ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 31-03-2015

Αριθ. Πρωτ.: Γ/ΕΞ/2048/31-03-2015

Α Π Ο Φ Α Σ Η ΑΡ. 39/2015

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την 03-03-2015, σε συνέχεια της από 20-01-2015 τακτικής συνεδρίασής της και εξ αναβολής της από 16-12-2014 συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Π. Χριστόφορος, Πρόεδρος της Αρχής, και τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Αν. – Ιωάν. Μεταξάς, Δ. Μπριόλας, Α. Συμβώνης, ως εισηγητής, και Κ. Χριστοδούλου. Το τακτικό μέλος Π. Τσαντίλας, αν και προσκλήθηκε νομίμως, δεν προσήλθε λόγω κωλύματος. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, ο Κ. Λιμνιώτης, ειδικός επιστήμων – πληροφορικός, ως βοηθός εισηγητή. Επίσης, παρέστη, με εντολή του Προέδρου, και η Ε. Παπαγεωργοπούλου, υπάλληλος του Διοικητικού – Οικονομικού Τμήματος της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Υποβλήθηκε στην Αρχή η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/687/03-02-2014 καταγγελία του κ. Α σχετικά με την υπηρεσία «Winbank for cards» που παρέχει η Τράπεζα Πειραιώς σε χρήστες των ηλεκτρονικών της υπηρεσιών τραπεζικής μέσω της ιστοσελίδας www.winbank.gr. Με βάση την εν λόγω καταγγελία, αλλά και κατόπιν ελέγχου της συγκεκριμένης ιστοσελίδας, φαίνεται ότι αν ο επισκέπτης της εν λόγω ιστοσελίδας εισαγάγει τα στοιχεία μιας πιστωτικής κάρτας που έχει χορηγήσει η Τράπεζα σε κάποιον πελάτη της, καθώς επίσης και την ημερομηνία γέννησης του κατόχου αυτής της κάρτας, θα μπορεί να λάβει πληροφορίες περί των κινήσεων της κάρτας (αγορές/χρεώσεις και πληρωμές), χωρίς να είναι σε εφαρμογή άλλος μηχανισμός αυθεντικοποίησης του χρήστη. Τα στοιχεία της κάρτας που απαιτείται να

εισαγάγει ο επισκέπτης της ανωτέρω ιστοσελίδας είναι ο αριθμός αυτής, ο τριψήφιος αριθμός CVV/CVC (Card Verification Value/Card Validation Code), καθώς επίσης και η ημερομηνία λήξης αυτής.

Η Αρχή, στο πλαίσιο εξέτασης της εν λόγω καταγγελίας, απέστειλε στην Τράπεζα Πειραιώς (εφεξής, υπεύθυνος επεξεργασίας) το υπ' αριθμ. πρωτ. Γ/ΕΞ/687-1/17-02-2014 έγγραφο, με το οποίο – μεταξύ άλλων – ζητούσε τις απόψεις επί των καταγγελλομένων. Ακολούθως, ο υπεύθυνος επεξεργασίας απάντησε με το υπ' αριθμ. πρωτ. …/…/…/2014 έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/1767/18-03-2014 έγγραφο), ενώ πρόσθετες διευκρινίσεις δόθηκαν μετέπειτα, κατόπιν του υπ' αριθμ. πρωτ. Γ/ΕΞ/687-2/01-08-2014 εγγράφου της Αρχής, με το υπ' αριθμ. πρωτ. …/…/…/2014 έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/5314/09-09-2014). Με βάση τα ανωτέρω έγγραφα του υπευθύνου επεξεργασίας, προκύπτουν τα εξής:

α) Η συγκεκριμένη διαδικτυακή υπηρεσία παρέχεται από το 2005 και έχει ως στόχο την αμεσότερη πληροφόρηση για τις κινήσεις των πιστωτικών τους καρτών (χρεώσεις και πιστώσεις) στους πελάτες της Τράπεζας – κατόχους πιστωτικών καρτών, οι οποίοι δεν επιθυμούν να είναι εγγεγραμμένοι χρήστες στις υπηρεσίες ηλεκτρονικής τραπεζικής (winbank) και να αξιοποιούν το πλήθος των υπηρεσιών που αυτή προσφέρει[1]. Όπως αναφέρει η Τράπεζα, κανείς πελάτης της δεν έχει θέσει υπόψη της ότι κινδύνευσαν προσωπικά του δεδομένα μέσω της υπηρεσίας «Winbank for cards».

β) Στο πλαίσιο της υπηρεσίας «Winbank for cards», ο πελάτης της Τράπεζας – κάτοχος πιστωτικής κάρτας εισάγει τα προαναφερθέντα στοιχεία αυτής, καθώς και την ημερομηνία γέννησής του, προκειμένου να αποκτήσει πρόσβαση σε πληροφορίες σχετικά με το υπόλοιπο της πιστωτικής του κάρτας, τις κινήσεις που έχει πραγματοποιήσει με την κάρτα μέχρι την προηγούμενη μέρα, αλλά και σε παλαιότερα αντίγραφα των ενημερωτικών δελτίων αυτής (statements) – δηλαδή αποκτά την πληροφόρηση που περιέχεται και στα μηνιαία ενημερωτικά δελτία που αποστέλλει η Τράπεζα στους κατόχους πιστωτικών καρτών μέσω συμβατικού ταχυδρομείου (στην ταχυδρομική διεύθυνση που οι τελευταίοι έχουν δηλώσει). Δεν υπάρχει η δυνατότητα, μέσω της υπηρεσίας «Winbank for cards», πραγματοποίησης συναλλαγών.

γ) Η ανωτέρω αναφερόμενη δυνατότητα χρήσης της εν λόγω υπηρεσίας συνομολογείται μεταξύ του πελάτη και της Τράπεζας στο πλαίσιο της σύμβασης χορήγησης πιστωτικής κάρτας, παρέχεται δε αποκλειστικά για το σκοπό της σωστής εξυπηρέτησης, υποστήριξης και

[1] Επισημαίνεται ότι η πρόσβαση των εγγεγραμμένων (ήτοι εξουσιοδοτημένων) χρηστών στις υπηρεσίες ηλεκτρονικής τραπεζικής winbank πραγματοποιείται μέσω μηχανισμού αυθεντικοποίησης των χρηστών που βασίζεται στη χρήση συνθηματικών.

παρακολούθησης της συναλλακτικής σχέσης του πελάτη-κατόχου της κάρτας με την Τράπεζα.

Περαιτέρω, όπως αναφέρεται στο πληροφοριακό δελτίο που είναι αναρτημένο στην ιστοσελίδα της Τράπεζας, ο κάτοχος της κάρτας έχει τη δυνατότητα, με ένα τηλεφώνημα (χρέωσης ως κλήσης προς το εσωτερικό), να ζητήσει την εξαίρεση της κάρτας του από την υπηρεσία «Winbank for cards».

δ) Η υπηρεσία «Winbank for cards» παρέχεται εξ αρχής σε όλους τους πελάτες, ανεξάρτητα αν έχουν εγγραφεί στις υπηρεσίες ηλεκτρονικής τραπεζικής (winbank) ή όχι.

ε) Ο κάτοχος πιστωτικής κάρτας είναι υποχρεωμένος να μεριμνά για την αποτελεσματική φύλαξή της, υποχρέωση που ούτως ή άλλως βαρύνει συμβατικώς όλους τους κατόχους πιστωτικών καρτών. Σύμφωνα άλλωστε με τα συναλλακτικά ήθη αλλά και με συμβατική υποχρέωση του κατόχου, κάθε απώλεια ή κλοπή πρέπει να γνωστοποιείται στην Τράπεζα από τον κάτοχο, ο δε κάτοχος – και μόνο αυτός – έχει δικαίωμα χρήσης της κάρτας, ενώ η μεταβίβαση αυτής ή της χρήσης της απαγορεύεται.

Επιπροσθέτως, η έλλειψη επίδειξης της δέουσας επιμέλειας κάθε κατόχου της κάρτας σε ό,τι αφορά στη μυστικότητα των στοιχείων της εγκυμονεί πολύ μεγαλύτερους κινδύνους από την απλή πρόσβαση στις κινήσεις και στις οφειλές αυτής.

στ) Η Τράπεζα έχει λάβει ασφαλιστικές δικλείδες για την προστασία των δεδομένων που καταχωρίζονται ή εμφανίζονται (ψηφιακά πιστοποιητικά, συμμόρφωση με το πρότυπο PCI κτλ.), ενώ υπάρχει και ειδικό τμήμα που παρακολουθεί επί εικοσιτετραώρου βάσεως, επί επτά (7) ημέρες την εβδομάδα, την πιθανή εμφάνιση ύποπτων συναλλαγών.

Η Τράπεζα Πειραιώς κλήθηκε νομίμως, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/687-3/27-11-2014 έγγραφο της Αρχής, σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 16-12-2014, ως υπεύθυνος επεξεργασίας, για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει διεξοδικά τις απόψεις του επί των ανωτέρω. Ο υπεύθυνος επεξεργασίας, διά του νομίμου εκπροσώπου του κ. Θωμά Στάικου, δικηγόρου, ζήτησε - με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/7874/15-12-2014 αίτημα - και έλαβε από την Αρχή αναβολή για τη συζήτηση της υπόθεσης την Τρίτη 20-01-2015. Στη συνεδρίαση της 20-01-2015, παρέστησαν νομίμως, ως εκπρόσωποι του υπευθύνου επεξεργασίας, ο Β , Δ/ντής για την υπηρεσία winbank, καθώς επίσης και ο κ. Θ. Στάικος, δικηγόρος. Κατά την ακρόαση, οι ως άνω εκπρόσωποι εξέθεσαν προφορικά τις απόψεις τους. Κατόπιν της ακρόασης, ο υπεύθυνος επεξεργασίας κατέθεσε εμπροθέσμως σχετικό υπόμνημα (αρ. πρωτ. Γ/ΕΙΣ/492/28-01-2015), στο οποίο επισημαίνονται τα εξής:

α) Οι πελάτες λαμβάνουν γνώση της συγκεκριμένης υπηρεσίας με τρεις τρόπους: i) από

τον υπάλληλο που τον ενημερώνει κατά τη διάρκεια υπογραφής της σύμβασης, ii) από την ίδια τη σύμβαση, iii) από το διαδικτυακό τόπο, που είναι πάντα ενεργός και έχει ευρεία επισκεψιμότητα από τους πελάτες της Τράπεζας ή τους εν δυνάμει πελάτες της Τράπεζας,

β) Εάν ο πελάτης καταχωρήσει κάποιο από τα στοιχεία πιστοποίησης εσφαλμένα, το σύστημα απαγορεύει την είσοδό του στην τρίτη προσπάθεια,

γ) Ο Όμιλος της Τράπεζας Πειραιώς, για τα μέτρα ασφάλειας που εφαρμόζει, έχει λάβει διεθνή πιστοποιητικά, τα οποία προσκομίστηκαν κατά τη διάρκεια της ακρόασης (αρ. πρωτ. Γ/ΕΙΣ/291/20-01-2015),

δ) Δεν υπήρξε ποτέ διαμαρτυρία-όχληση, δικαστική ή εξώδικη, για παραβίαση δεδομένων προσωπικού χαρακτήρα, η οποία να έχει ως γενεσιουργό αιτία τη συγκεκριμένη τραπεζική υπηρεσία "winbank for cards".

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων και μνεία των λεχθέντων κατά τη συνεδρίαση της 20-01-2015, άκουσε τον εισηγητή και τις διευκρινίσεις του βοηθού εισηγητή, ο οποίος στη συνέχεια αποχώρησε πριν από τη διάσκεψη και τη λήψη απόφασης, κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Το άρθρο 2 του ν. 2472/1997, ορίζει ότι «δεδομένα προσωπικού χαρακτήρα» είναι «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων». «Υποκείμενο των δεδομένων» είναι «το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική».

Στο ίδιο άρθρο επίσης ορίζεται ως επεξεργασία δεδομένων προσωπικού χαρακτήρα «κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή». Επίσης, ως υπεύθυνος επεξεργασίας ορίζεται οποιοσδήποτε καθορίζει το

σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

2. Σύμφωνα με το αρ. 4 παρ. 1 στοιχ. α) του ν. 2472/1997, τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται με τρόπο θεμιτό και νόμιμο, για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών (αρχή του σκοπού). Επιπλέον, σύμφωνα με το αρ. 4 παρ. 1 στοιχ. β) του ν. 2472/1997, τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας (αρχή της αναλογικότητας). Περαιτέρω, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο όταν το υποκείμενο έχει δώσει τη συγκατάθεσή του, όπως επιτάσσει το αρ. 5 παρ. 1 του ν. 2472/1997. Σημειώνεται ότι, σύμφωνα με το άρθρο 2 στοιχ. ια΄ του ν. 2472/1997, ως συγκατάθεση νοείται «*κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως που εκφράζεται με τρόπο σαφή, και εν πλήρη επιγνώσει, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο της επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*».

Κατ' εξαίρεση επιτρέπεται η επεξεργασία προσωπικών δεδομένων, και χωρίς τη συγκατάθεση του υποκειμένου τους, εφόσον συντρέχει κάποια από τις περιπτώσεις που προβλέπονται, κατά τρόπο περιοριστικό, στην παρ. 2 του άρθρου αυτού. Ειδικότερα, η επεξεργασία επιτρέπεται και χωρίς τη συγκατάθεση όταν: «*α) είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία το συμβαλλόμενο μέρος είναι υποκείμενο των δεδομένων (…)*».

3. Στην προκειμένη περίπτωση, η επεξεργασία προσωπικών δεδομένων μέσω της διαδικτυακής υπηρεσίας «Winbank for cards» αποσκοπεί, όπως προαναφέρθηκε, στην αμεσότερη πληροφόρηση των πελατών του υπεύθυνου επεξεργασίας, που είναι κάτοχοι πιστωτικών καρτών, για τις κινήσεις των καρτών αυτών, και οι οποίοι δεν επιθυμούν να είναι εγγεγραμμένοι χρήστες στις υπηρεσίες ηλεκτρονικής τραπεζικής (winbank),. Ως εκ τούτου, καθίσταται σαφές ότι η εν λόγω επεξεργασία δεν μπορεί να εκληφθεί ως απολύτως απαραίτητη στο πλαίσιο των συμβατικών σχέσεων μεταξύ του υπευθύνου επεξεργασίας και των υποκειμένων των δεδομένων (ήτοι των πελατών), αφού η συγκεκριμένη πληροφόρηση για τις κινήσεις των καρτών μπορεί να παρέχεται και με άλλους τρόπους όπως μέσω ταχυδρομείου - η οποία μέθοδος εξάλλου ήδη ακολουθείται με βάση τα όσα δήλωσε ο υπεύθυνος επεξεργασίας: σημειωτέο δε ότι η παροχή της συγκεκριμένης διαδικτυακής υπηρεσίας δεν είναι συνήθης σε τράπεζες που επίσης παρέχουν πιστωτικές κάρτες στους πελάτες τους. Κατά συνέπεια, για την εν λόγω επεξεργασία δεν συντρέχει το στοιχείο της

αναγκαιότητας και κατά αυτόν τον τρόπο δεν μπορεί να έχει εφαρμογή η ως άνω εξαίρεση του άρ. 5 παρ. 2 στοιχ. α) του ν. 2472/1997.

Με βάση τα παραπάνω, προκύπτει ότι η υπηρεσία «Winbank for cards» θα πρέπει να παρέχεται σε κάθε πελάτη του υπεύθυνου επεξεργασίας μόνο κατόπιν συγκατάθεσής του – ήτοι ο πελάτης θα πρέπει να δηλώσει σαφώς, ρητώς και ειδικώς (άρ. 2 στοιχ. ια΄ του ν. 2472/1997) ότι συγκατατίθεται για την εν λόγω επεξεργασία Η απαίτηση ότι το υποκείμενο των δεδομένων πρέπει να δώσει τη συγκατάθεσή του υποδηλώνει ότι η απλή αδράνειά του δεν επαρκεί και ότι απαιτείται κάποιο είδος θετικής ενέργειάς του για να υπάρχει συγκατάθεση (explicit consent ή αλλιώς σύστημα opt-in) – άλλωστε, διαφορετικά, ο υπεύθυνος επεξεργασίας δεν έχει τη βεβαιότητα που απαιτείται για την ύπαρξη συγκατάθεσης (πβλ. Γνώμη 15/2011 της Ο.Ε. του Αρ. 29). Σημειωτέον, σύμφωνα με τα όσα αναφέρονται στις απαντήσεις του υπεύθυνου επεξεργασίας, η υπηρεσία «Winbank for cards» παρέχεται σε όλους τους πελάτες ανεξαιρέτως – ακόμα και σε αυτούς οι οποίοι χρησιμοποιούν τις γενικές υπηρεσίες ηλεκτρονικής τραπεζικής (winbank), οι οποίοι, με βάση τα όσα δήλωσε ο υπεύθυνος επεξεργασίας, δεν αποτελούν το κοινό στο οποίο απευθύνεται κατ' αρχάς η εν λόγω υπηρεσία - εκτός και αν πελάτης δηλώσει μέσω τηλεφώνου ότι δεν την επιθυμεί (σύστημα «opt-out»). Τούτο όμως δεν είναι σύμφωνο με τον ορισμό της συγκατάθεσης του άρ. 2 του ν. 2472/1997.

Εξάλλου, προκειμένου οι πελάτες του υπεύθυνου επεξεργασίας να παρέχουν την ελεύθερη, ρητή και ειδική συγκατάθεσή τους (άρθρο 2 στοιχ. ια΄ του ν. 2472/1997) για τη συγκεκριμένη επεξεργασία, απαιτείται να έχουν προηγουμένως ενημερωθεί για τα βασικά στοιχεία αυτής. Τέτοια ενημέρωση ωστόσο δεν φαίνεται ότι παρέχεται επαρκώς. Συγκεκριμένα, ο υπεύθυνος επεξεργασίας αναφέρει ότι η παροχή της εν λόγω υπηρεσίας συνομολογείται μεταξύ του πελάτη και της Τράπεζας στο πλαίσιο της σύμβασης χορήγησης πιστωτικής κάρτας. Ωστόσο, από το υπόδειγμα της σύμβασης που επισυνάφθηκε με το υπ' αριθμ. πρωτ. …/…/…/2014 έγγραφο του υπευθύνου επεξεργασίας δεν προκύπτει ότι παρέχεται πλήρης ενημέρωση (συγκεκριμένα, στη σύμβαση αναφέρεται: *«(…) Ο κάτοχος μπορεί να ενημερώνεται για το μηνιαίο λογαριασμό του με τους εξής τρόπους: α) (…) β (…), γ) από την ηλεκτρονική διεύθυνση www.winbank.gr (…) ή και από την υπηρεσία winbank for cards (…)»),* αφού αν ο πελάτης-κάτοχος πιστωτικής κάρτας δεν επισκεφθεί το διαδικτυακό τόπο της Τράπεζας (κάτι που είναι πιθανό, ιδίως δε για τους πελάτες που δεν αξιοποιούν τις γενικές υπηρεσίες ηλεκτρονικής τραπεζικής (winbank)), δεν θα είναι ενήμερος για τα χαρακτηριστικά της εν λόγω υπηρεσίας, η οποία μάλιστα ενέχει και κινδύνους ως προς την ασφάλεια των προσωπικών δεδομένων, όπως επισημαίνεται στη συνέχεια στη Σκέψη 4. όπως

Με βάση το υπόμνημα του υπεύθυνου επεξεργασίας, η ενημέρωση τελικά επαφίεται στους εκάστοτε υπαλλήλους του υπευθύνου επεξεργασίας και είναι προφορική.

Συνεπώς, για τη συγκεκριμένη επεξεργασία δεν πληρούνται οι προϋποθέσεις του άρθρου 5 του ν. 2472/1997.

4. Το άρθρο 10, παρ. 3 του ν. 2472/1997 ορίζει ότι ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.

Στη συγκεκριμένη περίπτωση, τα δεδομένα που αφορούν στην κίνηση της πιστωτικής κάρτας αποκαλύπτουν πληροφορίες ιδιαίτερα σημαντικές για τον κάτοχό της, όπως πληροφορίες οικονομικής φύσης από τις οποίες μπορούν να προκύψουν συμπεράσματα για την οικονομική του κατάσταση και το καταναλωτικό του προφίλ - τα ενδιαφέροντά του. Ως εκ τούτου, μη εξουσιοδοτημένη πρόσβαση τρίτων στα δεδομένα που παρέχει η υπηρεσία «Winbank for cards» μπορεί να επιφέρει δυσμενείς συνέπειες στο υποκείμενο των δεδομένων (κάτοχο της κάρτας). Τούτο δε επιτείνεται από το γεγονός ότι κάθε μη εξουσιοδοτημένη πρόσβαση στα ως άνω δεδομένα δεν γίνεται αντιληπτή από τον κάτοχο της κάρτας - αφού ο χρήστης της υπηρεσίας δεν μπορεί να γνωρίζει τις προσβάσεις που πραγματοποιούνται για τις κινήσεις των καρτών του μέσω της διαδικτυακής αυτής υπηρεσίας - με αποτέλεσμα να υφίσταται κίνδυνος συνεχών παράνομων προσβάσεων σε μόνιμη βάση και για πολύ μεγάλα χρονικά διαστήματα, χωρίς αυτό να γίνεται αντιληπτό. Συνεπώς, για την πρόσβαση στα δεδομένα που παρέχει η υπηρεσία θα πρέπει να είναι σε εφαρμογή ισχυροί μηχανισμοί αυθεντικοποίησης των χρηστών αυτής.

Ο υπάρχων μηχανισμός αυθεντικοποίησης βασίζεται κατά κύριο λόγο σε στοιχεία που αναγράφονται επάνω στην πιστωτική κάρτα, καθώς και στην ημερομηνία γέννησης του κατόχου τους, ενώ επιπροσθέτως, όπως αναφέρει ο υπεύθυνος επεξεργασίας στο υπόμνημά του, το σύστημα δεν επιτρέπει την πρόσβαση στην τρίτη αποτυχημένη προσπάθεια. Τα ανωτέρω όμως δεν μπορούν να θεωρηθούν επαρκής μηχανισμός για την πιστοποίηση της ταυτότητας του χρήστη της υπηρεσίας για τους κάτωθι λόγους: α) τα στοιχεία που αναγράφονται επάνω στην κάρτα μπορούν να τεθούν σε γνώση οποιουδήποτε τρίτου στον οποίο δίνεται η δυνατότητα να έχει φυσική πρόσβαση στην κάρτα έστω και για λίγα δευτερόλεπτα (π.χ. έμπορος/πωλητής σε κατάστημα, άτομο του στενού

οικογενειακού/φιλικού περιβάλλοντος του κατόχου κτλ.), β) η ημερομηνία γέννησης του κατόχου της κάρτας μπορεί να είναι ήδη γνωστή σε κάποιον τρίτο (π.χ. σε άτομο του στενού περιβάλλοντος) ή σε ορισμένες περιπτώσεις μπορεί να ευρεθεί από το Διαδίκτυο (π.χ. από κάποια διαδικτυακή υπηρεσία κοινωνικής δικτύωσης ή από δημόσια προσβάσιμη διαδικτυακή πηγή[2]). Επιπλέον, η ημερομηνία γέννησης εμφανίζεται και σε έγγραφα στα οποία δύναται να έχει, έστω και προσωρινά, νόμιμη πρόσβαση κάποιος τρίτος ο οποίος θα μπορούσε επίσης να έχει ταυτόχρονα προσωρινή πρόσβαση και στην πιστωτική κάρτα (για παράδειγμα, τέτοιο έγγραφο είναι η άδεια οδήγησης, η οποία μπορεί να επιδοθεί, μαζί με την πιστωτική κάρτα, σε κατάστημα ενοικίασης αυτοκινήτων).

Ως εκ τούτου, ο μηχανισμός αυθεντικοποίησης των χρηστών της υπηρεσίας «Winbank for cards» που έχει επιλέξει ο υπεύθυνος επεξεργασίας δεν είναι επαρκής, λαμβάνοντας υπόψη τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των υπό επεξεργασία δεδομένων. Άλλωστε, το γεγονός ότι δεν υπήρξε ποτέ, προς τον υπεύθυνο επεξεργασίας, διαμαρτυρία από πελάτη του για παραβίαση δεδομένων προσωπικού χαρακτήρα δεν συνεπάγεται ότι τέτοια παραβίαση δεν έλαβε χώρα, ακριβώς γιατί οι ως άνω παράνομες προσβάσεις που περιγράφονται δεν μπορούν να γίνουν αντιληπτές.

Κατά συνέπεια, για τη συγκεκριμένη επεξεργασία δεν πληρούνται οι προϋποθέσεις του άρθρου 10 του ν. 2472/1997.

6. Ενόψει των παραβάσεων που διαπιστώθηκαν, και λαμβάνοντας υπόψη και τις διεθνείς πιστοποιήσεις ασφαλείας πού έχει λάβει ο υπεύθυνος επεξεργασίας, η Αρχή κρίνει ότι πρέπει να επιβληθεί στον υπεύθυνο επεξεργασίας η προβλεπόμενη στο άρθρο 21 παρ. 1 στοιχ. α΄ του ν. 2472/1997 κύρωση της προειδοποίησης όσον αφορά στη μη λήψη σαφούς, ρητής και ειδικής συγκατάθεσης των πελατών του για τη διαδικτυακή υπηρεσία «winbank for cards», καθώς και για τη μη λήψη των ενδεδειγμένων μέτρων ασφαλείας κατά την επεξεργασία προσωπικών δεδομένων μέσω της συγκεκριμένης διαδικτυακής εφαρμογής, ήτοι για το μη ισχυρό μηχανισμό αυθεντικοποίησης των χρηστών αυτής.

Ειδικότερα, για την υπηρεσία “winbank for cards”, ο υπεύθυνος επεξεργασίας θα πρέπει να πράξει τα κάτωθι:

α) Να διασφαλίσει ότι, για τους νέους πελάτες-κατόχους πιστωτικών καρτών, η υπηρεσία «Winbank for cards» θα παρέχεται μόνο εφόσον δηλώσουν ρητώς και ειδικώς ότι την επιθυμούν (σύστημα «opt-in»), αφού προηγουμένως ενημερωθούν για τα βασικά

[2] Για παράδειγμα, η ημερομηνία γέννησης προκύπτει άμεσα από τον Αριθμό Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), ο οποίος μπορεί να εμφανίζεται σε έγγραφο ανηρτημένο στον ιστοτόπο ΔΙΑΥΓΕΙΑ ή στον ιστοτόπο του Α.Σ.Ε.Π.

χαρακτηριστικά αυτής. Η δήλωση συγκατάθεσης θα πρέπει να παρέχεται από τους πελάτες, με φυσική τους παρουσία, σε κατάστημα της Τράπεζας ή ηλεκτρονικά, με τρόπο τέτοιο που να διασφαλίζεται η πιστοποίηση της ταυτότητας του αιτούντος. Επισημαίνεται ιδιαίτερα ότι η υπογραφή από τον πελάτη της σύμβασης χορήγησης πιστωτικής κάρτας δεν συνεπάγεται αυτόματα την αποδοχή χρήσης της εν λόγω υπηρεσίας, γιατί δεν πιστοποιείται ότι τηρήθηκαν τα ανωτέρω.

β) Να φροντίσει αμελλητί, για τους νυν πελάτες-κατόχους πιστωτικών καρτών της Τράπεζας, που δεν έχουν δηλώσει την αντίρρησή τους για την εν λόγω υπηρεσία, να υπάρξει ατομική ενημέρωση σχετικά με την υπηρεσία «Winbank for cards» (μέσω ταχυδρομικής επιστολής, μηνύματος ηλεκτρονικού ταχυδρομείου ή σύντομου γραπτού μηνύματος SMS), στην οποία ενημέρωση θα αναφέρεται ότι η υπηρεσία είναι ήδη ενεργή, θα περιγράφονται τα χαρακτηριστικά αυτής αλλά και ο τρόπος με τον οποίο μπορεί κάποιος να ζητήσει τη διακοπή της.

γ) Να τροποποιήσει, εντός τριών μηνών, την υπηρεσία «Winbank for cards» ως προς τα μέτρα ασφάλειας αυτής, έτσι ώστε να υλοποιείται στο πλαίσιο αυτής ισχυρός μηχανισμός αυθεντικοποίησης των χρηστών της. Προς τούτο σημειώνεται ότι, για την αυθεντικοποίηση θα πρέπει να απαιτείται κωδικός πρόσβασης (συνθηματικό) από τον κάθε χρήστη (είτε ένα γενικό συνθηματικό είτε συνθηματικό μιας χρήσης), κατά τρόπο τέτοιο ώστε αυτό να είναι εις γνώσιν μόνο του ιδίου. Η χορήγηση αυτού στο χρήστη θα γίνεται κατόπιν αίτησής του, η οποία αυτομάτως θα υπέχει και θέση δήλωσης συγκατάθεσης για την επεξεργασία προσωπικών δεδομένων μέσω της εν λόγω υπηρεσίας.

δ) Να διασφαλίζει ότι, για κάθε τυχόν μελλοντική τροποποίηση της εν λόγω υπηρεσίας, θα παρέχεται πρόσφορη σχετική ενημέρωση στους χρήστες αυτής (για παράδειγμα, μέσω αναδυόμενου ηλεκτρονικού μηνύματος κατά τη σύνδεσή τους).

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

Απευθύνει, με βάση το άρθρο 21 παρ. 1 στοιχ. α' του ν. 2472/1997, προειδοποίηση στην Τράπεζα Πειραιώς, ως υπεύθυνο επεξεργασίας, για παραβίαση του άρθρου 5 του ν. 2472/1997 και για την παραβίαση του άρθρου 10 του ν. 2472/1997, αναφορικά με την επεξεργασία προσωπικών δεδομένων μέσω της διαδικτυακής υπηρεσίας «winbank for cards».

Καλεί την Τράπεζα Πειραιώς να λάβει τα κατάλληλα μέτρα για τη νόμιμη επεξεργασία

προσωπικών δεδομένων των πελατών της μέσω της διαδικτυακής υπηρεσίας «winbank for cards», όπως αυτά περιγράφονται στο σημείο 6 του σκεπτικού της παρούσας, καθώς επίσης και να ενημερώσει σχετικώς την Αρχή για την τήρηση των ανωτέρω.

Ο Πρόεδρος	**Η γραμματέας**
Πέτρος Χριστόφορος	**Ειρήνη Παπαγεωργοπούλου**