ΑΠΔΠΧ 6/2022 ΕΠΙΒΟΛΗ ΠΡΟΣΤΙΜΟΥ ΓΙΑ ΣΥΝΕΧΙΖΟΜΕΝΟ ΠΕΡΙΣΤΑΤΙΚΟ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΤΡΑΠΕΖΑ

Σουζάνα Παπακωνσταντίνου
Δικηγόρος – Υπ. Δρ. Συνταγματικού Δικαίου Τμήμα Δημόσιας Διοίκησης – Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών, Μ.Δ.Ε. Κοινωνικής Προστασίας (Δίκαιο Κοιν. Ασφάλισης – Δημ. Δ. Υγείας) – Νομική Σχολή ΕΚΠΑ

Ι. ΙΣΤΟΡΙΚΟ:

Υποβλήθηκε στην Αρχή η με αρ. πρωτ. Γ/ΕΙΣ/8267/02-12-2020 καταγγελία της Α, με την οποία η τελευταία κατήγγειλε επαναλαμβανόμενο περιστατικό παραβίασης και μη ικανοποίηση του δικαιώματος διόρθωσης των προσωπικών της δεδομένων από την καταγγελλόμενη Τράπεζα Πειραιώς[1]. Πιο αναλυτικά:

1. Η καταγγέλλουσα γνωστοποίησε προφορικώς προς την καταγγελλόμενη Τράπεζα (σε κατάστημά της), αλλά και γραπτώς, μέσω e-mail, προς τον Υπεύθυνο Προστασίας Δεδομένων της Τράπεζας ότι οι κινήσεις της χρεωστικής της κάρτας κοινοποιούνταν από την καταγγελλόμενη σε ηλεκτρονικές διευθύνσεις που ανήκουν σε τρίτο πρόσωπο.
2. Στη συνέχεια, η Α κατήγγειλε τη μη ικανοποίηση του δικαιώματος διόρθωσης των προσωπικών της δεδομένων, καθώς, παρά το αίτημά της να λαμβάνει τη σχετική ενημέρωση στην ορθή διεύθυνση ηλεκτρονικού ταχυδρομείου της, οι ειδοποιήσεις σχετικά με τις κινήσεις της χρεωστικής της κάρτας συνέχισαν να αποστέλλονται σε διευθύνσεις που δεν της ανήκουν, όπως πληροφορήθηκε και από τον αποδέκτη τους.
3. Η Αρχή, εξετάζοντας την εν λόγω καταγγελία, κάλεσε με το υπ' αρ. πρωτ. Γ/ΕΞ/740/02-03-2021 έγγραφό της την καταγγελλόμενη να εκθέσει τις απόψεις της επί των καταγγελλομένων, να εξηγήσει τι ακριβώς συνέβη στην υπό κρίση περίπτωση, αλλά και ποια είναι η προβλεπόμενη διαδικασία αποφυγής παρόμοιου περιστατικού. Παράλληλα, η καταγγελλόμενη κλήθηκε να διευκρινίσει στην απάντησή της τα εξής: α) Εάν και με ποιο τρόπο ανταποκρίθηκε στο γραπτό αίτημα της καταγγέλλουσας προς τον Υπεύθυνο Προστασίας Δεδομένων της καταγγελλόμενης για διόρθωση των προσωπικών της δεδομένων, αναφέροντας σε περίπτωση μη έγκυρης ανταπόκρισης

[1] ΑΠΔΠΧ 6/2022, σελ. 1.

τους λόγους καθυστέρησης, β) για ποιο λόγο δεν προέβη η καταγγελλόμενη σε γνωστοποίηση του εν λόγω περιστατικού παραβίασης στην Αρχή σύμφωνα με το άρθρο 33 ΓΚΠΔ, αμέσως μόλις ειδοποιήθηκε σχετικά από την καταγγέλλουσα, γ) εάν και με ποιο τρόπο ενημέρωσε την καταγγέλλουσα για την καταγγελλόμενη παραβίαση, παρέχοντάς της τις απαιτούμενες από το άρθρο 34 ΓΚΠΔ πληροφορίες, δ) ποια μέτρα έλαβε η καταγγελλόμενη για την αντιμετώπιση του υπό εξέταση επαναλαμβανόμενου περιστατικού παραβίασης δεδομένων και για την άμβλυνση των δυσμενών συνεπειών του, ήτοι για τον μετριασμό του κινδύνου που επήλθε στην καταγγέλλουσα από αυτό.

4. Στην απάντησή της με το υπ' αρ. πρωτ. Γ/ΕΙΣ/1772/12-03/2021 έγγραφό της, η καταγγελλόμενη ανέφερε τα εξής: α) Ο λογαριασμός της καταγγέλλουσας Α είναι κοινός/διαζευκτικός με τον Β, συνδικαιούχο στον λογαριασμό, β) η δηλωθείσα ηλεκτρονική διεύθυνση από τον συνδικαιούχο του λογαριασμού διαφέρει μόνο κατά μια τελεία από την ηλεκτρονική διεύθυνση του φερόμενου ως τελικού αποδέκτη των ειδοποιήσεων Alerts. Επιπλέον, αυτή η διαφοροποίηση δεν αναγνωρίζεται από την υπηρεσία ηλεκτρονικής αλληλογραφίας Gmail της Google, με αποτέλεσμα η ηλεκτρονική αλληλογραφία που αποστέλλεται προς τη δηλωθείσα διεύθυνση με την τελεία, να παραδίδεται τελικά στην ηλεκτρονική διεύθυνση χωρίς την τελεία, καθώς το σύστημα τις θεωρεί ταυτόσημες.

5. Ακόμα, η καταγγελλόμενη υποστήριξε ότι απέστειλε απάντηση προς την καταγγέλλουσα, επισημαίνοντας ότι έπρεπε να ελεγχθούν οι δηλωθείσες ηλεκτρονικές διευθύνσεις από όλους τους συνδικαιούχους, ενώ υπέδειξε και τους τρόπους ελέγχου. Περαιτέρω, ισχυρίστηκε ότι δεν ασκήθηκε το δικαίωμα διόρθωσης σύμφωνα με το άρθρο 16 ΓΚΠΔ, καθώς οι ισχυρισμοί που πρόβαλε η καταγγέλλουσα δεν αφορούσαν σε προσωπικά δεδομένα της ίδιας, αλλά σε προσωπικά δεδομένα τρίτου. Επίσης, ισχυρίστηκε ότι ο συνδικαιούχος δεν είχε απευθύνει μέχρι τότε κανένα αίτημα προς την Τράπεζα και δεν είχε εξουσιοδοτήσει νόμιμα την καταγγέλλουσα να ασκήσει για λογαριασμό του τα δικαιώματά του που απορρέουν από τον ΓΚΠΔ. Επιπλέον, ανέφερε ότι είχε προβεί σε όλες τις απαιτούμενες ενέργειες, εφαρμόζοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη νόμιμη τήρηση, την επεξεργασία και την ασφαλή φύλαξη του αρχείου δεδομένων προσωπικού χαρακτήρα. Τέλος, ισχυρίστηκε ότι δεν προωθήθηκαν ποτέ προσωπικά δεδομένα σε ηλεκτρονική διεύθυνση τρίτου, και άρα δεν υφίστατο περιστατικό παραβίασης, διαρροής προσωπικών δεδομένων και συνεπώς καμία προϋπόθεση από αυτές που προβλέπονται στα άρθρα 33 και 34 του ΓΚΠΔ.

6. Στη συνέχεια, η καταγγέλλουσα, με το υπ' αρ. πρωτ. Γ/ΕΙΣ/2171/30-03-2021 έγγραφό της ενημέρωσε την Αρχή ότι το πρόβλημα εξακολουθούσε να υφίσταται και να αποστέλλονται οι ειδοποιήσεις στην ηλεκτρονική διεύθυνση τρίτου. Προς απόδειξη αυτού, επισύναψε δεκατέσσερα (14) μηνύματα ειδοποιήσεων που είχαν αποσταλεί στη διεύθυνση του τρίτου προσώπου και είχαν προωθηθεί στην καταγγέλλουσα προς ενημέρωσή της από το τρίτο πρόσωπο.

7. Ακολούθως, η Αρχή με τα υπ' αρ. πρωτ. Γ/ΕΞ/2288/12-10-2021 και Γ/ΕΞ/2289/12-10-2021, κάλεσε τα εμπλεκόμενα μέρη σε ακρόαση σε συνεδρίαση του τμήματος της Αρχής στις 19.10.2021 και κατόπιν αναβολής στις 10.11.2021, ενώ ορίσθηκε 15ήμερη προθεσμία υποβολής Υπομνημάτων, μέχρι την 01.12.2021.

8. Η καταγγέλλουσα δεν υπέβαλε υπόμνημα, αλλά τοποθετήθηκε βάσει του υπ' αρ. πρωτ. Γ/ΕΙΣ/7139/04-11-2021 εγγράφου της που είχε υποβάλει πριν από την ακρόαση. Υποστή-

ριξε δε, όλα όσα ανέφερε στην καταγγελία της και επιπλέον ότι ο σύζυγός της και συνδικαιούχος του λογαριασμού, είχε επισκεφθεί ξανά την Τράπεζα ζητώντας να διαγραφεί από συνδικαιούχος του λογαριασμού, ώστε να παύσουν να αποστέλλονται ειδοποιήσεις στη λάθος ηλεκτρονική διεύθυνση, καθώς όποια προηγούμενη προσπάθεια είχε επιχειρηθεί τηλεφωνικώς και διά ζώσης, είχε αποτύχει.

9. Η καταγγελλόμενη με το υπ΄ αρ. πρωτ. Γ/ΕΙΣ/7890/02-12-2021 υπόμνημά της, αλλά και κατά τη διάρκεια της ακρόασης, υποστήριξε όλα όσα είχε επικαλεστεί με το υπ' αρ. πρωτ. Γ/ΕΙΣ/12-03-2021 έγγραφό της. Πιο αναλυτικά ισχυρίστηκε τα εξής: α) Δεν τυγχάνουν εφαρμογής τα προβλεπόμενα στο άρθρο 16 ΓΚΠΔ περί δικαιώματος διόρθωσης, καθώς η καταγγέλλουσα δεν αιτήθηκε τη διόρθωση των δικών της προσωπικών δεδομένων, αλλά των προσωπικών δεδομένων τρίτου, β) ότι η Τράπεζα απέστειλε νομότυπα όλες τις ειδοποιήσεις στην ηλεκτρονική διεύθυνση που είχε δηλωθεί από τον συνδικαιούχο της καταγγέλλουσας και πως το σφάλμα της κατάληξης σε άλλον αποδέκτη λόγω μη αναγνώρισης του συμβόλου της τελείας (.) αποτελεί σφάλμα της Google αποκλειστικά, χωρίς τη δυνατότητα παρέμβασης από την Τράπεζα, γ) ότι οποιαδήποτε αυτόβουλη απόπειρα διευθέτησης του ζητήματος εκ μέρους της Τράπεζας θα ήταν παράνομη, ενώ τυχόν τηλεφωνική ενημέρωση του συνδικαιούχου από την Τράπεζα θα αποτελούσε «*εξ ορισμού επεξεργασία των δεδομένων του, εκτός των νόμιμων σκοπών επεξεργασίας των προσωπικών δεδομένων του*». Επίσης, δήλωσε ότι ο συνδικαιούχος μετέβη σε κατάστημα της Τράπεζας και προέβη σε κατάργηση της υπηρεσίας και αλλαγή της δηλωθείσας ηλεκτρονικής του διεύθυνσης και πως, συνεπώς, έχει ολοκληρωθεί η εν λόγω υπόθεση, χωρίς να έχει παρατηρηθεί οποιοδήποτε περιστατικό διαρροής προσωπικών δεδομένων της καταγγέλλουσας που να χρήζει περαιτέρω λήψης μέτρων. Τέλος, δήλωσε πως η υπό κρίση καταγγελία αποδεικνύεται αβάσιμη.

II. ΝΟΜΟΘΕΣΙΑ - ΝΟΜΟΛΟΓΙΑ:

Στο δεύτερο τμήμα του Κεφαλαίου IV, στα άρθρα 32-34 ΓΚΠΔ, θεμελιώνεται η ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα, στο άρθρο 32 ΓΚΠΔ προβλέπεται η κατοχύρωση της ασφάλειας της επεξεργασίας μέσω της εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων από τον υπεύθυνο επεξεργασίας και τον εκτελούντα. Επίσης, στα άρθρα 33 και 34 ΓΚΠΔ, προβλέπεται η υποχρέωση του υπεύθυνου επεξεργασίας να γνωστοποιεί στην αρμόδια εποπτική αρχή κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, αλλά και η υποχρέωσή του να ανακοινώνει την παραβίαση δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων. Επιπλέον, στο άρθρο 24 του ΓΚΠΔ, θεμελιώνεται η ευθύνη του υπεύθυνου επεξεργασίας, που πηγάζει από τις θεμελιώδεις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως είναι η «αρχή της ακεραιότητας» και η «αρχή της εμπιστευτικότητας» (άρθ. 5 παρ. 1 εδ. στ΄ ΓΚΠΔ). Πιο αναλυτικά:

1. Αρθ. 5 ΓΚΠΔ:

1. Σύμφωνα με το άρθ. 5 παρ. 1 εδ. στ' ΓΚΠΔ, «*τα δεδομένα προσωπικού χαρακτήρα 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»)*».

2. Στο Προοίμιο του ΓΚΠΔ και συγκεκριμένα στην Αιτιολογική Σκέψη 39 ορίζεται ότι «*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 τη χρήση αυτών των δεδομένων προσωπικού χαρακτήρα και του εν λόγω εξοπλισμού».

2. Άρθ. 4 ΓΚΠΔ
Σύμφωνα με το άρθ. 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 διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία».*

3. Άρθ. 24 ΓΚΠΔ:
Σύμφωνα με το άρθ. 24 παρ. 1 ΓΚΠΔ, *«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 τα 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».*

4. Αρθ. 32 ΓΚΠΔ:

1. Κατά το άρθ. 32 παρ. 1 του ΓΚΠΔ, *«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) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας».*

2. Σύμφωνα με την παρ. 2 του άρθ. 32 ΓΚΠΔ, *«κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφαλείας 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. Αρθ. 33 ΓΚΠΔ:

Α. Σύμφωνα με το άρθ. 33 παρ. 1 ΓΚΠΔ, *«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».

Β. Επιπλέον, 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 τη Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα[2], ανάμεσα στους τύπους σύμφωνα με τους οποίους κατηγοριοποιούνται οι παραβιάσεις προσωπικών δεδομένων, είναι αυτός που γίνεται με βάση την «αρχή της εμπιστευτικότητας», όταν διαπιστώνεται πρόσβαση άνευ δικαιώματος σε προσωπικά δεδομένα («confidentiality breach»).

Γ. Επίσης, σύμφωνα με τις Αιτιολογικές Σκέψεις 85 και 75 του ΓΚΠΔ, η παραβίαση δεδομένων προσωπικού χαρακτήρα μπορεί, εάν δεν αντιμετωπιστεί κατάλληλα και έγκαιρα, να έχει ως αποτέλεσμα σωματική, υλική ή ηθική βλάβη, όπως για παράδειγμα απώλεια του ελέγχου επί των δεδομένων προσωπικού χαρακτήρα, περιορισμό δικαιωμάτων, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, κ.ά[3].

Δ. Κατά την παράγραφο 5 του άρθ. 33 ΓΚΠΔ, *«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»*.

6. Αρθ. 34 ΓΚΠΔ:

Α. Σύμφωνα με το άρθ. 34 παρ. 1 ΓΚΠΔ, *«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»*.

Β. Επίσης, κατά την παράγραφο 2 του άρθ. 34 ΓΚΠΔ, *«στην ανακοίνωση στο υποκείμενο των δεδομένων (...) 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)»*.

III. Η ΑΠΟΦΑΣΗ ΤΗΣ ΑΡΧΗΣ:

Η Αρχή, λαμβάνοντας υπόψη όλα τα ανωτέρω, επέβαλε στην καταγγελλόμενη Τράπεζα Πειραιώς Α.Ε., ως υπεύθυνο επεξεργασίας, χρηματικό πρόστιμο ύψους δέκα χιλιάδων (10.000€) ευρώ για τη διαπιστωθείσα παράβαση της αρχής της εμπιστευτικότητας του άρθ. 5 παρ. 1 εδ. στ' ΓΚΠΔ και των υποχρεώσεών της εκ των άρθρων 33 και 34 ΓΚΠΔ, σύμφωνα με το άρθ. 58 παρ. 2 εδ. θ΄ ΓΚΠΔ. Επιπλέον, η Αρχή απηύθυνε στην καταγγελλόμενη Τράπεζα προειδοποίηση σύμφωνα με

[2] *Guidelines on Personal data breach notification under Regulation 2016/679,* WP 250 rev. 1.

[3] Βλ. Σχετ. ΑΠΔΠΧ 6/2022, σελ. 10.

το άρθ. 58 παρ. 2 εδ. α΄, ώστε να θέσει σε εφαρμογή κατάλληλα τεχνικά και οργανωτικά μέτρα προς επιβεβαίωση της ορθότητας των διευθύνσεων e-mail που δηλώνονται στην Τράπεζα για τη λήψη ειδοποιήσεων Alerts.

Στην απόφαση αυτή της Αρχής, συνετέλεσαν τα εξής πραγματικά περιστατικά:

1. Η παραβίαση των αρχών της ακεραιότητας και της εμπιστευτικότητας αφορούσε και τους δυο συνδικαιούχους του τραπεζικού λογαριασμού, καθώς η κοινοποίηση των δεδομένων προσωπικού χαρακτήρα προς τρίτο πρόσωπο, εν αγνοία των υποκειμένων των δεδομένων, αφορούσε δεδομένα και των δυο συνδικαιούχων.
2. Η παραβίαση ήταν επαναλαμβανόμενη και διαρκής, παρά τη διαμαρτυρία της καταγγέλλουσας.
3. Η καταγγελλόμενη, ως υπεύθυνος επεξεργασίας, μόλις έλαβε γνώση του περιστατικού αδράνησε, δεν αξιολόγησε το περιστατικό, δεν προέβη στις απαιτούμενες με βάση τον ΓΚΠΔ ενέργειες για την άρση των συνεπειών της παραβίασης (γνωστοποίηση παραβίασης στην Αρχή και ανακοίνωση στο υποκείμενο των δεδομένων), ούτε στη λήψη διορθωτικών μέτρων για την ασφάλεια των δεδομένων (π.χ. παύση της αποστολής ειδοποιήσεων Alerts μέχρι την επίλυση του ζητήματος).
4. Η καταγγελλόμενη, ως υπεύθυνος επεξεργασίας, μην πράττοντας όλα όσα έχει ευθύνη να πράξει από τον ΓΚΠΔ[4], «μετακύλησε» την ευθύνη στον συνδικαιούχο του λογαριασμού της καταγγέλλουσας, αδρανώντας και αναμένοντας από εκείνον να ασκήσει το δικαίωμα διόρθωσης[5].
5. Η καταγγελλόμενη επικαλέστηκε ότι το σφάλμα έγκειτο στον συσχετισμό λόγω μιας τελείας (.) και πως αφορούσε τη Google αποκλειστικά και όχι την ίδια, κάτι το οποίο δεν ισχύει, αφενός γιατί η προσθήκη τελείας δεν αλλάζει κάτι επί της ουσίας στους λογαριασμούς e-mail της Google[6], αφετέρου γιατί το σφάλμα ήταν η εκ παραδρομής τοποθέτηση του γράμματος (i) αντί του γράμματος (e).
6. Η καταγγελλόμενη, ως υπεύθυνος επεξεργασίας, είχε εφαρμόσει εκ των προτέρων ελλιπή τεχνικά και οργανωτικά μέτρα ασφάλειας, που οδήγησαν στο περιστατικό.
7. Η φύση, η βαρύτητα και η διάρκεια της παράβασης αποτέλεσαν σημαντικές παραμέτρους που ελήφθησαν υπόψη κατά την απόφαση της Αρχής.
8. Η παράβαση έθιξε δύο (2) φυσικά πρόσωπα ως υποκείμενα των δεδομένων προσωπικού χαρακτήρα, χωρίς όμως αυτά να υποστούν οικονομική ζημία.
9. Υπήρξε αμέλεια και όχι δόλος από την πλευρά της καταγγελλόμενης.
10. Τα υποκείμενα των δεδομένων είχαν συντρέχουσα αμέλεια.
11. Δεν υπήρχε προηγούμενη παράβαση της καταγγελλόμενης ως υπεύθυνου επεξεργασίας.

IV. ΣΚΕΨΕΙΣ - ΠΑΡΑΤΗΡΗΣΕΙΣ:

Η απόφαση 6/2022 της Αρχής είναι σπουδαίας σημασίας, καθώς οφείλουμε να συγκρατήσουμε τα εξής:

1. Κατοχυρώνονται οι θεμελιώδεις αρχές της ακεραιότητας και της εμπιστευτικότητας, που

[4] Βλ. σχετ. Σκ. 7, ΑΠΔΠΧ 6/2022, σελ. 13.
[5] Βλ. σχετ. Σκ. 5, ΑΠΔΠΧ 6/2022, σελ. 11-12.
[6] Βλ. σχετ. Σκ. 6, ΑΠΔΠΧ 6/2022, σελ. 12.

αποτελούν «νεωτερισμό[7]» του ΓΚΠΔ και που πρέπει να διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και που εξασφαλίζουν τη νομιμότητά της.

2. Διαφαίνεται η σημασία της θεμελιώδους αρχής της λογοδοσίας[8] του υπεύθυνου επεξεργασίας στον ΓΚΠΔ, στην οποία ερείδονται όλες οι διατάξεις που αφορούν στην ευθύνη του να προβαίνει στις απαραίτητες ενέργειες και να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, τόσο για να προλαμβάνει όσο και για να αντιμετωπίζει τυχόν παραβίαση δεδομένων προσωπικού χαρακτήρα. Η αρχή της λογοδοσίας λειτουργεί σαν «μηχανισμός εγγύησης[9]» της τήρησης των αρχών που πρέπει να διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επίσης, μέσω της θεσμοθέτησης της αρχής αυτής, αναδεικνύεται η επιλογή του Ευρωπαίου νομοθέτη για μετακύληση της ευθύνης της εφαρμογής του ΓΚΠΔ από τις εποπτικές αρχές στους υπεύθυνους επεξεργασίας, ώστε η προστασία δεδομένων «*να γίνει κτήμα καθενός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα*[10]».
3. Ο υπεύθυνος επεξεργασίας μόλις αντιλαμβάνεται την παραβίαση δεν θα πρέπει να αδρανεί[11] και να αναμένει από τα υποκείμενα των δεδομένων να ασκήσουν εκείνοι τα δικαιώματα που προβλέπονται στον ΓΚΠΔ. Αντιθέτως, οφείλει μόλις αντιλαμβάνεται την παραβίαση δεδομένων προσωπικού χαρακτήρα, να τη γνωστοποιεί στην Αρχή και να ενημερώνει ενδελεχώς[12] τα υποκείμενα των δεδομένων σχετικά με αυτή.
5. Ο υπεύθυνος επεξεργασίας, όταν υπάρχει παραβίαση θα πρέπει να εξετάζει «συσταλτικά» το βαθμό της νομιμοποίησης του υποκειμένου που ζητά την άρση της παραβίασης, όταν παραβίαση συνίσταται στην κοινοποίηση σε τρίτο πρόσωπο και δικών του δεδομένων προσωπικού χαρακτήρα.
6. Απώτερο στόχο για τον υπεύθυνο επεξεργασίας θα πρέπει να αποτελεί η άρση της παραβίασης δεδομένων προσωπικού χαρακτήρα και η αποκατάσταση των δικαιωμάτων των υποκειμένων των δεδομένων.

---

7 Βλ. σχετ. Ι. Ιγγλεζάκη, *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Interactive Learning*, 3η Έκδοση, 2020, σελ. 77.

8 Βλ. σχετ. περί αρχής της λογοδοσίας ΑΠΔΠΧ 68/2018, Σκ. 2, σελ 3 και ΑΠΔΠΧ 69/2018, Σκ. 2, σελ. 3.

9 Βλ. σχετ. Λ. Μήτρου, «Υποχρεώσεις του υπεύθυνου επεξεργασίας», σε: Λ. Κοτσαλής/Κ. Μενουδάκος, *Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων*, Εκδ. Σάκκουλα, 2017, σελ. 91.

10 Βλ. σχετ. Ι. Ιγγλεζάκη, ό.π. (υποσ. 7), σελ. 77.

11 Σε αντίστοιχες αποφάσεις της Αρχής όπου υπήρξε παραβίαση των αρχών της ακεραιότητας και της εμπιστευτικότητας, όπως στην ΑΠΔΠΧ 68/2018 και στην ΑΠΔΠΧ 69/2018, ο υπεύθυνος επεξεργασίας (επίσης Τράπεζα), αφενός γνωστοποίησε την παραβίαση στην Αρχή (έστω και καθυστερημένα), αφετέρου ενημέρωσε τα υποκείμενα των δεδομένων. Επιπλέον, προέβη και σε λήψη μέτρων, όπως η θέσπιση ελεγκτικών μηχανισμών και δικλείδων ασφαλείας για την αποφυγή μελλοντικών παραβιάσεων (ΑΠΔΠΧ 68/2018) ή ο ανασχεδιασμός της λειτουργίας των παρεχόμενων υπηρεσιών, προκειμένου να αποκλεισθούν ανθρώπινα λάθη (ΑΠΔΠΧ 69/2018). Για αυτό τον λόγο και σε αυτές τις αποφάσεις η Αρχή προέβη μόνον σε επίπληξη.

12 Βλ. σχετ. Φ. Παναγοπούλου-Κουτνατζή, «Το νέο πλαίσιο των ανανεωμένων δικαιωμάτων», σε: *Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR)*, Νομική Βιβλιοθήκη, 2018, σελ. 32: «*Η σχετική ενημέρωση πρέπει να είναι ενδελεχής, περιλαμβάνοντας το είδος δεδομένων, τον αριθμό θιγόμενων ατόμων, τον τρόπο παραβιάσεως, τα άτομα που έλαβαν γνώση των δεδομένων, τον τρόπο αναγνωρίσεως της παραβιάσεως κ.ο.κ. Περαιτέρω, πρέπει να υφίσταται ενημέρωση αναφορικά με τις υπάρχουσες καταγεγραμμένες διαδικασίες αντιμετωπίσεως του περιστατικού και εν γένει τις διαδικασίες χειρισμού περιστατικού παραβιάσεως δεδομένων, τη διερεύνηση, τα διορθωτικά μέτρα, τα υπάρχοντα μέτρα ασφαλείας, τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και τις μελλοντικές ενέργειες του υπεύθυνου επεξεργασίας*».

V. ΕΠΙΛΟΓΟΣ:

Θα μπορούσαμε να συμπεράνουμε ότι η Απόφαση 6/2022 της ΑΠΔΠΧ θεμελιώνεται επί της ουσίας σε δυο βασικούς πυλώνες: Αφενός, στην κατανόηση του «πυρήνα» του ΓΚΠΔ, που δεν είναι άλλος από την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων προσωπικού χαρακτήρα. Αφετέρου στην αναγνώριση της «επαυξημένης»[13] ευθύνης του υπεύθυνου επεξεργασίας, όπως κατοχυρώνεται από τον ΓΚΠΔ, σύμφωνα με την οποία οφείλει να ενεργεί άμεσα και να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα –προληπτικά και κατασταλτικά– προκειμένου να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

Επιπλέον, μέσω της Απόφασης γίνεται σαφές ότι πρωτεύοντα στόχο του υπεύθυνου επεξεργασίας θα πρέπει να αποτελεί η άρση της παραβίασης και η αποκατάσταση των δικαιωμάτων των υποκειμένων των δεδομένων, σύμφωνα με την αρχή της νομιμότητας και όχι η υπό στενή έννοια αναζήτηση της νομιμοποίησης των εμπλεκόμενων υποκειμένων, όταν εκ του αποτελέσματος θίγονται άμεσα τα δικαιώματά τους.

Εν κατακλείδι, για ακόμη μια φορά, με αφορμή την Απόφαση της Αρχής, αναδεικνύεται η σημασία του ΓΚΠΔ, ο οποίος, λειτουργώντας ως θεσμικό εργαλείο, στοχεύει στη συνεχή εξέλιξη του *«νομολογιακώς διαπλασμένου»*[14] δικαίου της προστασίας δεδομένων προσωπικού χαρακτήρα: Ενός δικαίου που απώτερο στόχο του έχει τον σεβασμό και τη διαφύλαξη των θεμελιωδών δικαιωμάτων του ατόμου και που λειτουργεί ως εγγύηση του κράτους δικαίου, προς επίτευξη της κοινωνικής ευημερίας και της προόδου. ❑

[13] Βλ. σχετ. Φ. Παναγοπούλου-Κουτνατζή, *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ*, Εκδ. Σάκκουλα, 2017, σελ. 31.

[14] Βλ. σχετ. Σ. Βλαχόπουλο, «Διασυνοριακή μεταβίβαση δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση προς τρίτες χώρες: Οι τελευταίες εξελίξεις», σε *Προστασία των δεδομένων προσωπικού χαρακτήρα. Εξελίξεις ενόψει της θέσης σε εφαρμογή του νέου Γενικού Κανονισμού ΕΕ 2016/679*, Εκδ. Σάκκουλα, 2018, σελ. 32-33.