ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 10-01-2025
Αριθ. Πρωτ.: 147

ΑΠΟΦΑΣΗ 3/2025

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε, μετά από πρόσκληση του Προέδρου της, σε συνεδρίαση μέσω τηλεδιάσκεψης στις 18-06-2024, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Στη συνεδρίαση παρέστησαν ο Πρόεδρος της Αρχής, Κωνσταντίνος Μενουδάκος, τα τακτικά μέλη Χαράλαμπος Ανθόπουλος, Σπυρίδων Βλαχόπουλος, Χρήστος Καλλονιάτης, Γρηγόριος Τσόλιας, το αναπληρωματικό μέλος Νικόλαος Φαλδαμής σε αντικατάσταση του τακτικού μέλους Αικατερίνης Ηλιάδου, η οποία παρότι κλήθηκε νομίμως εγγράφως δεν παρέστη λόγω κωλύματος, και το τακτικό μέλος Κωνσταντίνος Λαμπρινουδάκης ως εισηγητής. Παρούσες, χωρίς δικαίωμα ψήφου, ήταν οι Χάρις Συμεωνίδου και Γεωργία Παναγοπούλου, ειδικές επιστήμονες – ελέγκτριες, ως βοηθοί εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών υποθέσεων της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Με τις καταγγελίες με αριθ. πρωτ. Γ/ΕΙΣ/9060/24-07-2022 του Α και Γ/ΕΙΣ/9061/24-07-2022 της Β, όμοιου περιεχομένου, οι καταγγέλλοντες στρέφονται κατά της Εθνικής Τράπεζας (στο εξής αναφερόμενη ως καταγγελλόμενη), καταγγέλλοντας πιθανό περιστατικό παραβίασης των δεδομένων τους και μη ικανοποίηση του δικαιώματος πρόσβασής τους κατά το άρθρο 15 ΓΚΠΔ. Ειδικότερα, σύμφωνα με τις ανωτέρω όμοιες καταγγελίες, στις 26/3/2022, ο πελάτης της Εθνικής Τράπεζας Γ προσπάθησε να μεταφέρει το ποσό των 90€ μέσω του συστήματος IRIS

Λεωφ. Κηφισίας 1-3, 11523 Αθήνα
T: 210 6475 600 • E: contact@dpa.gr • www.dpa.gr

από την εφαρμογή iBank Pay στον καταγγέλλοντα Α, χρησιμοποιώντας τον αριθμό του κινητού τηλεφώνου του τελευταίου, τον οποίο είχε αποθηκευμένο στις επαφές του. Ωστόσο, σύμφωνα με τις καταγγελίες, παρ' όλο που η συναλλαγή ολοκληρώθηκε και εστάλη σχετική επιβεβαίωση στον πληρωτή, το ποσό δεν πιστώθηκε στον λογαριασμό του πρώτου καταγγέλλοντος Α, αλλά στον λογαριασμό της δεύτερης καταγγέλλουσας Β, με την οποία, όπως αναφέρει, δεν συνδέεται με κανένα τρόπο. Σύμφωνα με τις ως άνω καταγγελίες, η συναλλαγή αυτή δεν ήταν δυνατό να ακυρωθεί, ενώ σε συνέχεια του ανωτέρω περιστατικού, οι καταγγέλλοντες το γνωστοποίησαν στην καταγγελλόμενη Τράπεζα και άσκησαν το κατ' άρθρο 15 ΓΚΠΔ δικαίωμα πρόσβασής τους στα προσωπικά δεδομένα τους, προκειμένου να πληροφορηθούν σχετικά με τη διαφαινόμενη αδικαιολόγητη σύνδεση των λογαριασμών τους, αφ' ενός μέσω της φόρμας παραπόνων της ιστοσελίδας της Τράπεζας (https://www.nbg.gr/el/footer/forma-paraponwn) και αφ' ετέρου μέσω ηλεκτρονικού μηνύματος στη διεύθυνση dpo@nbg.gr του Υπευθύνου Προστασίας Δεδομένων της Τράπεζας, στις 29/3/2022. Ωστόσο, όπως αναφέρουν οι καταγγέλλοντες, η Τράπεζα δεν απάντησε ποτέ στο παράπονο που υπέβαλαν, ενώ ούτε το αίτημά τους προς τον Υπεύθυνο Προστασίας Δεδομένων ικανοποιήθηκε, παρότι ενημερώθηκαν από την αρμόδια μονάδα της Τράπεζας εντός τριάντα (30) ημερών από την υποβολή του αιτήματος, ότι θα κάνει χρήση των επιπλέον εξήντα (60) ημερών για την απάντηση, χωρίς κάποια αιτιολόγηση (σημ. στην εν λόγω απάντηση, που προσκομίζεται ως συν. 5, αναφέρεται ότι «*λόγω της δυσμενούς τρέχουσας συγκυρίας, δεν είναι δυνατή η ικανοποίηση του αιτήματός σας εντός προθεσμίας ενός μήνα*»). Σύμφωνα δε με τις καταγγελίες, η καταγγελλόμενη δεν είχε ακόμα απαντήσει επί της ουσίας των ανωτέρω αιτημάτων, ενώ το ίδιο περιστατικό συνέβη στις 19/6/2022, όταν ποσό ύψους 490 ευρώ που προοριζόταν για τον πρώτο καταγγέλλοντα πιστώθηκε στο λογαριασμό της δεύτερης καταγγέλλουσας. Στο πλαίσιο διερεύνησης των καταγγελιών, η Αρχή με το Γ/ΕΞΕ/2877/15-11-2022 έγγραφο κοινοποίησε τις καταγγελίες και όλα τα σχετικά έγγραφα στην καταγγελλόμενη Τράπεζα και την κάλεσε να εκθέσει τις απόψεις της επί των καταγγελλομένων, παρέχοντας κάθε σχετικό στοιχείο τεκμηρίωσης. Την κάλεσε ειδικότερα α) να γνωρίσει στην Αρχή εάν και με ποιον τρόπο ανταποκρίθηκε στα ως άνω αιτήματα πρόσβασης των καταγγελλόντων, καθώς και πού οφείλεται τυχόν

καθυστέρηση, β) να διευκρινίσει εάν αξιολόγησε τα ανωτέρω εκτιθέμενα πραγματικά περιστατικά ως πιθανό περιστατικό παραβίασης προσωπικών δεδομένων και σε ποιες ενέργειες προέβη αναφορικά με τον χειρισμό του.

Με την υπ' αρ. πρωτ. Γ/ΕΙΣ/12646/19-12-2022 απάντησή της, η καταγγελλόμενη Τράπεζα, αρχικά περιέγραψε τον τρόπο λειτουργίας της εφαρμογής i-bank Pay, μέσω της οποίας οι πελάτες έχουν τη δυνατότητα να μεταφέρουν χρήματα άμεσα σε λογαριασμούς φίλων τους «γνωρίζοντας απλά το τηλέφωνό τους ή το προφίλ τους στο facebook», και η οποία χρησιμοποιείται με χρήση κωδικών digital banking, προπληρωμένης κάρτας ή i-bank Payband. Μέσω αυτής παρέχονται δύο τρόποι αποστολής χρημάτων: α) μεταξύ πελατών της Εθνικής Τράπεζας που εγγράφονται στην υπηρεσία p2p (person to person) με την οποία μεταφέρουν χρήματα στις επαφές τους που είναι επίσης πελάτες εγγεγραμμένοι στην ίδια υπηρεσία και β) σε εγγεγραμμένους στην υπηρεσία IRIS Online Payments του διατραπεζικού συστήματος ΔΙΑΣ, οι οποίοι διατηρούν λογαριασμό είτε στην Εθνική είτε σε άλλη τράπεζα. Η Τράπεζα διευκρίνισε ότι αν ο αποδέκτης της πληρωμής δεν έχει την εφαρμογή i-bank pay, αρκεί να είναι εγγεγραμμένος στην υπηρεσία IRIS Online Payments, οπότε η αποστολή των χρημάτων σε αυτόν γίνεται με χρήση είτε του αριθμού τηλεφώνου είτε του ΑΦΜ του. Σημείωσε επίσης ότι για πληρωμές άνω των 25 ευρώ για φίλους και άνω των 75 ευρώ για εμπόρους, εκτός από το username και το password του χρήστη, απαιτείται και η εισαγωγή OTP (One Time Password). Αναφορικά με τα καταγγελλόμενα πραγματικά περιστατικά, η Τράπεζα απάντησε ότι κατόπιν διερεύνησης από την αρμόδια Μονάδα της προέκυψαν τα εξής:

- ότι η καταγγέλλουσα Β εγγράφηκε στην υπηρεσία i-bank Pay p2p επιλέγοντας ως τηλέφωνο μεταφοράς τον αριθμό κινητού τηλεφώνου Ψ, δηλαδή τον αριθμό που σύμφωνα με την καταγγελία ανήκει στον καταγγέλλοντα Α, «*γεγονός που σημαίνει ότι η ίδια είχε τη δεδομένη χρονική στιγμή το εν λόγω τηλέφωνο στη διάθεσή της και καταχώρισε το μήνυμα OTP που εστάλη (στη συσκευή τηλεφώνου) κατά την εγγραφή στην υπηρεσία. Κατά συνέπεια στα συστήματα της ΕΤΕ, ο εν λόγω τηλεφωνικός αριθμός συνδέθηκε με τον καταθετικό λογαριασμό της Β για μεταφορές p2p*».

- ότι παράλληλα, ο Α είχε εγγραφεί στην υπηρεσία IRIS Online Payments της ΔΙΑΣ με τον ίδιο ανωτέρω αναφερόμενο αριθμό τηλεφώνου (Ψ).

- ότι η από 26.3.2022 μεταφορά του ποσού των 90€ έγινε από τον Γ με χρήση της εφαρμογής i-bank Pay προς τον αριθμό κινητού τηλεφώνου της επιλογής του (Ψ) και πιστώθηκε άμεσα σε λογαριασμό που ήταν συνδεδεμένος με την υπηρεσία τη δεδομένη χρονική στιγμή, δηλαδή τον καταθετικό λογαριασμό της Β, σύμφωνα δε με τους όρους χρήσης της υπηρεσίας i-bank Pay, η μεταφορά χρημάτων δεν ακυρώνεται ούτε ανακαλείται.

- ότι μετά τη διαμαρτυρία των πελατών δρομολογήθηκαν οι απαραίτητες ενέργειες για τη διερεύνηση του περιστατικού και η Τράπεζα κατέβαλε κάθε δυνατή προσπάθεια για την αντιμετώπισή του σε συνεργασία με τη ΔΙΑΣ Α.Ε., δεδομένης της πολυπλοκότητάς του. Στο πλαίσιο αυτό εστάλη μήνυμα στην Β ότι το θέμα εξετάζεται, καθώς και επιστολή στον Α (από 13/9/2022) να προβεί στην απεγκατάσταση και εκ νέου εγκατάσταση της εφαρμογής με την επισήμανση να επανέλθει για περαιτέρω διερεύνηση σε περίπτωση μη επίλυσης. Καθώς δε ο πελάτης δεν επανήλθε, θεωρήθηκε ότι το ζήτημα είχε επιλυθεί.

- ότι στη συνέχεια, με αφορμή το έγγραφο της Αρχής, «*η υπόθεση επανεξετάστηκε και το ζήτημα που είχε ανακύψει με κάποιες περαιτέρω συστημικές ενέργειες που διενεργήθηκαν από την αρμόδια Μονάδα της Τράπεζας επιλύθηκε πλήρως*». Συγκεκριμένα, αφαιρέθηκε η εγγραφή της καταγγέλλουσας Β στην υπηρεσία p2p με το τηλέφωνο του καταγγέλλοντος Α, ενώ παράλληλα ζητήθηκε από τον Α να προβεί στις αναγκαίες διορθωτικές ενέργειες. Η Τράπεζα αναφέρει ότι το ζήτημα «*αφορούσε σε συστημική διαδικασία της εφαρμογής*» και προκειμένου να επιβεβαιωθεί η επίλυσή του πραγματοποιήθηκε δοκιμαστική συναλλαγή, η οποία ολοκληρώθηκε επιτυχώς.

- ότι, επομένως, δεν πρόκειται για περιστατικό παραβίασης προσωπικών δεδομένων, αλλά για συστηματική παραμετροποίηση, η οποία αποκαταστάθηκε πλήρως και οφείλονταν στην αρχική εγγραφή της καταγγέλλουσας Β στην εφαρμογή με τηλεφωνικό αριθμό που, όπως προέκυψε, ανήκει στον καταγγέλλοντα Α.

Στη συνέχεια, κατόπιν σχετικού αιτήματος της καταγγέλλουσας (με αρ. πρωτ. Γ/ΕΙΣ/135/10-01-2023), η Αρχή με το Γ/ΕΞΕ/72/10-01-2023 έγγραφό της, διαβίβασε την εν λόγω απάντηση της Τράπεζας στην καταγγέλλουσα, η οποία ακολούθως επανήλθε με το Γ/ΕΙΣ/3885/23-05-2023 συμπληρωματικό της έγγραφο, με το οποίο αφ’ ενός μεν αμφισβητεί τους ισχυρισμούς της Τράπεζας, αφ’ ετέρου επισημαίνει ότι

η Τράπεζα δεν απάντησε αναφορικά με τη μη ικανοποίηση του δικαιώματος πρόσβασής της στα προσωπικά της δεδομένα. Συγκεκριμένα, η καταγγέλλουσα αναφέρει ότι σε τηλεφωνική της επικοινωνία με την καταγγελλόμενη τράπεζα σχετικά με το ζήτημα, όταν ρώτησε πότε ακριβώς πραγματοποίησε την εγγραφή, έλαβε την αόριστη απάντηση «ου πολύ παλιά» και τονίζει ότι δεν πραγματοποίησε την εγγραφή στην εφαρμογή με τον αριθμό του Α, αφού σε αυτή την περίπτωση όλες οι συναλλαγές που θα πραγματοποιούσε μέσω της εφαρμογής θα έπρεπε να επιβεβαιώνονται από τον Α, πράγμα που ουδέποτε συνέβη. Επιπλέον, η καταγγέλλουσα αναφέρει ότι στον ίδιο τον Α δεν δόθηκε η ίδια πληροφόρηση, ενώ σε τηλεφωνική του επικοινωνία με την Τράπεζα, μετά τη 2η περίπτωση λανθασμένης μεταφοράς χρημάτων (στις 19.6.2022), η Τράπεζα τον ενημέρωσε ότι δεν έχει συνδεδεμένο με κανένα πελάτη της τον εν λόγω τηλεφωνικό αριθμό (Ψ).

Ακολούθως, και δεδομένων των ανωτέρω, κρίθηκε από την Αρχή αναγκαία η διενέργεια διοικητικού ελέγχου, βάσει της υπ' αρ. πρωτ. Γ/ΕΞΕ/2564/16-10-2023 εντολής ελέγχου του Προέδρου της Αρχής, η οποία διαβιβάστηκε με το Γ/ΕΞΕ/2570/16-10-2023 έγγραφο στην καταγγελλόμενη τράπεζα. Στο πλαίσιο του ελέγχου, με το ίδιο έγγραφο ζητήθηκε από την Τράπεζα η συμπλήρωση ερωτηματολογίου με προθεσμία απάντησης την 20/10/2023, πριν τη διενέργεια επιτόπιου ελέγχου στις εγκαταστάσεις της Τράπεζας, στις 25/10/2023, προκειμένου να συμπληρωθούν τα απαραίτητα στοιχεία, τεκμήρια και να διασαφηνιστούν οι απαντήσεις της Τράπεζας. Κατόπιν αιτήματος παράτασης της ανωτέρω προθεσμίας, το ερωτηματολόγιο απαντήθηκε με το Γ/ΕΙΣ/7704/31-10-2023 έγγραφο, όπως συμπληρώθηκε με το Γ/ΕΙΣ/7728/31-10-2023 συμπληρωματικό έγγραφο της Τράπεζας.

Με το εν λόγω έγγραφο, απατώντας στα ερωτήματα, η Τράπεζα ανέφερε, μεταξύ άλλων, τα εξής σημαντικά στοιχεία:

- Το τηλέφωνο Ψ, δηλαδή ο αριθμός που σύμφωνα με την καταγγελία ανήκει στον καταγγέλλοντα Α, είχε δηλωθεί στην εφαρμογή i-bank Pay της ΕΤΕ ως δεύτερο τηλέφωνο βάσει του οποίου μπορούσε να εντοπιστεί η Β από φίλους της προκειμένου να λάβει χρήματα.
- Προέκυψε ότι το ζήτημα οφειλόταν αποκλειστικά και μόνο σε μεμονωμένη ανθρώπινη αστοχία στο πλαίσιο ενσωμάτωσης της

υπηρεσίας IRIS pay στο Mobile Banking. Συγκεκριμένα, διαπιστώθηκε ότι κατά την ως άνω συστημική ενσωμάτωση που πραγματοποιήθηκε τον Ιούνιο του 2020, το δεύτερο τηλέφωνο που είχε καταχωρήσει η πελάτισσα στην εφαρμογή, ενεργοποιήθηκε στον λογαριασμό της στο i-bank Pay. Επισημαίνεται ότι η αρμόδια Μονάδα της Τράπεζας διερευνά τυχόν ενεργοποίηση άλλων τηλεφωνικών αριθμών, ελέγχοντας άμεσα όλους τους χρήστες της εφαρμογής.

Κατόπιν αυτών, την Τετάρτη 1/11/2023 πραγματοποιήθηκε σύμφωνα με τα παραπάνω, ο επιτόπιος έλεγχος στις εγκαταστάσεις της καταγγελλόμενης από τις ελέγκτριες της Αρχής, Γεωργία Παναγοπούλου και Χάρις Συμεωνίδου. Κατά τον έλεγχο, παρευρέθησαν εκ μέρους της Τράπεζας τα ακόλουθα στελέχη: η Δ, Επικεφαλής Διεύθυνσης Business Regulatory Compliance & Client Conduct της Τράπεζας και του Ομίλου, ο Ε, Επικεφαλής Διεύθυνσης Ψηφιακού Μετασχηματισμού, η ΣΤ, Υπεύθυνη Προστασίας Δεδομένων, η Ζ, Επικεφαλής Τομέα Τήρησης Κανονισμών και Διασφάλισης Ποιότητας, η Η, Επικεφαλής Τομέα Client Conduct της Τράπεζας, η Θ, Επικεφαλής Τομέα Διαχείρισης Εφαρμογών, Υπηρεσιών Αρχιτεκτονικής και Εποπτείας Θεμάτων Πληροφορικής της Τράπεζας και του Ομίλου, η Ι, Αναπληρώτρια Υπεύθυνη Προστασίας Δεδομένων της Τράπεζας και η Κ, Επικεφαλής Υποδιεύθυνσης Payments & Digital Services Compliance.

Όπως προέκυψε κατά τον επιτόπιο έλεγχο, η καταγγελλόμενη όντως διαπίστωσε ότι λόγω συστημικού σφάλματος, ενώ θα έπρεπε το δεύτερο τηλέφωνο που είχε καταχωρήσει η πελάτισσα στην εφαρμογή να είχε επιβεβαιωθεί με OTP προκειμένου να επικυρωθεί και να συνδεθεί με το όνομά της, αυτό επικυρώθηκε και εισήχθη κατά την ενσωμάτωση της υπηρεσίας IRIS pay στο Mobile Banking της καταγγελλόμενης. Δηλαδή ο κώδικας που εκτελέστηκε εισήγαγε και τα τηλέφωνα τα οποία ήταν σε κατάσταση «εκκρεμούς επαλήθευσης» και τα οποία δεν είχαν επικυρωθεί με OTP (one time password). Η λανθασμένη αυτή διαδικασία έτρεξε για το σύνολο των τηλεφώνων που βρίσκονταν σε αυτή την κατάσταση. Κατά τον έλεγχο, αναγνωρίστηκε επίσης η ανάγκη υποβολής γνωστοποίησης περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα και δηλώθηκε ότι έχει ανασταλεί η λειτουργία της εφαρμογής i-bank Pay, μέχρι να διερευνηθεί πλήρως το περιστατικό.

Την επόμενη ημέρα, η καταγγελλόμενη και ελεγχόμενη Τράπεζα υπέβαλε την υπ' αρ. πρωτ. Γ/ΕΙΣ/7785/02-11-2023 γνωστοποίηση περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 33 ΓΚΠΔ.

Στην υποβληθείσα φόρμα γνωστοποίησης και στα σχετικά πεδία αναφέρονται, μεταξύ άλλων, τα εξής στοιχεία που αφορούν το περιστατικό:

- Πλήθος αρχείων (κατά προσέγγιση) που αφορά το περιστατικό:
  Ένα (1) αρχείο (πίνακας στη βάση δεδομένων i-bank Pay/mobile banking)
- Πλήθος προσώπων (κατά προσέγγιση) που αφορά το περιστατικό:
  Υπάρχει ένα επιβεβαιωμένο περιστατικό που αφορά δύο πρόσωπα. Η αρμόδια Μονάδα της Τράπεζας διερευνά εάν έχουν επηρεαστεί και άλλοι πελάτες.
- Αναλυτική περιγραφή των μέτρων που είχαν ληφθεί πριν το περιστατικό:
  Σύμφωνα με τις προδιαγραφές της εφαρμογής i-bank Pay, προκειμένου να συνδέσει ένας χρήστης το κινητό του τηλέφωνο με συγκεκριμένο προϊόν (καταθετικό λογαριασμό / prepaid κάρτα / payband), καταχωρούσε καταρχήν τους κωδικούς Internet / Mobile Banking που τηρούσε στην Τράπεζα και στη συνέχεια το κινητό του και επιβεβαίωνε τη σχετική σύνδεση καταχωρώντας το OTP που του έστελνε η Τράπεζα για το σκοπό αυτό. - Η αρμόδια Μονάδα της Τράπεζας είχε προβεί σε όλους τους απαιτούμενους ελέγχους για την ορθή εφαρμογή της εφαρμογής (functional tests) και κατά τεκμήριο η υπηρεσία λειτούργησε χωρίς προβλήματα από την εισαγωγή της το 2016. - Ειδικά και προκειμένου να αντιμετωπίσουμε ενδεχόμενο αποστολής χρημάτων σε λάθος αποδέκτη (εκτιμώντας φυσικά ότι κάτι τέτοιο αν συνέβαινε θα οφείλονταν σε λάθος καταχώρηση τηλεφωνικού αριθμού στις επαφές του αποστολέα και ΟΧΙ σε πρόβλημα της τράπεζας) είχαμε προβλέψει να εμφανίζεται masked το ονοματεπώνυμο του δικαιούχου του αποδέκτη λογαριασμού προτού ολοκληρωθεί η αποστολή ώστε να είναι δυνατός ένας τελευταίος έλεγχος και επιβεβαίωση από τον αποστολέα. - Επιπλέον, στο πλαίσιο ενσωμάτωσης της υπηρεσίας i-bank Pay στο Mobile Banking και σε συνέχεια της κατάργησης της δυνατότητας σύνδεσης κάρτας στην υπηρεσία, ο πελάτης μπορούσε πλέον να συνδέσει με την υπηρεσία μόνο το κινητό τηλέφωνο που έχει δηλωμένο / επιβεβαιωμένο στο πελατοκεντρικό σύστημα της Τράπεζας.

- Φύση των πιθανών συνεπειών που θα έχουν τα πρόσωπα που επηρεάζονται από το περιστατικό:

  Εκ παραδρομής μη εγκεκριμένη (χωρίς ΟΤΡ) ενεργοποίηση κινητού τηλεφώνου που είχε καταχωρήσει η ίδια στην εφαρμογή i-bank Pay και που θα μπορούσε ενδεχομένως να οδηγήσει σε οικονομική απώλεια και αδικαιολόγητο πλουτισμό.

- Ενημερώσατε τα πρόσωπα που επηρεάστηκαν από το περιστατικό; (ΝΑΙ/ΟΧΙ/ΟΧΙ ΑΚΟΜΗ, ΑΛΛΑ ΘΑ ΕΝΗΜΕΡΩΘΟΥΝ / ΔΕΝ ΑΠΟΦΑΣΙΣΤΗΚΕ ΑΚΟΜΗ ΑΝ ΠΡΕΠΕΙ ΝΑ ΕΝΗΜΕΡΩΘΟΎΝ)

  Οι πελάτες είχαν ενημερωθεί προφορικά για την επίλυση του ζητήματος και την αποκατάσταση του λανθασμένου τηλεφώνου. Άμεσα θα λάβουν εκ νέου ενημέρωση, εγγράφως, για τα αποτελέσματα της πρόσφατης διερεύνησης. Επιπλέον, αφού ολοκληρωθεί η έρευνα, θα ενημερωθούν και τυχόν άλλα πρόσωπα που έχουν επηρεαστεί.

- Περιγραφή των μέτρων που λήφθηκαν για την αντιμετώπιση της παραβίασης:

  Α. Η άμεση αναστολή της εφαρμογής i-bank Pay

  Β. Ο έλεγχος ύπαρξης τυχόν αντίστοιχων ζητημάτων επί του συνόλου των χρηστών της εφαρμογής (σύνολο χρηστών i-bank pay: περίπου 76.000)

  Γ. Ο έλεγχος τυχόν κοινοποίησης στοιχείων χρηστών της εφαρμογής εκ των ζητημάτων που ενδεχομένως ανακύψουν εκ της ενέργειας Β.

  Δ. Ο σχεδιασμός και η υλοποίηση επιπλέον διορθωτικών μέτρων, εφόσον απαιτηθεί, όπως η επαναφορά των στοιχείων στην προτέρα κατάσταση, η θέσπιση επιπλέον δικλείδων ασφαλείας κλπ.

  Ε. Επιβεβαίωση μέσω εμφάνισης splash banner στην εφαρμογή Mobile Banking του κινητού τηλεφώνου που είναι δηλωμένο στην υπηρεσία IRIS Pay

  Ζ. Η διόρθωση της mobile εφαρμογής ώστε όταν ο χρήστης αιτείται την ενεργοποίηση σύνδεσης τηλεφώνου που βρίσκεται σε εκκρεμότητα να γίνεται μόνο με κωδικό επαλήθευσης και μόνο σε εύλογο χρονικό διάστημα από τη στιγμή της δημιουργίας της εκκρεμότητας και σε καμία περίπτωση να μην εκτελείται αυτόματη ενεργοποίηση τηλεφώνου.

Με το Γ/ΕΙΣ/8183/17-11-2023 έγγραφό της η Τράπεζα ενημέρωσε την Αρχή ότι η περαιτέρω διερεύνηση της υπόθεσης βρίσκεται σε εξέλιξη από πλευράς της, προκειμένου να υποβάλει εντός των προσεχών ημερών συμπληρωματική γνωστοποίηση με επιπρόσθετα στοιχεία. Στη συνέχεια, με το Γ/ΕΙΣ/8348/23-11-2023 έγγραφό της, η Τράπεζα προσκόμισε στην Αρχή το ιστορικό των κινήσεων της Β στην εφαρμογή i-bank Pay της Τράπεζας, όπως αυτό διαβιβάστηκε από την αρμόδια Μονάδα της Τράπεζας, στο οποίο αποτυπώνεται τόσο η αρχική εγγραφή της στην υπηρεσία, όσο και οι ενέργειες που σχετίζονται με τη σύνδεση των αριθμών τηλεφώνου με το λογαριασμό της.

Από το ιστορικό αυτό προκύπτουν τα εξής:

Η καταγγέλλουσα γράφτηκε στην υπηρεσία 14/4/2019, στις 21:02:04 μέσω της εφαρμογής i-bank pay ακολουθώντας τη διαδικασία εγγραφής όπως φαίνεται και στις κινήσεις της. Στη συνέχεια έκανε επιλογή λογαριασμού (…) και κινητού τηλεφώνου (Χ). Αμέσως μετά κάνει αποδοχή των όρων και εισάγει το sms-otp (κωδικός επαλήθευσης που εστάλη στο κινητό Χ).

Στις 08/07/2019 η καταγγέλλουσα αλλάζει τον αριθμό τηλεφώνου που είχε συνδέσει στην υπηρεσία i-bank pay και βάζει τον αριθμό κινητού Ψ, χωρίς όμως την εισαγωγή κωδικού επιβεβαίωσης (sms otp). Η ενέργειά της αυτή παραμένει σε κατάσταση «εκκρεμότητας» (pending).

Στη συνέχεια βάζει τον αριθμό κινητού Χ και στη συνέχεια κάνει επαλήθευσή του βάζοντας το otp που στέλνει η τράπεζα.

Στη συνέχεια, στις 24/06/2020 συνδέθηκε στην εφαρμογή mobile και έγινε αυτόματα η εγγραφή της και από εκεί καθώς έγινε αυτόματα η κλήση για το device registration στο mobile.

Στο αρχείο καταγραφής η κατάσταση του κινητού Ψ φαίνεται “εκκρεμής» (status =pending) ενώ του Χ είναι ενεργή (status=active).

Στη συνέχεια. με την με αρ. πρωτ. Γ/ΕΙΣ/980/8-2-2024 συμπληρωματική γνωστοποίηση, ο υπεύθυνος επεξεργασίας συμπλήρωσε την ανάλυση του περιστατικού με τα παρακάτω στοιχεία:

- Χρόνος έναρξης του περιστατικού (έτος/μήνας/μέρα/ώρα):

  Ημερομηνία αναβάθμισης εφαρμογής Mobile Banking 24.06.2020

- Χρόνος λήξης του περιστατικού (έτος/μήνας/μέρα/ώρα)

  Ημερομηνία οριστικής διακοπής λειτουργίας της εφαρμογής ibank Pay (01.11.2023)

- Χρόνος που λάβατε γνώση του περιστατικού (έτος/μήνας/μέρα/ώρα)

  Στις 30/10/2023 επιβεβαιώθηκε το πρώτο περιστατικό και εκκινήθηκε η διαδικασία έρευνας για τον εντοπισμό και τυχόν άλλων συναφών περιστατικών.

- Τρόπος με τον οποίο λάβατε γνώση του περιστατικού

  Το περιστατικό διαπιστώθηκε κατόπιν έρευνας της Διεύθυνσης Ψηφιακού Μετασχηματισμού της Τράπεζας, στο πλαίσιο εκ νέου διερεύνησης καταγγελίας ενόψει του διοικητικού ελέγχου της Αρχής Σας.

- Φύση του περιστατικού:

  Κατά την ενσωμάτωση της υπηρεσίας IRIS Pay στην εφαρμογή Mobile Banking της Τράπεζας, ενεργοποιήθηκαν εκ παραδρομής στην εφαρμογή i-bank Pay της Τράπεζας κινητά τηλέφωνα τα οποία είχαν καταχωρηθεί από πελάτες, και για τα οποία δεν είχε ολοκληρωθεί εκ μέρους τους η επιβεβαίωσή τους μέσω καταχώρησης κωδικού μίας χρήσης (OTP).

- Αιτία/ες του περιστατικού:

  Μεμονωμένο Σφάλμα λογισμικού

- Πλήθος αρχείων (κατά προσέγγιση) που αφορά το περιστατικό:

  Ένα (1) αρχείο (πίνακας στη βάση δεδομένων i-bank Pay/mobile banking)

- Πλήθος προσώπων (κατά προσέγγιση) που αφορά το περιστατικό:

  Πέραν του περιστατικού για το οποίο σας είχαμε ενημερώσει με την από 02.11.2023 αρχική γνωστοποίησή μας, επιβεβαιώθηκε κατόπιν διερεύνησης ότι υπάρχουν επιπλέον 24 περιπτώσεις πελατών, για τους οποίους είχε ενεργοποιηθεί εκ παραδρομής στην εφαρμογή i-bank pay τηλέφωνο για το οποίο δεν είχε ολοκληρωθεί εκ μέρους τους η επαλήθευσή του μέσω καταχώρησης κωδικού μίας χρήσης (OTP).

- Φύση των πιθανών συνεπειών που θα έχουν τα πρόσωπα που επηρεάζονται από το περιστατικό:

Εκ παραδρομής μη εγκεκριμένη (χωρίς ΟΤΡ) ενεργοποίηση κινητών τηλεφώνων που είχαν καταχωρήσει οι ίδιοι οι πελάτες στην εφαρμογή i-bank Pay και που θα μπορούσε ενδεχομένως να οδηγήσει σε οικονομική απώλεια και αδικαιολόγητο πλουτισμό. Στο πλαίσιο αυτό, βάσει της σχετικής μας διερεύνησης, διαπιστώθηκε ότι πραγματοποιήθηκαν 38 εσφαλμένες εγχρήματες συναλλαγές που έγιναν από 33 πελάτες συνολικού ποσού 2.149,66 ευρώ.

- Ενημερώσατε τα πρόσωπα που επηρεάστηκαν από το περιστατικό; (ΝΑΙ/ΟΧΙ/ΟΧΙ ΑΚΟΜΗ, ΑΛΛΑ ΘΑ ΕΝΗΜΕΡΩΘΟΥΝ / ΔΕΝ ΑΠΟΦΑΣΙΣΤΗΚΕ ΑΚΟΜΗ ΑΝ ΠΡΕΠΕΙ ΝΑ ΕΝΗΜΕΡΩΘΟΎΝ)

  Η πελάτισσα που σχετίζεται με το πρώτο επιβεβαιωμένο περιστατικό για το οποίο σας είχαμε κάνει αρχική γνωστοποίηση στις 02.11.2023 έχει ήδη λάβει συμπληρωματική ενημέρωση από την Τράπεζα σε σχέση με την υπόθεσή της. Επιπλέον, η Τράπεζα θα προβεί σε οικονομική αποζημίωση των πελατών που επηρεάστηκαν από το ζήτημα, και θα τους ενημερώσει σχετικά.
- Ημερομηνία κατά την οποία ενημερώσατε τα πρόσωπα (έτος/μήνας/μέρα): *07.11.2023 (ενημέρωση των πελατών που σχετίζονται με το πρώτο επιβεβαιωμένο περιστατικό)*
- Ημερομηνία στην οποία θα ενημερώσετε τα πρόσωπα (έτος/μήνας/μέρα ή ΑΠΡΟΣΔΙΟΡΙΣΤΟ, αν δεν έχει προσδιοριστεί):

  Σταδιακή ενημέρωση, η οποία πρόκειται να ολοκληρωθεί εντός του Φεβρουαρίου 2024.

  Επισυνάπτονται τα σχετικά μηνύματα που εστάλησαν.
- Περιγραφή των μέτρων που λήφθηκαν για την αντιμετώπιση της παραβίασης:

Α. Η άμεση αναστολή της εφαρμογής i-bank Pay

Β. Ο έλεγχος ύπαρξης τυχόν αντίστοιχων ζητημάτων επί του συνόλου των χρηστών της εφαρμογής (σύνολο χρηστών i-bank pay: περίπου 76.000)

Γ. Ο έλεγχος τυχόν κοινοποίησης στοιχείων χρηστών της εφαρμογής εκ των ζητημάτων που ενδεχομένως ανακύψουν εκ της ενέργειας Β.

Δ. Ο σχεδιασμός και η υλοποίηση επιπλέον διορθωτικών μέτρων, εφόσον απαιτηθεί, όπως η επαναφορά των στοιχείων στην προτέρα κατάσταση, η θέσπιση επιπλέον δικλείδων ασφαλείας κλπ.

Ε. Επιβεβαίωση μέσω εμφάνισης splash banner στην εφαρμογή Mobile Banking του κινητού τηλεφώνου που είναι δηλωμένο στην υπηρεσία IRIS Pay

ΣΤ. Η διόρθωση της mobile εφαρμογής ώστε όταν ο χρήστης αιτείται την ενεργοποίηση σύνδεσης τηλεφώνου που βρίσκεται σε εκκρεμότητα να γίνεται μόνο με κωδικό επαλήθευσης και μόνο σε εύλογο χρονικό διάστημα από τη στιγμή της δημιουργίας της εκκρεμότητας και σε καμία περίπτωση να μην εκτελείται αυτόματη ενεργοποίηση τηλεφώνου.

Ζ. Η οικονομική αποκατάσταση των προσώπων που επηρεάστηκαν από το περιστατικό.

Σε συνέχεια των ανωτέρω, η Αρχή με τις Γ/ΕΞΕ/532/12-02-2024, Γ/ΕΞΕ/526/12-02-2024 και Γ/ΕΞΕ/531/12-02-2024 κλήσεις της, αντίστοιχα, κάλεσε τους καταγγέλλοντες Α και Β και την καταγγελλόμενη σε ακρόαση ενώπιον της Ολομέλειας της Αρχής στις 20/2/2024, προκειμένου να εκθέσουν τις απόψεις τους για την υπόθεση. Κατά τη συνεδρίαση της 20/2/2024 η συζήτηση της υπόθεσης αναβλήθηκε, κατόπιν αιτήματος της καταγγέλλουσας, για την 12/3/2024. Κατά τη συνεδρίαση της 12/3/2024 παρέστησαν οι καταγγέλλοντες Α και Β, με την πληρεξούσια δικηγόρο τους Μαγδαλένα Εύα Παβλικόβσκα (Α.Μ. ΔΣΑ …), και εκ μέρους της Εθνικής Τράπεζας οι Ε, Βοηθός Γενικός Διευθυντής Καινοτομίας και Ψηφιακών Συνεργασιών, η Ζ, Επικεφαλής Τομέα Τήρησης Κανονισμών και Διασφάλισης Ποιότητας, η Η, Επικεφαλής Τομέα Συμπεριφοράς πελατών, η Δ, και ο Λ, Διευθυντές Συμμόρφωσης Επιχειρηματικής Ρύθμισης και Συμπεριφοράς πελατών της Τράπεζας και του Ομίλου, η ΣΤ Υπεύθυνη Προστασίας Δεδομένων της Εθνικής Τράπεζας και η Ι, Αναπληρώτρια Υπεύθυνη Προστασίας Δεδομένων. Κατά τη συνεδρίαση χορηγήθηκε προθεσμία για την υποβολή υπομνήματος και τα μέρη υπέβαλαν εμπρόθεσμα, η Β το Γ/ΕΙΣ/2993/01-04-2024 υπόμνημα, η Εθνική Τράπεζα το Γ/ΕΙΣ/2994/01-04-2024 υπόμνημα, ενώ ο Α, με το Γ/ΕΙΣ/2963/29-03-2024 έγγραφό του δήλωσε ότι ανακαλεί την υπ' αρ. πρωτ. Γ/ΕΙΣ/9060/24-07-2022 καταγγελία του, λόγω παροχής ικανοποιητικών

διευκρινίσεων από την καταγγελλόμενη Τράπεζα, κατά τη διάρκεια της συνεδρίασης της Ολομέλειας της Αρχής που έλαβε χώρα στις 12/03/2024.

Τόσο κατά τη συνεδρίαση όσο και με το υπόμνημά της, η καταγγέλλουσα Β επανέλαβε τα αναφερόμενα στην καταγγελία της, τονίζοντας ότι χρειάστηκαν πολλές επικοινωνίες αλλά και η υποβολή της καταγγελίας στην Αρχή προκειμένου να ασχοληθεί η Τράπεζα με το ζήτημα και υποστηρίζοντας ότι μέχρι το σημείο εκείνο δεν είχε δοθεί καμία πειστική απάντηση από την Τράπεζα σε σχέση με το περιστατικό. Η καταγγέλλουσα επεσήμανε ιδιαίτερα την καθυστέρηση στην ικανοποίηση του δικαιώματος πρόσβασής της, το οποίο ασκήθηκε στις 29/3/2022 και τελικά, κατόπιν της από 29/4/2022 ενημέρωσης ότι θα γίνει χρήση της παράτασης κατά δύο μήνες «λόγω δυσμενούς τρέχουσας συγκυρίας», η οποία ουδέποτε εξηγήθηκε, τελικά ικανοποιήθηκε εκπρόθεσμα στις 7/11/2023, και κατά την άποψή της, όχι επαρκώς, αφού στην απάντηση της Τράπεζας αναφέρεται ότι «εκ παραδρομής το κινητό του Α ενεργοποιήθηκε στο προφίλ της», δεν της χορηγήθηκαν όμως τα προσωπικά της δεδομένα, τα οποία η Τράπεζα επεξεργάστηκε αναφορικά με το περιστατικό. Τέλος, η καταγγέλλουσα αναφέρει ότι έλαβε απαντήσεις «*διά τηλεφώνου και ηλεκτρονικής αλληλογραφίας οι οποίες βασίζονταν ενδεχομένως σε συσχέτιση δεδομένων λόγω διαπροσωπικής σχέσης*».

Η Εθνική Τράπεζα, τόσο διά των εκπροσώπων της κατά την ακρόαση όσο και με το υπόμνημά της, ανέφερε τα εξής: Πράγματι στα τέλη Μαρτίου 2022 δέχθηκε ένα παράπονο για ένα ζήτημα που αφορούσε την εφαρμογή ibank Pay, η οποία λειτουργούσε από το έτος 2016 χωρίς προβλήματα. Ειδικότερα, οι καταγγέλλοντες ανέφεραν στην Τράπεζα ότι στις 26/3/2022 πραγματοποιήθηκε μεταφορά χρημάτων από τον λογαριασμό του χρήστη της εφαρμογής Γ προς το κινητό τηλέφωνο Ψ, το οποίο τη δεδομένη χρονική στιγμή ήταν συνδεδεμένο με τον λογαριασμό της καταγγέλλουσας Β, ενώ, σύμφωνα με τους πελάτες, τα χρήματα έπρεπε να πιστωθούν σε λογαριασμό διαφορετικού πελάτη, του καταγγέλλοντος Α, και ζήτησαν τη διερεύνηση του περιστατικού. Περαιτέρω στις 29/3/2022 οι πελάτες υπέβαλαν από κοινού αίτημα για άσκηση δικαιώματος πρόσβασης στα προσωπικά τους δεδομένα. Σύμφωνα με την Τράπεζα, το γραφείο DPO έλαβε το αίτημα και δρομολόγησε τις απαιτούμενες ενέργειες για τη διερεύνηση του ζητήματος, ελέγχοντας αρχικά εάν είχαν παρατηρηθεί δυσλειτουργίες όσον αφορά τη χρήση της

εφαρμογής. Δεδομένης της πολυπλοκότητας της υπόθεσης, απεστάλη στις 29/4/2022 επιστολή στην καταγγέλλουσα Β, μέσω της οποίας η Τράπεζα την ενημέρωνε ότι οι απαιτούμενες ενέργειες βρίσκονταν σε εξέλιξη και το αίτημά της θα ικανοποιούνταν εντός τριών μηνών από την υποβολή του. Δεδομένου ότι η εγγραφή στην εφαρμογή απαιτούσε την καταχώρηση του αριθμού κινητού τηλεφώνου από τον ίδιο τον χρήστη, η Τράπεζα θεώρησε ότι είχε πραγματοποιηθεί κανονικά εγγραφή της καταγγέλλουσας με ΟΤΡ και διερεύνησε το πρόβλημα στα επόμενα στάδια, μετά την εγγραφή, εστιάζοντας στον Α. Σε τηλεφωνική επικοινωνία που είχε ο καταγγέλλων στις 19/6/2022 με την Τράπεζα προκειμένου να την ενημερώσει για δεύτερο περιστατικό, κατά το οποίο χρήματα από διαφορετικό αποστολέα που προορίζονταν για τον ίδιο είχαν καταλήξει ξανά στον λογαριασμό της Β, η εκπρόσωπος της Τράπεζας παρείχε πληροφορίες σχετικά με τον τρόπο εγγραφής στην υπηρεσία IRIS pay, είτε μέσω της εφαρμογής i-bank Pay είτε μέσω του Mobile Banking και για τα δεδομένα που απαιτούνταν για την εγγραφή, πρότεινε στους καταγγέλλοντες να υποβάλουν εκ νέου φόρμα επικοινωνίας προς την Τράπεζα με λεπτομέρειες για τη δεύτερη συναλλαγή και συμφωνήθηκε ότι ο Α θα θεωρείται ο πρώτος και κύριος εμπλεκόμενος στην υπόθεση, αφού ήταν αυτός που θα μπορούσε να υποστεί οικονομική ζημία από το πρόβλημα. Από την εν λόγω αρχική διερεύνηση προέκυψε ότι δεν είχε παρατηρηθεί κάποια δυσλειτουργία στην εφαρμογή και ότι το τηλέφωνο Ψ είχε δηλωθεί από την καταγγέλλουσα Β ως δεύτερο τηλέφωνο βάσει του οποίου μπορούσε να εντοπιστεί από φίλους προκειμένου να λάβει χρήματα, ενώ στα στοιχεία που τηρεί η Τράπεζα για τον Α δεν υπήρχε καταχωρημένο κινητό τηλέφωνο αλλά μόνο σταθερό. Στη συνέχεια, στις 13/9/2022 η Τράπεζα έστειλε στον Α ενημέρωση μέσω e-mail με συγκεκριμένες οδηγίες προς επίλυση του ζητήματος (απεγγραφή και εκ νέου εγγραφή), με την επισήμανση να επανέλθει σε περίπτωση μη επίλυσης και δεδομένου ότι ο πελάτης δεν επανήλθε, η Τράπεζα θεώρησε ότι το πρόβλημα αποκαταστάθηκε. Στη συνέχεια, μετά το από 15/11/2022 έγγραφο της Αρχής, με το οποίο γνωστοποιήθηκαν στην Τράπεζα οι υπό κρίση καταγγελίες, η Τράπεζα διερεύνησε και πάλι το ζήτημα, επικοινώνησε ξανά με τον Α και αφού έλαβαν χώρα οι απαραίτητες συστημικές ενέργειες προκειμένου να απενεργοποιηθεί το δεύτερο τηλέφωνο στην εφαρμογή, καθώς και δοκιμαστική πληρωμή προκειμένου να επιβεβαιωθεί ότι το ζήτημα αποκαταστάθηκε πλήρως, η

Τράπεζα επικοινώνησε με την Β στις 16/12/2022 και απέστειλε την ίδια μέρα απάντηση προς την Αρχή. Σταθμίζοντας δε τα αποτελέσματα της διαδικασίας, κρίθηκε ότι δεν συνέτρεχαν οι προϋποθέσεις γνωστοποίησης περιστατικού παραβίασης ή καταγραφής περιστατικού σύμφωνα με τον ΓΚΠΔ, καθώς, αφ'ενός αφορούσε σε μεμονωμένο περιστατικό και αφ' ετέρου δεν προκλήθηκε κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Στη συνέχεια και με αφορμή τον διοικητικό έλεγχο της Αρχής σύμφωνα με το από 16/10/2023 έγγραφο, η Τράπεζα αναφέρει ότι προχώρησε σε ενδελεχή και πιο εκτεταμένο έλεγχο όλων των διαδικασιών, χωρίς να θεωρεί κανένα στάδιο ως δεδομένο και έτσι εντόπισε το πρόβλημα: Η εφαρμογή i-bank Pay ήταν διαθέσιμη μέχρι το έτος 2018 μόνο για τους πελάτες της Εθνικής. Το 2018 ξεκίνησε να λειτουργεί το σύστημα IRIS της ΔΙΑΣ και το 2020 το ibank εντάχθηκε στο IRIS. Ειδικότερα διαπιστώθηκε ότι λόγω μεμονωμένου σφάλματος λογισμικού στο πλαίσιο της ενσωμάτωσης της υπηρεσίας IRIS pay στο Mobile Banking τον Ιούνιο του 2020, το δεύτερο τηλέφωνο που είχε καταχωρήσει η Β στην εφαρμογή ενεργοποιήθηκε εκ παραδρομής στο λογαριασμό της στο i-bank Pay, χωρίς να έχει ολοκληρωθεί εκ μέρους της η επιβεβαίωση μέσω κωδικού μιας χρήσης (ΟΤΡ). Η Τράπεζα γνωστοποίησε το περιστατικό ως παραβίαση προσωπικών δεδομένων στις 2/11/2023, απέστειλε συμπληρωματική ενημέρωση στους καταγγέλλοντες (Συνημμένα 7 και 8 στο υπόμνημά της) και προχώρησε σε περαιτέρω έρευνα του ζητήματος προκειμένου να εντοπίσει τυχόν αντίστοιχα περιστατικά επί του συνόλου των χρηστών της εφαρμογής, καταλήγοντας στο συμπέρασμα ότι όσοι αριθμοί τηλεφώνου ήταν σε εκκρεμή κατάσταση (pending) χωρίς δηλαδή να έχουν επιβεβαιωθεί με ΟΤΡ, ενεργοποιήθηκαν στους αντίστοιχους λογαριασμούς. Η Τράπεζα διευκρίνισε ότι το σφάλμα αφορούσε μόνο την εφαρμογή ibank Pay, και όχι το σύστημα IRIS συνολικά, επομένως επηρέαζε μόνο τις πληρωμές από κατόχους λογαριασμών της Εθνικής Τράπεζας. Εν προκειμένω, η καταγγέλλουσα Β, ενώ είχε πραγματοποιήσει κανονικά εγγραφή τον Απρίλιο του 2019 με τον δικό της αριθμό τηλεφώνου, τον Ιούλιο 2019 (8/7/2019) προσπάθησε να κάνει μια αλλαγή τηλεφώνου με τον αριθμό του Α, χωρίς η αλλαγή να ολοκληρωθεί με ΟΤΡ και έτσι η εγγραφή του νέου αριθμού έμεινε ως εκκρεμής και παρέμεινε ενεργός ο πραγματικός αριθμός της Β. Ωστόσο, κατά την ενσωμάτωση της εφαρμογής στο IRIS το 2020 ο δεύτερος αριθμός ενεργοποιήθηκε και συνδέθηκε με τον τραπεζικό λογαριασμό της

Β. Η Τράπεζα διευκρίνισε ότι ο Α δεν διέθετε λογαριασμό στην Εθνική Τράπεζα κι έτσι ο αριθμός του δεν ήταν καταχωρημένος στα συστήματά της. Σύμφωνα με τους ισχυρισμούς της Τράπεζας, επρόκειτο για ένα εντελώς απροσδόκητο “bug” στο σύστημα, το οποίο ήταν πολύ δύσκολο να βρεθεί, ενώ η αρχική διερεύνηση από τους τεχνικούς της οδήγησε στην αρχική εσφαλμένη απάντηση προς τους καταγγέλλοντες. Από τον ενδελεχή έλεγχο αντίστοιχων ζητημάτων επί του συνόλου των χρηστών της εφαρμογής (76.000) προέκυψε ότι η εκ παραδρομής ενεργοποίηση τηλεφώνου είχε πραγματοποιηθεί σε άλλους 24 πελάτες και διαπιστώθηκε ότι είχαν πραγματοποιηθεί 38 εσφαλμένες συναλλαγές συνολικού ύψους 2.149,66 ευρώ. Αναφορικά με την καθυστέρηση στην ικανοποίηση του δικαιώματος πρόσβασης, η Τράπεζα επανέλαβε ότι επρόκειτο για ένα πρόβλημα πολύ δύσκολο να εντοπιστεί αφού δεν βρισκόταν στο σημείο που το έψαχνε, αλλά οφειλόταν σε μια εσφαλμένη παραμετροποίηση κατά την αναβάθμιση της εφαρμογής, τονίζοντας ότι στις προθέσεις της Τράπεζας ήταν να ενημερώσει εγκαίρως τους καταγγέλλοντες, όμως το ζήτημα βρισκόταν υπό διερεύνηση όλο το διάστημα μέχρι τον Νοέμβριο του 2023 και σε κάθε περίπτωση φρόντιζε να τους κρατά ενήμερους μέχρι την ολοκλήρωση της διερεύνησης. Τέλος, με το υπόμνημά της, η Τράπεζα αναφέρει ότι, αφού έθεσε σε αναστολή την εφαρμογή i-bank Pay από τις 2-11-2023 και απέστειλε συμπληρωματικές απαντήσεις προς τους καταγγέλλοντες στις 7-11-2023, έχει προβεί στον σχεδιασμό και την υλοποίηση επιπλέον διορθωτικών μέτρων, όπως η διενέργεια ελέγχου ώστε να μην συνδέονται τηλέφωνα που το αίτημα σύνδεσής τους βρίσκεται σε εκκρεμότητα για μεγάλο χρονικό διάστημα, και η περιοδική, τακτική διαγραφή των εκκρεμών τηλεφώνων σε λογαριασμούς, καθώς και στις ακόλουθες ενέργειες:

- Επιβεβαίωση μέσω εμφάνισης splash banner στην εφαρμογή Mobile Bankingου του κινητού τηλεφώνου που είναι δηλωμένο στην υπηρεσία IRIS Pay
- Διόρθωση της mobile εφαρμογής ώστε όταν ο χρήστης αιτείται την ενεργοποίηση σύνδεσης τηλεφώνου που βρίσκεται σε εκκρεμότητα να γίνεται μόνο με κωδικό επαλήθευσης και μόνο σε εύλογο χρονικό διάστημα από τη στιγμή της εκκρεμότητας και σε καμία περίπτωση να μην εκτελείται αυτόματη ενεργοποίηση τηλεφώνου

- Επικοινωνία με πελάτες στους οποίους εντοπίστηκε ότι είχαν ενεργοποιηθεί εκ παραδρομής συνδέσεις κινητών τηλεφώνων με τους λογαριασμούς τους και οικονομική αποκατάσταση των προσώπων που επηρεάστηκαν από το περιστατικό.

Η Αρχή, μετά από εξέταση των στοιχείων του φακέλου και αφού άκουσε τον εισηγητή και τις διευκρινίσεις από τη βοηθό εισηγητή, μετά από διεξοδική συζήτηση

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ 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 των καταγγελιών της Β και του Α κατά της Εθνικής Τράπεζας της Ελλάδος Α.Ε. 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 το άρθρο 15 παρ. 1 και 3 ΓΚΠΔ «*1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες: […] 3. Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. […] Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα και εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή που χρησιμοποιείται συνήθως.».* Επιπλέον, σύμφωνα με το άρθρο 12 ΓΚΠΔ «*1. Ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων* […] *κάθε ανακοίνωση στο πλαίσιο των άρθρων 15* […] *2. Ο υπεύθυνος επεξεργασίας διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων που προβλέπονται στα άρθρα 15* […] *3. Ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων πληροφορίες για την ενέργεια που πραγματοποιείται κατόπιν αιτήματος δυνάμει των άρθρων 15 έως 22 χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος. Η εν λόγω προθεσμία*

μπορεί να παραταθεί κατά δύο ακόμη μήνες, εφόσον απαιτείται, λαμβανομένων υπόψη της πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων. Ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων για την εν λόγω παράταση εντός μηνός από την παραλαβή του αιτήματος, καθώς και για τους λόγους της καθυστέρησης. […] *4. Εάν ο υπεύθυνος επεξεργασίας δεν ενεργήσει επί του αιτήματος του υποκειμένου των δεδομένων, ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων, χωρίς καθυστέρηση και το αργότερο εντός μηνός από την παραλαβή του αιτήματος, για τους λόγους, για τους οποίους δεν ενήργησε και για τη δυνατότητα υποβολής καταγγελίας σε εποπτική αρχή και άσκησης δικαστικής προσφυγής*». Από τις ανωτέρω διατάξεις προκύπτει ότι καθιερώνεται το δικαίωμα πρόσβασης του υποκειμένου στα προσωπικά δεδομένα που το αφορούν με κύριο σκοπό να βεβαιώνεται το υποκείμενο για την ακρίβεια και τον σύννομο χαρακτήρα της επεξεργασίας των δεδομένων του. Ως εκ τούτου, για την ικανοποίηση του δικαιώματος πρόσβασης δεν απαιτείται η επίκληση εννόμου συμφέροντος, αφού αυτό ενυπάρχει και αποτελεί βάση του δικαιώματος πρόσβασης του υποκειμένου να λάβει γνώση πληροφοριών που το αφορούν και οι οποίες έχουν καταχωρηθεί σε αρχείο που τηρεί ο υπεύθυνος επεξεργασίας, έτσι ώστε να πραγματώνεται η βασική αρχή του δικαίου για την προστασία των προσωπικών δεδομένων, που συνίσταται στη διαφάνεια της επεξεργασίας ως προϋπόθεση κάθε περαιτέρω ελέγχου της νομιμότητάς της εκ μέρους του υποκειμένου των δεδομένων[1].

4. 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*

[1] Βλ. ενδεικτικά ΑΠΔ 2/2020, 23/2020, 16/2017, 98/2014, 149/2014, 72/2013 και 71/2013, ομοίως.

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) 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».

5. Σύμφωνα με τη διάταξη του άρθρου 25 παρ. 1, παρ. 2 του ΓΚΠΔ (Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού): «*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 από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. 2. Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα*

τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων».

6. Σύμφωνα με το άρθρο 4 παρ. 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 (πλέον ΕΣΠΔ) 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. Μπορεί επίσης να περιλαμβάνει οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα γι' αυτά τα πρόσωπα (βλ. και αιτ. σκέψεις 85 και 75*)» (Κεφάλαιο Ι.Β.3). Όπως δε επισημαίνεται στις Κατευθυντήριες Γραμμές 9/2022 του ΕΣΠΔ για τη γνωστοποίηση περιστατικών παραβίασης προσωπικών δεδομένων

σύμφωνα με τον ΓΚΠΔ[2], «*τα περιστατικά ασφαλείας δεν περιορίζονται στις περιπτώσεις (μοντέλα απειλής) όπου πραγματοποιείται επίθεση προερχόμενη από εξωτερική πηγή σε έναν οργανισμό, αλλά περιλαμβάνουν περιστατικά που προκύπτουν από εσωτερικές διαδικασίες που παραβιάζουν τις αρχές της ασφάλειας της επεξεργασίας*» (σελ. 8, υποσημ. 16).

7. 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, στο οποίο ορίζεται ότι «*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*». Όσον αφορά το χρόνο λήψης γνώσης του περιστατικού από τον Υπεύθυνο Επεξεργασίας, στις ως άνω ΚΓ της ΟΕ29 (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*

[2] "Guidelines 9/2022 on personal data breach notification under GDPR", version 2.0, adopted 28.3.2023, διαθέσιμες (στην αγγλική) στη διεύθυνση https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_el

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». 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)*». 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 τα εκεί αναφερόμενα στοιχεία, ώστε να είναι σε θέση να συμπεριλάβει τις σχετικές πληροφορίες 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,[3] 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 (βλ. και Απόφαση 35/2023 ΑΠΔ).

8. Στην προκειμένη περίπτωση, από την εξέταση του συνόλου των στοιχείων του φακέλου και κατόπιν της ακροαματικής διαδικασίας προέκυψαν τα εξής:

Στις 14/4/2019, η καταγγέλλουσα, η οποία διατηρούσε λογαριασμό στην Εθνική Τράπεζα, πραγματοποίησε εγγραφή στην εφαρμογή i-bank Pay, συνδέοντας τον τραπεζικό λογαριασμό της με τον αριθμό του κινητού της τηλεφώνου (Χ),

[3] Βλ. και τις προαναφερόμενες Κατευθυντήριες Γραμμές 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,[…]".*

προκειμένου να δέχεται πληρωμές από τρίτους με χρήση του αριθμού αυτού. Στις 8/7/2019 η καταγγέλλουσα, πιθανόν εκ παραδρομής, επιχείρησε να αλλάξει τον δηλωθέντα αριθμό τηλεφώνου στην εφαρμογή, συμπληρώνοντας τον αριθμό του Α (Ψ), χωρίς όμως αυτή η αλλαγή να ολοκληρωθεί με τη διαδικασία επιβεβαίωσης μέσω αποστολής κωδικού μιας χρήσης (one time password – OTP). Έτσι η εγγραφή του νέου αριθμού έμεινε σε κατάσταση εκκρεμότητας (pending) ενώ ο πραγματικός αριθμός της καταγγέλλουσας (Χ) παρέμεινε ενεργός στην εφαρμογή και συνδεδεμένος με τον τραπεζικό λογαριασμό της. Ωστόσο, κατά την ενσωμάτωση της εφαρμογής i-bank Pay στην υπηρεσία IRIS Online Payments του διατραπεζικού συστήματος ΔΙΑΣ, στην οποία προχώρησε η Εθνική Τράπεζα το έτος 2020, ο δεύτερος αριθμός (Ψ), ο οποίος βρισκόταν σε κατάσταση εκκρεμότητας, ενεργοποιήθηκε και συνδέθηκε με τον τραπεζικό λογαριασμό της καταγγέλλουσας. Το ζήτημα οφείλεται σε εσφαλμένη παραμετροποίηση από πλευράς της τράπεζας κατά την αναβάθμιση της εφαρμογής mobile banking, την οποία η Τράπεζα αποδίδει σε μεμονωμένη ανθρώπινη αστοχία. Παρότι, όπως διαπιστώθηκε, ο Α διέθετε λογαριασμό στην Εθνική Τράπεζα, στην καρτέλα πελάτη του περιλαμβανόταν μόνο αριθμός σταθερού τηλεφώνου, ενώ ο αριθμός του κινητού του τηλεφώνου δεν ήταν καταχωρημένος στα συστήματα της Τράπεζας. Ο Α χρησιμοποιούσε το σύστημα πληρωμών IRIS Online Payments μέσω λογαριασμού που διέθετε σε άλλη τράπεζα, ο οποίος και είναι συνδεδεμένος με τον αριθμό κινητού τηλεφώνου του (Ψ). Η εσφαλμένη ενεργοποίηση του αριθμού αυτού στο προφίλ της Β και η σύνδεσή του με τον δικό της τραπεζικό λογαριασμό είχε ως αποτέλεσμα, σε προσπάθεια του τρίτου Γ να μεταφέρει στον Α το ποσό των 90€ μέσω της εφαρμογής i-bank Pay την 26/3/2022, η μεταφορά να γίνει προς τον λογαριασμό της Β. Περαιτέρω, διαπιστώθηκε ότι παρά την άμεση ενημέρωση της Τράπεζας από τους καταγγέλλοντες για το ζήτημα και την άσκηση δικαιώματος πρόσβασης εκ μέρους τους (στις 29/3/2022), η Τράπεζα αρκέστηκε στη σύσταση προς τον Α να απεγκαταστήσει και να εγκαταστήσει ξανά την εφαρμογή, ενώ προχώρησε σε διερεύνηση της υπόθεσης μόνο αφού της κοινοποιήθηκαν οι καταγγελίες που είχαν υποβληθεί στην Αρχή. Ωστόσο η αρχική αυτή διερεύνηση δεν κατέδειξε την ουσία του ζητήματος και οδήγησε στην παροχή εσφαλμένης πληροφόρησης προς τους καταγγέλλοντες, ότι δηλαδή ο αριθμός του Α είχε ενεργοποιηθεί από την Β με χρήση κωδικού μιας χρήσης (OTP). Μετά από

αρκετούς μήνες και με αφορμή τον επιτόπιο έλεγχο της Αρχής στην Τράπεζα (τέλος Οκτωβρίου 2023), η τελευταία προχώρησε σε περαιτέρω διερεύνηση του ζητήματος, η οποία είχε ως αποτέλεσμα τη διαπίστωση του προβλήματος. Έτσι, τον Νοέμβριο του 2023 η Τράπεζα προχώρησε σε αναστολή της εφαρμογής i-bank Pay, υποβολή γνωστοποίησης περιστατικού παραβίασης στην Αρχή, εκ νέου ενημέρωση των καταγγελλόντων και σε ενδελεχή έλεγχο αντίστοιχων ζητημάτων επί του συνόλου των χρηστών της εφαρμογής (76.000), από τον οποίο προέκυψε ότι η εκ παραδρομής ενεργοποίηση τηλεφώνου είχε πραγματοποιηθεί σε άλλους 24 πελάτες της, ενώ είχαν πραγματοποιηθεί 38 εσφαλμένες συναλλαγές συνολικού ύψους 2.149,66 ευρώ. Η Τράπεζα ανέφερε ότι επικοινώνησε με τους εν λόγω πελάτες και αποκατέστησε οικονομικά τα πρόσωπα που επηρεάστηκαν από το περιστατικό. Επιπλέον η Τράπεζα ανέφερε ότι έλαβε περαιτέρω διορθωτικά μέτρα προς αποφυγή παρόμοιων περιστατικών στο μέλλον, όπως η διενέργεια τακτικών ελέγχων, η περιοδική, τακτική διαγραφή των εκκρεμών τηλεφώνων σε λογαριασμούς, η λήψη μέτρων ώστε η ενεργοποίηση σύνδεσης τηλεφώνου να γίνεται μόνο με κωδικό επαλήθευσης και μόνο σε εύλογο χρονικό διάστημα από τη στιγμή της εκκρεμότητας και σε καμία περίπτωση να μην εκτελείται αυτόματη ενεργοποίηση τηλεφώνου και το κινητό τηλέφωνο που είναι δηλωμένο στην υπηρεσία IRIS Pay να επιβεβαιώνεται μέσω εμφάνισης splash banner στην εφαρμογή Mobile Banking.

9.Με βάση τα ανωτέρω δεδομένα, η Αρχή κρίνει ότι από τις ενέργειες και παραλείψεις της Εθνικής Τράπεζας, ως υπεύθυνου επεξεργασίας, στοιχειοθετείται:

i. Παραβίαση των βασικών αρχών της ακρίβειας, ακεραιότητας και εμπιστευτικότητας των δεδομένων (άρθρου 5, παρ. 1 εδ. δ΄ και στ΄ ΓΚΠΔ) σε συνδυασμό με ελλείψεις κατάλληλων μέτρων ασφάλειας (άρθρο 32 του ΓΚΠΔ), όπως μη επαρκής διαδικασία διαχείρισης αλλαγών και ελλιπής έλεγχος λειτουργικότητας και ποιότητας του λογισμικού, με αποτέλεσμα να μην εντοπιστούν τα σφάλματα πριν αυτό μπει σε παραγωγική λειτουργία και συνεπώς, όπως προεκτέθηκε, την συστημική εσφαλμένη σύνδεση κινητών τηλεφώνων των υποκειμένων των δεδομένων με τραπεζικούς λογαριασμούς τρίτων, την τήρηση ανακριβών προσωπικών δεδομένων και τελικά την αποκάλυψη σε τρίτους πληροφοριών που αφορούν τραπεζικές συναλλαγές των υποκειμένων των δεδομένων.

ii. Παραβίαση του άρθρου 25 του ΓΚΠΔ για την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, αφού, όπως προέκυψε, η ανωτέρω παραβίαση προέκυψε λόγω εσφαλμένου σχεδιασμού (παραμετροποίησης) της διαδικασίας ενσωμάτωσης της εφαρμογής i-bank Pay στην υπηρεσία IRIS Online Payments του διατραπεζικού συστήματος ΔΙΑΣ, στην οποία προχώρησε η Εθνική Τράπεζα το έτος 2020, με αποτέλεσμα να μην απαιτείται η επιβεβαίωση των εκκρεμών αριθμών με κωδικό μιας χρήσης (OTP) προκειμένου να ενεργοποιηθούν και να συνδεθούν με τους τραπεζικούς λογαριασμούς όσων χρηστών είχαν τέτοιους αριθμούς σε εκκρεμότητα.

iii. Παραβίαση των άρθρων 33 και 34 ΓΚΠΔ στο πλαίσιο χειρισμού του περιστατικού παραβίασης, δεδομένου ότι από τη στιγμή που η καταγγελλόμενη Τράπεζα έλαβε γνώση του ζητήματος από τους καταγγέλλοντες δεν προχώρησε σε ενέργειες προς διερεύνηση του περιστατικού, τις οποίες όφειλε και μπορούσε να κάνει, όπως διαπιστώθηκε όταν η Αρχή την ενημέρωσε για τη διενέργεια διοικητικού ελέγχου.

iv. Παραβίαση του κατ' άρθρο 15 ΓΚΠΔ δικαιώματος πρόσβασης των καταγγελλόντων, καθώς η Τράπεζα δεν χειρίστηκε τα από 29/3/2022 αιτήματα των καταγγελλόντων ως αιτήματα πρόσβασης κατά το άρθρο 15 ΓΚΠΔ, αλλά αρκέστηκε στην παροχή ενημέρωσης για το περιστατικό μόνο προς τον Α, η οποία μάλιστα αρχικά ήταν εσφαλμένη, όπως προαναφέρθηκε. Η ορθή ενημέρωση των καταγγελλόντων σε σχέση με το εν λόγω περιστατικό έλαβε χώρα στις 7/11/2023 και μόνο μετά τη διενέργεια διοικητικού ελέγχου εκ μέρους της Αρχής.

10. 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. Περαιτέρω η Αρχή, έλαβε υπόψη τα κριτήρια επιμέτρησης του προστίμου που ορίζονται στο άρθρο 83 παρ. 2 του ΓΚΠΔ, τις παραγράφους 4 εδ. α) και 5 εδ. α) και β) του ίδιου άρθρου που έχουν 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, ιδίως δε τα κριτήρια και τις ειδικές περιστάσεις που παρατίθενται στη συνέχεια:

- ότι η φύση της παράβασης αφορά βασικές αρχές του ΓΚΠΔ,
- ότι η επεξεργασία εντάσσεται στις βασικές δραστηριότητες του υπεύθυνου επεξεργασίας,
- ότι ο αριθμός των επηρεαζόμενων υποκειμένων ήταν μικρός,
- ότι οι κατηγορίες των προσωπικών δεδομένων που αφορά η επεξεργασία, ενέχουν υψηλό κίνδυνο, ως οικονομικά δεδομένα, ενώ η οικονομική ζημία στη συγκεκριμένη περίπτωση ήταν μικρή λόγω μικρών ποσών που μεταφέρθηκαν σε λανθασμένο τραπεζικό λογαριασμό,
- ότι δεν έγινε ορθή αξιολόγηση των καταγγελιών των υποκειμένων και των αιτημάτων τους για πρόσβαση στα προσωπικά τους δεδομένα, ενώ το συστημικό σφάλμα εντοπίστηκε μόνο κατόπιν του ελέγχου της Αρχής,
- ότι, πάντως, μετά τη διαπίστωση του προβλήματος η Τράπεζα έλαβε μέτρα προς αποκατάσταση της ζημίας που είχαν υποστεί τα υποκείμενα και αποτροπή παρόμοιων περιστατικών στο μέλλον, και
- ότι ο τζίρος (ακαθάριστος κύκλος εργασιών) της Τράπεζας για το τελευταίο οικονομικό έτος (2023) ανήλθε σε περίπου 2,6 δις ευρώ[4]

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η ΑΡΧΗ

Α. Επιβάλλει στην Εθνική Τράπεζα της Ελλάδος Α.Ε., ως υπεύθυνο επεξεργασίας, με βάση το άρθρο 58 παρ. 2 εδ. θ’ του ΓΚΠΔ, διοικητικό πρόστιμο ύψους εκατό χιλιάδων (100.000€) ευρώ, για τις διαπιστωθείσες παραβάσεις των άρθρων 5 παρ. 1 εδ. δ’ και

[4] Βλ. την Ετήσια Χρηματοοικονομική Έκθεση της Τράπεζας για το έτος 2023, διαθέσιμη στον σύνδεσμο https://www.nbg.gr/-/jssmedia/Files/Group/enhmerwsh-ependutwn/Annual_Financial_Reports/Annual-Financial-Report-2023-GR.pdf

στ’ σε συνδ. με το άρθρο 32 ΓΚΠΔ, και των άρθρων 25, 33 και 34 ΓΚΠΔ, σύμφωνα με όσα αναφέρονται στα σημεία i.-iii. της σκέψης 9 ανωτέρω.

Β. Επιβάλλει στην Εθνική Τράπεζα της Ελλάδος Α.Ε., ως υπεύθυνο επεξεργασίας, με βάση το άρθρο 58 παρ. 2 εδ. θ’ του ΓΚΠΔ, διοικητικό πρόστιμο ύψους είκοσι χιλιάδων (20.000€) ευρώ, για τη διαπιστωθείσα παράβαση του κατά το άρθρο 15 ΓΚΠΔ δικαιώματος πρόσβασης των καταγγελλόντων σύμφωνα με όσα αναφέρονται στο σημείο iv. της σκέψης 9 ανωτέρω.

Ο Πρόεδρος	**Η Γραμματέας**
Κωνσταντίνος Μενουδάκος	**Ειρήνη Παπαγεωργοπούλου**