Η καταγγελλόμενη Τράπεζα, τόσο κατά τη συνεδρίαση όσο και με το υπόμνημά της, υποστήριξε τα εξής:

- Ότι σύμφωνα με την κατάθεση του υπαλλήλου, στις …προσήλθε στο κατάστημα η Β, η οποία του ήταν παντελώς άγνωστη, και επικαλούμενη την ιδιότητα της κληρονόμου της αποθανούσας Γ, ζήτησε να λάβει γνώση της κίνησης των λογαριασμών της, ο δε υπάλληλος, χορήγησε τα ζητηθέντα στοιχεία, χωρίς να ζητήσει τη γνωμάτευση της Νομικής Υπηρεσίας, βασιζόμενος στο από … έγγραφο Νομιμοποίησης Κληρονόμων (προσκομίζεται ως Σχετικό 1), το οποίο είχε εκδοθεί νομοτύπως σύμφωνα με τις σχετικές διαδικασίες της Τράπεζας αφού είχαν ληφθεί υπόψη όλα τα απαραίτητα νομιμοποιητικά έγγραφα και το οποίο περιλάμβανε την αιτούσα ως νόμιμη κληρονόμο της ως άνω θανούσης, παραβλέποντας εκ παραδρομής το γεγονός ότι υπήρχαν συνδικαιούχοι στους λογαριασμούς και παρά το γεγονός ότι στις παρατηρήσεις του εν λόγω εγγράφου αναφέρεται ρητά το εξής: «*Στους κληρονόμους μπορεί να δοθεί ενημέρωση για τυχόν ατομικούς λογαριασμούς καθώς και για τυχόν άλλα προϊόντα και έννομες σχέσεις που τηρούσε στην Τράπεζά μας. Δεν θα πρέπει να δοθεί καμία πληροφορία για τυχόν κοινούς λογαριασμούς*». Η Τράπεζα ανέφερε ότι επρόκειτο για μια βεβιασμένη, απερίσκεπτη ενέργεια που οφειλόταν σε ανθρώπινο σφάλμα και όχι σε δόλο του υπαλλήλου, η οποία συνέβη χωρίς υπαιτιότητά της.

- Όσον αφορά τον τρόπο χειρισμού του περιστατικού αφού έλαβε γνώση του, η Τράπεζα υποστήριξε ότι κινητοποιήθηκαν αμέσως οι αρμόδιες Μονάδες και διερεύνησαν ενδελεχώς το περιστατικό, ακολούθως κινήθηκε πειθαρχική διαδικασία κατά του εν λόγω υπαλλήλου ο οποίος κλήθηκε να παράσχει εξηγήσεις και κατόπιν στάθμισης όλων των παραμέτρων της υπόθεσης, του επιβλήθηκε η πειθαρχική ποινή της έντονης προφορικής επίπληξης και τέθηκε σε καθεστώς συνεχούς εποπτείας και παρακολούθησης από τα αρμόδια όργανα της Τράπεζας.

- Αναφορικά με τη γενική συμμόρφωσή της με τον ΓΚΠΔ, η Τράπεζα τόνισε ότι έχει λάβει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια της επεξεργασίας, προς απόδειξη δε του σχετικού ισχυρισμού παραθέτει ενδεικτική περιγραφή των μέτρων αυτών προσκομίζοντας και επικαλούμενη τα σχετικά έγγραφα διαδικασιών και πολιτικών της, καθώς και έγγραφα ενημέρωσης και εκπαίδευσης των υπαλλήλων της για την προστασία του τραπεζικού απορρήτου και για την τήρηση των αρχών επεξεργασίας του ΓΚΠΔ. Επιπλέον η Τράπεζα επικαλείται τα σχετικά υπηρεσιακά σημειώματα που εκδίδει κατά καιρούς, απευθυνόμενη στο σύνολο του προσωπικού της, όπως επί του προκειμένου ζητήματος, το από … υπηρεσιακό σημείωμα … της Κανονιστικής Συμμόρφωσης Ομίλου, σχετικά με την τήρηση τραπεζικού απορρήτου (Σχετικό 4), όπου αναφέρεται ρητά ότι το τραπεζικό απόρρητο ισχύει ακόμα και στην περίπτωση κληρονόμων αποβιώσαντος συνδικαιούχου, οι οποίοι δεν δικαιούνται να λάβουν γνώση των κινήσεων και του υπολοίπου κοινού διαζευκτικού λογαριασμού, αλλά και άλλες Πολιτικές και Διαδικασίες που αφορούν τη διαχείριση των στοιχείων αποθανόντος πελάτη. Συνεπώς, η Τράπεζα ισχυρίζεται ότι έχει λάβει όλα τα απαιτούμενα μέτρα και έχει θεσπίσει όλες τις απαραίτητες διαδικασίες, όμως δεν μπορεί να αποτρέψει τον αστάθμητο παράγοντα του ανθρώπινου σφάλματος.

- Σε σχέση με τα μέτρα που έλαβε μετά την επέλευση του υπό κρίση περιστατικού για το μέλλον, η Τράπεζα ανέφερε ότι εξέδωσε το υπηρεσιακό σημείωμα 2022/1252 με ημερομηνία 23/06/2022 προς όλο το προσωπικό της (προσκομίζεται ως Σχετικό 10) και στο οποίο επαναλαμβάνονται οι οδηγίες περί αυστηρής τήρησης του τραπεζικού απορρήτου ακόμα και στην περίπτωση κληρονόμων αποβιώσαντος δικαιούχου, οι οποίοι δεν δικαιούνται να λάβουν γνώση των κινήσεων και του υπολοίπου κοινού διαζευκτικού λογαριασμού.

- Τέλος, αναφορικά με τη μη γνωστοποίηση του περιστατικού στην Αρχή κατ' άρθρο 33 ΓΚΠΔ και στο υποκείμενο, κατ' άρθρο 34 ΓΚΠΔ, η Τράπεζα επανέλαβε τον αρχικό ισχυρισμό της, ότι για να συντρέχει περιστατικό παραβίασης δεδομένων σύμφωνα με τον ορισμό του άρθρου 4 στοιχ. 12 ΓΚΠΔ, θα πρέπει να έχει συντελεστεί παραβίαση ασφάλειας, η οποία σχετίζεται με έλλειψη υιοθέτησης και εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων του άρθρου 32 ΓΚΠΔ, πράγμα που δεν συντρέχει εν προκειμένω, ενώ θεωρεί ότι το συγκεκριμένο περιστατικό δεν ανάγεται

στο πεδίο ευθύνης της Τράπεζας ούτε μπορεί να της καταλογιστεί, καθώς οφείλεται αποκλειστικά και μόνο σε ανθρώπινο λάθος, το οποίο η ίδια δεν θα μπορούσε να αποτρέψει. Συνεπώς, κατά την άποψή της, δεν έχει συντελεστεί παραβίαση των διατάξεων των άρθρων 32 και 33 ΓΚΠΔ.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου και αφού άκουσε τον εισηγητή και τη βοηθό εισηγήτρια, η οποία αποχώρησε μετά τη συζήτηση της υπόθεσης και πριν από τη διάσκεψη, μετά από διεξοδική συζήτηση

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 Τράπεζας Πειραιώς 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, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, β) της δυνατότητας διασφάλισης του απορρήτου, της*

ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος, δ) της διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας. 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 της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ (νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων –EDPB) 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.»* 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 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*». 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*». Συνεπώς, 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. Η υποχρέωση του άρθρο 33 είναι αυτοτελής και ανεξάρτητη από την υποχρέωση του υπεύθυνου επεξεργασίας να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας, που θεσπίζεται με το άρθρο 32 ΓΚΠΔ. 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)».

6. Στην υπό εξέταση περίπτωση από τα στοιχεία του φακέλου προέκυψαν τα εξής:

Στις … μετέβη σε κατάστημα της καταγγελλόμενης Τράπεζας η Β, η οποία επικαλούμενη την ιδιότητα της κληρονόμου της αποθανούσας Γ, ζήτησε να λάβει γνώση της κίνησης των λογαριασμών της τελευταίας. Ο υπάλληλος στον οποίο απευθύνθηκε, βασιζόμενος στο από … έγγραφο Νομιμοποίησης Κληρονόμων, το οποίο είχε εκδοθεί σύμφωνα με τις σχετικές διαδικασίες της Τράπεζας και το οποίο περιλάμβανε την αιτούσα ως νόμιμη κληρονόμο της ως άνω θανούσης, χωρίς να ζητήσει τη γνωμάτευση της Νομικής Υπηρεσίας, χορήγησε τις ζητηθείσες αναλυτικές κινήσεις των λογαριασμών, παραβλέποντας το γεγονός ότι σε δύο τραπεζικούς λογαριασμούς (με αριθμούς … και …) ο καταγγέλλων ήταν αρχικά συνδικαιούχος με πρώτη δικαιούχο τη θεία του, Γ, από δε τον θάνατό της στις … και εφεξής, ήταν μοναδικός δικαιούχος. Ακολούθως η Β υπέβαλε αγωγή ενώπιον του Μονομελούς Πρωτοδικείου Χ εναντίον του καταγγέλλοντος με αντικείμενο κληρονομικές αξιώσεις, στο πλαίσιο της οποίας επικαλέστηκε και προσκόμισε με τις από … προτάσεις της, τις εν λόγω αναλυτικές κινήσεις λογαριασμών του καταγγέλλοντος, οι οποίες αφορούσαν και το διάστημα μετά το θάνατο της πρώτης δικαιούχου και μέχρι τον …. Αμέσως μόλις έλαβε γνώση των παραπάνω, ο καταγγέλλων μετέβη στο Υποκατάστημα Ψ, όπου ο διευθυντής Δ επικαλέστηκε το τραπεζικό απόρρητο και ισχυρίστηκε ότι η Τράπεζα ουδέποτε θα χορηγούσε τα εν λόγω στοιχεία. Το μήνα … του … ο καταγγέλλων διαμαρτυρήθηκε εγγράφως για το εν λόγω περιστατικό στην Τράπεζα, υποβάλλοντας διά του πληρεξουσίου δικηγόρου του το υπ' αρ. πρωτ. … αίτημα και ακολούθως έλαβε την από … έγγραφη απάντηση, σύμφωνα με την οποία η Τράπεζα έχει λάβει όλα τα απαραίτητα μέτρα προκειμένου να διαφυλάσσεται το τραπεζικό απόρρητο των πελατών της σύμφωνα με το ισχύον θεσμικό πλαίσιο, καθώς

και ότι επιλαμβάνεται αρμοδίως σε περιπτώσεις όπως η υπό κρίση υπόθεση που της γνωστοποιήθηκε, κατ' εφαρμογή των εσωτερικών της διαδικασιών. Αν και η Τράπεζα φαίνεται ότι είχε λάβει κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας των δεδομένων, συμπεριλαμβανομένης της κατάλληλης εκπαίδευσης των υπαλλήλων της για τις διαδικασίες χορήγησης στοιχείων λογαριασμών σε κληρονόμους, δεν προέκυψε ότι προέβη σε οποιαδήποτε ενέργεια μετά την ειδοποίησή της από τον καταγγέλλοντα για το εν λόγω περιστατικό. Αφότου ζητήθηκαν οι απόψεις της Τράπεζας εκ μέρους της Αρχής (στις 20/5/2022) η Τράπεζα απάντησε (στις 6/6/2022) ότι είχε κινήσει πειθαρχική διαδικασία εναντίον του υπαλλήλου. Η εν λόγω διαδικασία είχε ως αποτέλεσμα την επιβολή της πειθαρχικής ποινής της έντονης προφορικής επίπληξης και την εποπτεία του υπαλλήλου, σύμφωνα με όσα υποστήριξε η Τράπεζα στο πλαίσιο της ακρόασης. Επιπλέον, σε συνέχεια του περιστατικού, η Τράπεζα εξέδωσε υπηρεσιακό σημείωμα (στις 23/06/2022) προς όλο το προσωπικό της με το οποίο υπενθυμίζονται οι οδηγίες περί αυστηρής τήρησης του τραπεζικού απορρήτου στην περίπτωση κληρονόμων αποβιώσαντος δικαιούχου κοινού λογαριασμού. Ωστόσο, μολονότι η Τράπεζα αναγνώρισε ότι η διαβίβαση των δεδομένων του καταγγέλλοντος εν προκειμένω έγινε παράνομα και οφείλεται σε σφάλμα του υπαλλήλου της, δεν προχώρησε σε γνωστοποίηση του περιστατικού στην Αρχή κατά το άρθρο 33 ΓΚΠΔ ούτε σε γνωστοποίησή του στον καταγγέλλοντα κατά το άρθρο 34 ΓΚΠΔ, θεωρώντας ότι δεν είχε τη σχετική υποχρέωση, δεδομένου ότι είχε λάβει επαρκή τεχνικά και οργανωτικά μέτρα ασφάλειας κατά το άρθρο 32 ΓΚΠΔ.

Δεδομένων των ανωτέρω εκτιθέμενων πραγματικών περιστατικών, διαπιστώνεται ότι η χορήγηση των προσωπικών δεδομένων του καταγγέλλοντος στην αντίδικό του εκ μέρους της καταγγελλόμενης Τράπεζας έγινε χωρίς νόμιμη βάση, κατά παράβαση της αρχής της νομιμότητας 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 επεξεργασία έλαβε χώρα παρά τις αντίθετες οδηγίες της καταγγελλόμενης, ως Υπεύθυνου Επεξεργασίας προς το προσωπικό της. Πρόκειται επομένως για περιστατικό παραβίασης δεδομένων (παραβίαση ασφάλειας που οδήγησε σε άνευ άδειας κοινολόγηση), το οποίο αποδίδεται σε παραδρομή

συγκεκριμένου υπαλλήλου. Το σφάλμα του υπαλλήλου της Τράπεζας δεν συνιστά λόγο απαλλαγής της από την ευθύνη της ορθής τήρησης των διαδικασιών που έχει θεσπίσει προς αποτροπή περιστατικών προσβολής των προσωπικών δεδομένων των πελατών της, διότι ο υπάλληλος ενεργούσε ως προστηθείς, στο πλαίσιο άσκησης των καθηκόντων που η Τράπεζα του είχε αναθέσει, με συνέπεια την αντικειμενική ευθύνη της Τράπεζας κατ' άρθρο 922 Α.Κ. Για τον ίδιο λόγο άλλωστε και δεδομένου ότι ο υπάλληλος ενεργεί υπό την εποπτεία και τις εντολές της Τράπεζας (βλ. άρθρο 29 ΓΚΠΔ και εξ αντιδιαστολής από τον ορισμό του «τρίτου» στο άρθρο 4 στοιχ. 10 ΓΚΠΔ), ο εκάστοτε υπάλληλος δεν θεωρείται τρίτος κατά την άσκηση των καθηκόντων που του έχουν ανατεθεί και οι ενέργειές του αποδίδονται ευθέως στην Τράπεζα, ως υπεύθυνο επεξεργασίας.

7. Περαιτέρω, παρ' όλο που η Τράπεζα αναγνωρίζει ότι παράνομα χορηγήθηκαν οι εν λόγω πληροφορίες που εμπίπτουν στο τραπεζικό απόρρητο του καταγγέλλοντος, και παρότι επικαλείται ότι διερεύνησε το περιστατικό, ότι κίνησε τη σχετική πειθαρχική διαδικασία και ότι εξέδωσε σχετικό υπηρεσιακό σημείωμα με το οποίο υπενθύμιζε στους υπαλλήλους τις υποχρεώσεις τους αναφορικά με τη διαχείριση των στοιχείων θανόντων, δεν γνωστοποίησε το συμβάν στην Αρχή ως περιστατικό παραβίασης δεδομένων κατά το άρθρο 33 ΓΚΠΔ ούτε προέβη σε γνωστοποίησή του προς το υποκείμενο κατά το άρθρο 34 ΓΚΠΔ, ισχυριζόμενη ότι αυτό δεν ανάγεται στο πεδίο ευθύνης της και επικαλούμενη σχετική απόφαση της Βελγικής Αρχής, σύμφωνα με την οποία, εφόσον έχουν ληφθεί κατάλληλα τεχνικά και οργανωτικά μέτρα κατά το άρθρο 32 ΓΚΠΔ και εφόσον το περιστατικό οφείλεται σε ανθρώπινο σφάλμα που δεν μπορεί να προληφθεί και να αποτραπεί, δεν υπάρχει υποχρέωση γνωστοποίησης.
Η Τράπεζα με το υπόμνημά της προσκόμισε επαρκή στοιχεία για την τεκμηρίωση του ισχυρισμού ότι έχει λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας της επεξεργασίας, επομένως προκύπτει ότι δεν υπήρξε παραβίαση του άρθρου 32 ΓΚΠΔ. Ωστόσο πρέπει να σημειωθεί ότι παρά τη λήψη και εφαρμογή κατάλληλων μέτρων ασφάλειας είναι πάντα πιθανό να συμβεί ένα περιστατικό το οποίο να αποφέρει πλήγμα στους στόχους της ασφάλειας, όπως εν προκειμένω στην εμπιστευτικότητα των δεδομένων. Τα τεχνικά και οργανωτικά μέτρα που περιγράφονται στο άρθρο 32 ΓΚΠΔ, είναι μεν απαραίτητα για το σκοπό της

πρόληψης, δεν είναι όμως ικανά να αποτρέψουν κάθε πιθανό περιστατικό ασφάλειας. Για το λόγο αυτό, συμπληρωματικά και ανεξάρτητα από την υποχρέωση που θεσπίζει το άρθρο 32 ΓΚΠΔ, στις περιπτώσεις περιστατικών παραβίασης ισχύουν και εφαρμόζονται τα άρθρα 33 και 34 ΓΚΠΔ, ώστε να αντιμετωπίσουν στην πράξη τυχόν παραβάσεις, κατά τρόπο «κατασταλτικό». Με άλλα λόγια, είναι δυνατόν να συμβεί μια παραβίαση της ασφάλειας χωρίς αυτή να οφείλεται σε παράβαση του άρθρου 32 ΓΚΠΔ, αντίθετα σε όσα υποστηρίζει η καταγγελλόμενη, καθώς μια τέτοια ερμηνεία δεν μπορεί να συναχθεί από το γράμμα των σχετικών διατάξεων. Περαιτέρω, από την παρ. 3 (στοιχ. δ) του άρθρου 33 ΓΚΠΔ προκύπτει η υποχρέωση του υπευθύνου επεξεργασίας να «*λάβει ή να προτείνει προς λήψη μέτρα για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της*». Εν προκειμένω, η Τράπεζα δεν επικαλέστηκε ότι έλαβε οποιοδήποτε μέτρο προς άμβλυνση των συνεπειών της συγκεκριμένης παράβασης, την οποία αναγνώρισε ως τέτοια και απέδωσε στο ανθρώπινο σφάλμα του υπαλλήλου της. Τέτοιο μέτρο θα μπορούσε να είναι, για παράδειγμα, ένα έγγραφο προς την αποδέκτη των δεδομένων, με το οποίο να δηλώνεται ότι η χορήγηση έλαβε χώρα παρανόμως, εκ παραδρομής του υπαλλήλου και να ζητείται η καταστροφή τους. Επιπλέον δεν ενημερώθηκε ο καταγγέλλων ως υποκείμενο σύμφωνα με το άρθρο 34 ΓΚΠΔ για τα σχετικά μέτρα, κατά τρόπο που θα μπορούσε πιθανώς να συμβάλει στην άμβλυνση των συνεπειών του περιστατικού παραβίασης (εάν, για παράδειγμα, ο καταγγέλλων προσκόμιζε στο Δικαστήριο ένα έγγραφο με το οποίο η Τράπεζα αναγνωρίζει ως μη νόμιμη τη διαβίβαση των στοιχείων στην αντίδικό του). Εν προκειμένω, για να ενημερωθεί το υποκείμενο για τη θέση της Τράπεζας ως προς το περιστατικό, χρειάστηκε να προβεί σε καταγγελία ενώπιον της Αρχής. Παρά το γεγονός, λοιπόν, ότι η Τράπεζα φαίνεται να έχει θεσπίσει επαρκή μέτρα ασφάλειας, τα οποία επικαιροποιεί όποτε αυτό παρίσταται αναγκαίο και άρα δεν διαπιστώνεται παράβαση του άρθρου 32 ΓΚΠΔ, διαπιστώνεται παράβαση των άρθρων 33 και 34 ΓΚΠΔ εκ μέρους της, για τους ανωτέρω αναφερόμενους λόγους.

8. Κατόπιν των ανωτέρω, από τα στοιχεία του φακέλου και κατόπιν της ακροαματικής διαδικασίας, η Αρχή διαπιστώνει εκ μέρους της καταγγελλόμενης Τράπεζας:

α) Παραβίαση της αρχής της νομιμότητας της επεξεργασίας (άρθρα 5 παρ. 1 α), 6 και 13 ΓΚΠΔ), δεδομένου ότι χορηγήθηκαν παράνομα, ήτοι χωρίς νόμιμη βάση και αδιαφανώς, χωρίς ενημέρωση του υποκειμένου, τα δεδομένα κινήσεων δύο τραπεζικών λογαριασμών του καταγγέλλοντος για χρονικό διάστημα 4 ετών.
β) Παραβίαση της αρχής της εμπιστευτικότητας των δεδομένων (άρθρο 5 παρ. 1 στ) ΓΚΠΔ), διότι η ως άνω επεξεργασία οδήγησε σε παράνομη διαρροή προσωπικών πληροφοριών του καταγγέλλοντος στην αντίδικό του.
γ) Παραβίαση των εκ των άρθρων 33 και 34 ΓΚΠΔ υποχρεώσεων της καταγγελλόμενης, δεδομένου ότι δεν γνωστοποίησε το περιστατικό στην Αρχή ή στο υποκείμενο, ούτε έλαβε μέτρα για την άμβλυνση των συνεπειών της παραβίασης, όπως θα ήταν, για παράδειγμα, η επικοινωνία με την αποδέκτρια των δεδομένων προκειμένου να επιστρέψει ή να καταστρέψει τα παρανόμως χορηγηθέντα προσωπικά δεδομένα.

9. Με βάση τα ανωτέρω, η Αρχή κρίνει ότι συντρέχει περίπτωση να ασκήσει τις κατά τα άρθρα 58 παρ. 2 θ) και 83 ΓΚΠΔ διορθωτικές εξουσίες της (επιβολή προστίμου) όσον αφορά τις ανωτέρω διαπιστωθείσες παραβάσεις. Για τον καθορισμό της κύρωσης η Αρχή λαμβάνει υπόψη τα κριτήρια επιμέτρησης του προστίμου που ορίζονται στο άρθρο 83 παρ. 2 του ΓΚΠΔ που έχουν εφαρμογή στην παρούσα υπόθεση.

Ειδικότερα, λαμβάνονται ιδιαιτέρως υπόψη:

α) Η φύση, η βαρύτητα και η διάρκεια της παράβασης: η παράβαση αφορούσε πληροφορίες για το υπόλοιπο και τις κινήσεις δύο τραπεζικών λογαριασμών του καταγγέλλοντος για 4 έτη, αφορούσε δηλαδή πληροφορίες ευαίσθητης φύσης που προστατεύονται από το τραπεζικό απόρρητο. Λαμβάνεται υπόψη ότι πιθανώς η αντίδικος του καταγγέλλοντος και αποδέκτρια των δεδομένων θα μπορούσε να αποκτήσει πρόσβαση στις εν λόγω πληροφορίες κατόπιν δικαστικής απόφασης (επίδειξη εγγράφων).
β) Το γεγονός ότι η παράβαση οφείλεται σε αμέλεια υπαλλήλου της Τράπεζας. Πρόκειται πάντως για βαριά αμέλεια, δεδομένου ότι το έγγραφο στο οποίο ο υπάλληλος βασίστηκε για να χορηγήσει τα ζητηθέντα στοιχεία στην αντίδικο του

καταγγέλλοντος (Νομιμοποίηση Κληρονόμων) περιλάμβανε τη ρητή παρατήρηση ότι δεν επιτρέπεται να δοθούν στους κληρονόμους πληροφορίες για κοινούς λογαριασμούς της θανούσης.

γ) Το γεγονός ότι η ενέργεια του υπαλλήλου της Τράπεζας θεμελιώνει και την ευθύνη της ως υπεύθυνου επεξεργασίας.

δ) Το γεγονός ότι από την παράβαση επηρεάστηκε μόνο ένα υποκείμενο.

ε) Το γεγονός ότι η καταγγελλόμενη Τράπεζα, ως υπεύθυνος επεξεργασίας, δεν προέβη σε οποιαδήποτε ενέργεια για την άμβλυνση των συνεπειών της παράβασης προς το υποκείμενο. Σημειώνεται ότι ο καταγγέλλων δεν θα είχε λάβει γνώση της θέσης της Τράπεζας για το περιστατικό, εάν δεν είχε προσφύγει στην Αρχή, αφού η αρχική από … ενημέρωσή του ήταν τυπική («τηρούμε όλα τα μέτρα, επιλαμβανόμαστε αρμοδίως» κλπ). Η αντίδραση της Τράπεζας αφού πληροφορήθηκε για το συμβάν από τον καταγγέλλοντα δεν ήταν άμεση, αντιθέτως πέρασαν αρκετοί μήνες μέχρι να το διερευνήσει, όταν ζητήθηκαν οι απόψεις της από την Αρχή.

στ) Ο βαθμός ευθύνης της Τράπεζας με βάση τα ληφθέντα τεχνικά και οργανωτικά μέτρα ασφάλειας: Από τα στοιχεία που προσκομίστηκαν στην Αρχή προκύπτει ότι η Τράπεζα έχει λάβει κατάλληλα τεχνικά και οργανωτικά μέτρα σύμφωνα με το άρθρο 32 ΓΚΠΔ, ωστόσο δεν προκύπτει ότι εφαρμόζονται σε κάθε περίπτωση ούτε ότι η Τράπεζα επιβλέπει την εφαρμογή τους ασκώντας περιοδικούς ελέγχους στο προσωπικό της.

ζ) Ο τρόπος με τον οποίος πληροφορήθηκε η Αρχή την παράβαση (μέσω καταγγελίας).

η) Το μεγάλο μέγεθος της καταγγελλόμενης Τράπεζας.

θ) Το γεγονός ότι στην Τράπεζα έχει επιβληθεί στο παρελθόν ξανά πρόστιμο για παράβαση της αρχής της εμπιστευτικότητας και των υποχρεώσεών της βάσει των άρθρων 33 και 34 ΓΚΠΔ (βλ. απόφαση 6/2022).

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η ΑΡΧΗ

Επιβάλλει στην Τράπεζα Πειραιώς Α.Ε. ως υπεύθυνο επεξεργασίας με βάση το άρθρο 58 παρ. 2 εδαφ. θ του ΓΚΠΔ συνολικό πρόστιμο ύψους τριάντα χιλιάδων (30.000 €) ευρώ για τις παραβάσεις της αρχής της νομιμότητας της επεξεργασίας (άρ. 5 παρ. 1 α) ΓΚΠΔ), της αρχής της εμπιστευτικότητας των δεδομένων (άρ. 5 παρ. 1 στ) ΓΚΠΔ) και των υποχρεώσεών της εκ των άρθρων 33 και 34 ΓΚΠΔ.

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