ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 08-06-2018
Αριθ. Πρωτ.: Γ/ΕΞ/4986/08-06-2018

Α Π Ο Φ Α Σ Η ΑΡ. 48/2018

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε στην έδρα της την 24/04/2018 και ώρα 10:00 μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος της Αρχής, Κωνσταντίνος Μενουδάκος και τα τακτικά μέλη της Αρχής Κωνσταντίνος Χριστοδούλου, Αντώνιος Συμβώνης, ως εισηγητής, Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, Χαράλαμπος Ανθόπουλος και Ελένη Μαρτσούκου. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, ο Κωνσταντίνος Λιμνιώτης, πληροφορικός ελεγκτής, ως βοηθός εισηγητή, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η Δ/νση Προστασίας Καταναλωτή του Υπουργείου Οικονομίας, Υποδομών, Ναυτιλίας και Τουρισμού διαβίβασε στην Αρχή, με το υπ' αριθμ. πρωτ. … και με ημερομηνία … έγγραφό της (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/2819/18-05-2015) την καταγγελία – με όλα τα συμπληρωματικά και σχετικά έγγραφα– του Α κατά της Εθνικής Τράπεζας της Ελλάδος ΑΕ –εφεξής, Εθνική Τράπεζα– αναφορικά με τη χρεωστική (debit) κάρτα που η Τράπεζα χορήγησε στις … στον καταγγέλλοντα πελάτη της, προς αντικατάσταση της παλαιάς του κάρτας. Η νέα αυτή κάρτα υποστηρίζει ανέπαφες (contactless) συναλλαγές – δηλαδή συναλλαγές που μπορούν να πραγματοποιηθούν χωρίς την εισαγωγή PIN από μεριάς του, παρά μόνο με επίδειξη της κάρτας, χωρίς επαφή ή τοποθέτηση, στην

αντίστοιχη συσκευή-«αναγνώστη» (reader), εφόσον η οικονομική συναλλαγή δεν ξεπερνάει το ύψος των εικοσιπέντε (25) Ευρώ. Ο καταγγέλλων ισχυρίζεται ότι δεν έδωσε την έγκρισή του προκειμένου να του χορηγηθεί χρεωστική κάρτα με αυτά τα χαρακτηριστικά (ήτοι ανέπαφη), καθώς επίσης και ότι δεν επιθυμεί να διαθέτει τέτοια κάρτα λόγω κινδύνων ασφάλειας που πηγάζουν από τη χρήση της. Στο ως άνω έγγραφο επισυνάπτεται επίσης και το έγγραφο που η Εθνική Τράπεζα απέστειλε στον καταγγέλλοντα στις …, σε απάντηση της έγγραφης αντίρρησής του που εξέφρασε προς την Τράπεζα για τη λήψη της κάρτας, στο οποίο έγγραφο αναφέρεται μεταξύ άλλων ότι η δυνατότητα χρήσης της DebitMasterCard τεχνολογίας ανέπαφων συναλλαγών για αγορές αξίας μικρότερης των 25 Ευρώ χωρίς τη χρήση PIN είναι ένα υποχρεωτικό χαρακτηριστικό της κάρτας σύμφωνα με τις οδηγίες του διεθνούς οργανισμού Mastercard. Αναφέρει επίσης η Εθνική Τράπεζα στην ως άνω απάντησή της ότι η νέα κάρτα πληροί όλες τις δικλείδες ασφαλείας που προβλέπουν οι διεθνείς οργανισμοί, καθώς επίσης και ότι η αντικατάσταση της παλαιάς κάρτας με τη νέα ανέπαφη κάρτα είναι σύμφωνη με τους όρους της σύμβασης με τον καταγγέλλοντα πελάτη της ως προς τη χρεωστική του κάρτα – συγκεκριμένα, παραπέμπει στον όρο 2 της μεταξύ τους σύμβασης, στον οποίο αναφέρεται ότι «η κάρτα στην οποία είναι αποτυπωμένο το όνομα του κατόχου ανήκει και παραμένει στην κυριότητα της Τράπεζας», καθώς και στον όρο 12 όπου αναφέρεται ότι «λόγω της αόριστης διάρκειας της παρούσας σύμβασης, η Τράπεζα διατηρεί το δικαίωμα μονομερούς συμπλήρωσης ή και τροποποίησης των όρων της σύμβασης για σπουδαίο λόγο». Περαιτέρω, επισημαίνεται στο εν λόγω έγγραφο ότι ο καταγγέλλων έχει τη δυνατότητα να αιτηθεί τη μεταβολή του ημερησίου ορίου αγορών του σε μηδέν (0) Ευρώ. Το εν λόγω έγγραφο διαβίβασε η Εθνική Τράπεζα στη Δ/νση Προστασίας Καταναλωτή, σε απάντησή σχετικού εγγράφου της Δ/νσης για τις απόψεις της Τράπεζας επί της καταγγελίας.

Η ίδια καταγγελία, με όλα τα συμπληρωματικά και σχετικά έγγραφα του φακέλου, διαβιβάστηκε στην Αρχή και από το Συνήγορο του Καταναλωτή με το με αρ. πρωτ. … και από … έγγραφό του (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/3198/05-06-2015). Σε σχετικό έγγραφο του Συνηγόρου του Καταναλωτή, η Εθνική Τράπεζα απάντησε διαβιβάζοντάς του την ως άνω αναφερθείσα απάντησή της προς τον καταγγέλλοντα. Ο Συνήγορος του Καταναλωτή ενημέρωσε σχετικώς τον καταγγέλλοντα, ο οποίος απάντησε στο Συνήγορο λέγοντας ότι υπάρχουν εγγενείς αδυναμίες της τεχνολογίας RFID –τεχνολογία που χρησιμοποιείται στις ανέπαφες κάρτες– ως προς την ασφάλεια, καθώς επίσης και ότι το κόστος αγοράς εξοπλισμού για αξιοποίηση αυτών των αδυναμιών δεν είναι μεγάλο, παραπέμποντας σε

αντίστοιχους διαδικτυακούς συνδέσμους[1] με σχετικές πληροφορίες, ενώ επίσης ζήτησε να κοινοποιηθεί η καταγγελία του, διά του Συνηγόρου, στην Αρχή.

Σημειώνεται επίσης ότι ο Συνήγορος του Καταναλωτή, με το με αρ. πρωτ. … και από … έγγραφό του το οποίο κοινοποίησε στην Αρχή (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/3444/16-06-2015) ενημέρωσε και την Τράπεζα της Ελλάδος για την εν λόγω καταγγελία, διαβιβάζοντάς της το σύνολο των εγγράφων του φακέλου της υπόθεσης.

Η Αρχή, στο πλαίσιο εξέτασης της εν λόγω καταγγελίας, απέστειλε στην Εθνική Τράπεζα το υπ' αριθμ. πρωτ. Γ/ΕΞ/2819-1/05-06-2015 έγγραφο, με το οποίο ζήτησε τις απόψεις της Τράπεζας επί της καταγγελίας, θέτοντας ειδικότερα και τα εξής ερωτήματα: α) Τι είδους δεδομένα τηρούνται στο chip της εν λόγω κάρτας, καθώς και ποια από αυτά αποστέλλονται στην αντίστοιχη συσκευή-«αναγνώστη» κατά τη διαδικασία χρέωσης του λογαριασμού του κατόχου της μέσω ανέπαφης συναλλαγής, β) τι είδους τεχνικά μέτρα είναι σε εφαρμογή για την προστασία των δεδομένων αυτών (τόσο αυτών που τηρούνται στην κάρτα όσο και αυτών που μεταδίδονται κατά την ανέπαφη συναλλαγή με τη συσκευή-«αναγνώστη»), γ) αν παρέχει στους πελάτες της τη δυνατότητα μη χορήγησής της ή πλήρους απενεργοποίησης του χαρακτηριστικού εκείνου της κάρτας που επιτρέπει την πραγματοποίηση ανέπαφων συναλλαγών. Ακολούθως, δεδομένου ότι παρήλθε διάστημα πλέον των δύο (2) μηνών χωρίς απάντηση, η Αρχή απέστειλε εκ νέου στην Εθνική Τράπεζα το υπ' αριθμ. πρωτ. Γ/ΕΞ/2819-2/16-09-2015 έγγραφο με το οποίο την καλούσε εκ νέου να υποβάλει τις απόψεις της και τις απαραίτητες διευκρινίσεις εντός δεκαπέντε (15) ημερών. Κατόπιν αυτού, η Εθνική Τράπεζα (και, ειδικότερα, η Δ/νση Κανονιστικής Συμμόρφωσης και Εταιρικής Διακυβέρνησης της Τράπεζας & του Ομίλου) απέστειλε στην Αρχή το υπ' αριθμ. πρωτ. …/… έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/5102/06-10-2015), στο οποίο επισημαίνει, μεταξύ άλλων ότι η Τράπεζα έχει υιοθετήσει την τεχνολογία ανέπαφων συναλλαγών της MasterCard, κατά την οποία η κάρτα MasterCard είναι εξοπλισμένη με ένα τσιπ και μία κεραία. Για αγορές μέχρι των 25 Ευρώ δεν απαιτείται ο κάτοχός της να εισάγει PIN – η πληρωμή πραγματοποιείται αυτόματα προσεγγίζοντας την κάρτα στο τερματικό, χωρίς να πρέπει να παραδοθεί στον ταμία. Το όριο των 25 Ευρώ έχει τεθεί από το διεθνή οργανισμό MasterCard ως προδιαγραφή του τερματικού και όχι ως χαρακτηριστικό της κάρτας, δεν δύναται να τροποποιηθεί και ισχύει σε όλη την Ευρώπη. Στο ίδιο έγγραφο επίσης αναφέρεται ότι η τεχνολογία των ανέπαφων συναλλαγών, η οποία βασίζεται στην ασύρματη τεχνολογία μικρής εμβέλειας NFC (Near Field Communication)

[1] Συγκεκριμένα, στους συνδέσμους https://greek1.blogspot.gr/2015/04/rfid.html#axzzEY1OR57oH και http://www.ebay.com/bhp/rfid-reader-writer-usb.

εφαρμόζεται ήδη σε πενήντα έξι (56) χώρες σε όλο τον κόσμο και σε είκοσι εννέα (29) χώρες στην Ευρώπη, είναι το ίδιο ασφαλής με την πιστωτική κάρτα MasterCard, ενώ αντίστοιχη τεχνολογία διατίθεται και από τη Visa.

Ως προς τα ειδικότερα ερωτήματα που είχε θέσει η Αρχή, η Εθνική Τράπεζα με το ως άνω έγγραφό της αναφέρει τα εξής:

α) Στο chip της κάρτας, εκτός από τις τεχνικές πληροφορίες που αφορούν την επικοινωνία της κάρτας με το τερματικό, τηρούνται ο αριθμός της κάρτας, η ημερομηνία λήξης της, το ονοματεπώνυμο του κατόχου της και το PIN σε κρυπτογραφημένη μορφή.

β) Τα κρυπτογραφικά κλειδιά για την προστασία (κρυπτογράφηση) των τηρούμενων δεδομένων τηρούνται μόνο από τον εκδότη της κάρτας, δηλαδή την Τράπεζα. Τα στοιχεία που αποστέλλονται κατά τη διενέργεια της ανέπαφης συναλλαγής είναι μόνο ο αριθμός της κάρτας και η ημερομηνία λήξης αυτής, καθώς και άλλες αποκλειστικά τεχνικές πληροφορίες για την ολοκλήρωση της συναλλαγής. Σε περιπτώσεις στις οποίες ο κάτοχος της κάρτας εισάγει PIN, αυτό πάντα κρυπτογραφείται προκειμένου να αποσταλεί για έλεγχο στον εκδότη.

γ) Δεδομένου ότι η τεχνολογία ανέπαφης συναλλαγής είναι τεχνικό χαρακτηριστικό της κάρτας, η Τράπεζα δεν μπορεί να επεμβαίνει στη λειτουργία της. Εναπόκειται στην ευχέρεια του κατόχου της να δηλώνει στον υπάλληλο της επιχείρησης με την οποία συναλλάσσεται ότι επιθυμεί να διενεργήσει τη συναλλαγή με χρήση PIN. Επίσης, ο κάτοχός της μπορεί να μεταβάλλει οποτεδήποτε το επιτρεπτό όριο για συναλλαγές μέσω κάρτας.

Τέλος, η Τράπεζα παρέχει και πρόσθετες πληροφορίες περί της ασφάλειας της επεξεργασίας, σημειώνοντας ότι με την ανέπαφη συναλλαγή δεν απομακρύνεται η κάρτα από τα χέρια του κατόχου της, καθώς επίσης και ότι δεν είναι δυνατόν να πραγματοποιηθεί κατά λάθος ανέπαφη συναλλαγή γιατί η κάρτα ενεργοποιείται αποκλειστικά και μόνο εάν ο κάτοχός της την πλησιάσει σε τερματικό σε απόσταση μικρότερη των 5 cm ενώ θα πρέπει να έχει ολοκληρωθεί και η σχετική διαδικασία στην ταμειακή μηχανή της επιχείρησης, ούτε υπάρχει ο κίνδυνος διπλής ή/και πολλαπλής χρέωσης. Επίσης, τυχόν δόλιες συναλλαγές, οι οποίες σύμφωνα με τα στατιστικά στοιχεία είναι μηδαμινές, μπορούν να αμφισβητηθούν από τον κάτοχο με την ίδια διαδικασία που ακολουθείται και στις συναλλαγές με πιστωτικές ή χρεωστικές κάρτες με χρήση PIN. Περαιτέρω, ο κάθε κάτοχος κάρτας πρέπει να λαμβάνει κάθε δυνατή πρόνοια για την ασφαλή φύλαξη της κάρτας του, ενώ η Τράπεζα παρέχει 24ωρη τηλεφωνική γραμμή εξυπηρέτησης για τυχόν δήλωση απώλειας ή κλοπής αυτής, ενώ επίσης υπάρχει και ειδική ομάδα που παρακολουθεί με

εξειδικευμένο λογισμικό όλες τις ηλεκτρονικές συναλλαγές, σε πραγματικό χρόνο, επί εικοσιτετράωρης βάσης, στο πλαίσιο ελέγχου, πρόληψης και καταστολής της ηλεκτρονικής απάτης. Τέλος, επισημαίνεται ότι οι δυνατότητες των καρτών για ανέπαφες συναλλαγές έχουν τεθεί βάσει προδιαγραφών διεθνών οργανισμών, επομένως δεν υπάρχει η δυνατότητα παρέκκλισης και ως εκ τούτου δεν υφίσταται πλέον η διάθεση των παλαιών χρεωστικών καρτών.

Στη συνέχεια, η Αρχή απέστειλε στην Εθνική Τράπεζα το υπ' αριθμ. πρωτ. Γ/ΕΞ/2819-3/30-10-2015 έγγραφο –και ακολούθως, λόγω μη λήψης απάντησης, το υπ' αριθμ. πρωτ. Γ/ΕΞ/663/05-02-2016 έγγραφο– προκειμένου να παρασχεθούν πρόσθετες διευκρινίσεις. Ειδικότερα, λαμβάνοντας υπόψη ότι κατά τη διενέργεια ανέπαφης συναλλαγής αποστέλλονται μη κρυπτογραφημένα ο αριθμός της κάρτας και η ημερομηνία λήξης αυτής, η Αρχή ζήτησε να τεκμηριωθούν επακριβώς οι λόγοι για τους οποίους δεν είναι εφικτή η απενεργοποίηση του χαρακτηριστικού εκείνου της κάρτας που επιτρέπει την πραγματοποίηση ανέπαφων συναλλαγών, σε περίπτωση που κάποιος πελάτης αιτηθεί μία τέτοια απενεργοποίηση, σημειώνοντας ότι, εφόσον η συγκεκριμένη λειτουργία άπτεται της τεχνικής υλοποίησης της κάρτας και δεν είναι η Τράπεζα σε θέση να απαντήσει, θα πρέπει να απευθυνθεί σχετικώς στον αρμόδιο φορέα (MasterCard ή και όποιον άλλον ενδεχομένως κρίνει η Τράπεζα απαραίτητο) προκειμένου να υπάρξει η σχετική τεκμηρίωση. Επίσης, η Αρχή ζήτησε να διαβιβαστεί οποιαδήποτε έγγραφη τεκμηρίωση διαθέτει η Τράπεζα που καταδεικνύει ότι λήφθηκαν υπόψη ζητήματα προστασίας προσωπικών δεδομένων ήδη κατά το σχεδιασμό της κάρτας (π.χ. μελέτη επιπτώσεων στην προστασία προσωπικών δεδομένων - Data Protection Impact Assessment - DPIA).

Σε απάντηση αυτού, η Εθνική Τράπεζα απέστειλε στην Αρχή το υπ' αριθμ. πρωτ. … και από … έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/1282/26-02-2016), στο οποίο επισυνάπτεται και η από … απάντηση της MasterCard προς την Τράπεζα. Όπως επισημαίνεται στο έγγραφο της MasterCard, οι εκδότες έχουν τη δυνατότητα να προσφέρουν στους κατόχους καρτών την επιλογή μεταξύ ανέπαφων ή συμβατικών τρόπων πληρωμής, ενώ επίσης η ενεργοποίηση και απενεργοποίηση του προφίλ που επιτρέπει τη διενέργεια ανέπαφων συναλλαγών είναι εφικτή μετά την έκδοση της κάρτας - δηλαδή, ο εκδότης δύναται να αποφασίσει αν θα ενεργοποιήσει την ανέπαφη διασύνδεση ή όχι για μία συγκεκριμένη κάρτα. Προς τούτο, η Εθνική Τράπεζα επισημαίνει στο ως άνω έγγραφό της ότι η απενεργοποίηση του προφίλ που επιτρέπει τη διενέργεια ανέπαφων συναλλαγών σε συγκεκριμένες κάρτες μετά την έκδοσή τους προϋποθέτει την υιοθέτηση διαφορετικής πολιτικής εξουσιοδοτήσεων για συγκεκριμένες κάρτες, η οποία απαιτεί πολύπλοκες και

τεχνικές μεταβολές και αναβαθμίσεις. Ως εκ τούτου, το σχετικό έργο επελέγη να μην υποστηριχθεί συστημικά από την Τράπεζα, δεδομένου ότι ο κάθε χρήστης διατηρεί την ευχέρεια να χρησιμοποιεί ή να μη χρησιμοποιεί κατά περίπτωση το συγκεκριμένο προφίλ. Συνεπώς, η ανέπαφη διασύνδεση αποτελεί εξ ορισμού (by default) χαρακτηριστικό των νέων χρεωστικών καρτών, ενώ δεν υποστηρίζεται συστημικά –και, ως εκ τούτου, δεν παρέχεται– διαφορετικό προϊόν (μη ανέπαφη κάρτα). Τέλος, στο ως άνω έγγραφο της MasterCard επισημαίνεται ότι έχει διενεργηθεί διεξοδική εκτίμηση επιπτώσεων στην ιδιωτικότητα (Privacy Impact Assessment) για το προϊόν ανέπαφων συναλλαγών, με βάση το αντίστοιχο πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID[2] (Privacy and Data Protection Impact Assessment Framework for RFID Applications) της Ε.Ε., ημερομηνίας 12-01-2011. Η εκτίμηση υποβλήθηκε σε ρυθμιστικές αρχές της Ευρώπης: οι γερμανικές ρυθμιστικές αρχές έμειναν απολύτως ικανοποιημένες και έκλεισαν την υπόθεση, ενώ οι ρυθμιστικές αρχές άλλων χωρών της ΕΕ όπως οι αρχές της Γαλλίας, της Ελβετίας και της Πολωνίας κατέληξαν στο συμπέρασμα ότι η εν λόγω τεχνολογία δεν εγείρει ζητήματα ιδιωτικής ζωής και προστασίας προσωπικών δεδομένων.

Δεύτερη συναφής καταγγελία διαβιβάστηκε στην Αρχή από το Συνήγορο του Καταναλωτή. Συγκεκριμένα, με το με αρ. πρωτ. … και από … έγγραφό του (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/1102/22-02-2016) διαβίβασε καταγγελία, μαζί με όλα τα σχετικά έγγραφα του φακέλου, του Β κατά της Τράπεζας Πειραιώς Α.Ε. –εφεξής, Τράπεζα Πειραιώς– με την οποία διαμαρτύρεται για την αλλαγή της χρεωστικής του κάρτας με νέα κάρτα με δυνατότητα για ανέπαφες συναλλαγών (όπως και στην προηγούμενη περίπτωση, μπορούν να πραγματοποιηθούν αγορές μέχρι είκοσι πέντε (25) Ευρώ χωρίς εισαγωγή PIN, με ανέπαφο τρόπο). Στο ως άνω έγγραφο επισυνάπτεται επίσης και το με αρ. πρωτ. … και από … έγγραφο που η Τράπεζα Πειραιώς απέστειλε στον καταγγέλλοντα και στο Συνήγορο του Καταναλωτή, σε απάντηση της έγγραφης αντίρρησης του καταγγέλλοντος προς την Τράπεζα. Στο έγγραφο αυτό της Τράπεζας Πειραιώς επισημαίνεται ότι οι ανέπαφες συναλλαγές έχουν καθιερωθεί ως ο βασικός εναλλακτικός τρόπος πληρωμής παγκοσμίως, ειδικά για αγορές μικρής αξίας, που μπορούν να πραγματοποιούνται γρήγορα και με ασφάλεια, χωρίς η κάρτα να απομακρύνεται από τα χέρια του κατόχου. Ως εκ τούτου, όπως αναφέρει η Τράπεζα στο έγγραφό της, το αίτημα του καταγγέλλοντος σχετικά με την υποχρεωτική εισαγωγή PIN σε κάθε συναλλαγή μέσω κάρτας δεν μπορεί να

[2] Σημειώνεται ότι πρόκειται για το Παράρτημα της Γνώμης 9/2011 της Ομάδας Εργασίας του Άρθρου 29 για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

ικανοποιηθεί. Περαιτέρω, στο ως άνω έγγραφο επισυνάπτεται και νεότερο έγγραφο του καταγγέλλοντος προς στο Συνήγορο του Καταναλωτή, στο οποίο παρατίθεται σειρά από διαδικτυακούς συνδέσμους[3] με πληροφορίες σχετικές με τα ζητήματα ασφάλειας που εγείρονται από τη χρήση κάρτας για ανέπαφες συναλλαγές, καθώς επίσης και το με αρ. πρωτ. … και από … έγγραφο του Συνηγόρου του Καταναλωτή προς την Τράπεζα της Ελλάδος, με την οποία –κατ' αναλογία με την προηγούμενη συναφή καταγγελία του Α– την ενημέρωσε και για την εν λόγω καταγγελία, διαβιβάζοντάς της το σύνολο των εγγράφων του φακέλου της υπόθεσης.

Η Αρχή, στο πλαίσιο εξέτασης της εν λόγω καταγγελίας, απέστειλε στην Τράπεζα Πειραιώς το υπ' αριθμ. πρωτ. Γ/ΕΞ/1102-1/18-04-2016 έγγραφο, με το οποίο ζητούσε τις απόψεις της επί των καταγγελλομένων, θέτοντας εκ νέου και τα ειδικότερα ερωτήματα που είχε απευθύνει, με τα προηγούμενα έγγραφά της, και στην Εθνική Τράπεζα. Ακολούθως η Τράπεζα Πειραιώς απάντησε με το υπ' αριθμ. πρωτ. … και από … έγγραφο (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/4118/29-06-2016), στο οποίο αναφέρει ότι η Τράπεζα, ως μέλος των διεθνών οργανισμών Visa και MasterCard, αλλά και βάσει της πιστοποίησης κατά το πρότυπο PCI/DSS (Payment Card Industry Data Security Standard) που διαθέτει ακολουθεί και εφαρμόζει πρωτόκολλα και διαδικασίες προκειμένου να καλύπτουν τις σύγχρονες ανάγκες και τεχνολογικές εξελίξεις. Παράλληλα, κάθε νέο προϊόν που φτάνει στο τελικό στάδιο της εμπορικής του διάθεσης έχει περάσει από όλα τα απαιτούμενα στάδια ελέγχου ώστε να λάβει τις αντίστοιχες πιστοποιήσεις από Οργανισμούς. Επιπλέον, η Τράπεζα για το σύνολο των συναλλαγών με κάρτες πραγματοποιεί συνεχείς ελέγχους για την ασφάλεια των πελατών σε 24ωρη βάση και όλες τις ημέρες του χρόνου. Οι εν λόγω έλεγχοι αφορούν τόσο τις κλασικές όσο και τις ανέπαφες συναλλαγές. Σε ό,τι αφορά στο αίτημα του πελάτη για απενεργοποίηση του ορίου των εικοσιπέντε (25) Ευρώ για ανέπαφες συναλλαγές χωρίς τη χρήση PIN, αυτό δεν είναι εφικτό να πραγματοποιηθεί δεδομένου ότι το συγκεκριμένο όριο ορίζεται από τους οργανισμούς Visa και MasterCard και αφορά τα δεδομένα υποδοχής των καρτών και όχι τις κάρτες. Επίσης η Τράπεζα αναφέρει ότι στόχος της συγκεκριμένης τεχνολογίας, η οποία χρησιμοποιείται διεθνώς, είναι η ευκολία χρήσης και η μείωση του χρόνου διεκπεραίωσης των συναλλαγών, καθώς επίσης και ότι, εφόσον ο πελάτης το επιθυμεί, έχει τη δυνατότητα να ζητήσει από τον υπάλληλο εξυπηρέτησης του καταστήματος να μην πραγματοποιήσει τη συναλλαγή ανέπαφα αλλά με εισαγωγή PIN,

[3] Συγκεκριμένα, οι σύνδεσμοι είναι http://makpress.blogspot.gr/2015/07/contactless.html, http://thesecretrealtruth.blogspot.com/2015/08/contactless.html, http://www.telegraph.co.uk/technology/internet-security/11758990/Contactless-cards-at-risk-of-fraud-warns-Which.html και http://www.theweek.co.uk/prosper/53317/contactless-cards-what-are-risks.

ακόμα και για αγορές μικρότερης αξίας από 25 Ευρώ. Η Τράπεζα Πειραιώς στο ίδιο έγγραφο αναφέρει επίσης τους αντίστοιχους ισχυρισμούς που είχε επικαλεστεί και η Εθνική Τράπεζα αναφορικά με το ότι δεν είναι δυνατόν να γίνει διπλή χρέωση ή χρέωση κατά λάθος με απλή διέλευση πλησίον του μηχανήματος υποδοχής, ότι για την πραγματοποίηση ανέπαφης συναλλαγής η κάρτα θα πρέπει να πλησιάσει σε απόσταση μικρότερη των 8 cm στο μηχάνημα υποδοχής και να παραμείνει κοντά σε αυτό για διάστημα αρκετό ώστε να ακουστεί ο χαρακτηριστικός ήχος, καθώς επίσης ότι ο πελάτης, όντας υπεύθυνος για τη φύλαξη και τη φύλαξη της κάρτας του –όπως και κάθε άλλης κάρτας, για ανέπαφες συναλλαγές ή όχι– θα πρέπει να λαμβάνει όλα τα προσήκοντα μέτρα ορθής χρήσης και προστασίας. Ως προς είδος των δεδομένων που τηρούνται στο chip της κάρτας, η Τράπεζα Πειραιώς αναφέρει στο έγγραφό της ότι αφορούν στοιχεία κοινά σε όλες τις χρεωστικές κάρτες, καθώς και στοιχεία που αφορούν τον εκάστοτε πελάτη (χωρίς να προσδιορίζει επακριβώς ποια είναι τα στοιχεία αυτά). Τέλος, η Τράπεζα Πειραιώς αναφέρει ότι ο καταγγέλλων, με την παραλαβή του νέου πλαστικού της κάρτας του λόγω λήξης της παλιάς, έλαβε και συνοδευτική επιστολή η οποία τον ενημέρωνε για τα χαρακτηριστικά της καθώς και για τη νέα τεχνολογία ανέπαφων συναλλαγών. Για τις περιπτώσεις έκδοσης νέων καρτών, οι πελάτες ενημερώνονται για την τεχνολογία ανέπαφων συναλλαγών, τις οποίες υποστηρίζουν οι κάρτες, μέσω της σύμβασης που υπογράφουν, αντίγραφο της οποίας και παραλαμβάνουν.

Σε συνέχεια των ανωτέρω, κατόπιν ειδικού προς τούτο ελέγχου που πραγματοποιήθηκε από υπαλλήλους της Αρχής στις 20-09-2016 μέσω της ελεύθερα διαθέσιμης εφαρμογής λογισμικού Credit Card Reader v.4.2.2 που διατίθεται για το λειτουργικό σύστημα Android, διαπιστώθηκε ότι τα δεδομένα που αποστέλλει μία ανέπαφη κάρτα MasterCard κατά την ανέπαφη λειτουργία της είναι πράγματι ο αριθμός της κάρτας και η ημερομηνία λήξης, αλλά επιπροσθέτως αποστέλλονται –επίσης μη κρυπτογραφημένα– στοιχεία που αφορούν πρόσφατες κινήσεις της κάρτας, ήτοι ημερομηνία της κίνησης και ύψος χρηματικού ποσού αυτής. Ο ίδιος έλεγχος, με την ίδια εφαρμογή λογισμικού, για τα δεδομένα που αποστέλλονται ανέπαφα από κάρτες VISA, δεν κατέδειξε την αποστολή των ως άνω δεδομένων κινήσεων της κάρτας (φαίνεται ότι, κατά τη λειτουργία ανέπαφων καρτών VISA, αποστέλλονται ο αριθμός της κάρτας και η ημερομηνία λήξης αυτής).

Βάσει της ανωτέρω διαπίστωσης, η Αρχή απέστειλε στη Mastercard Ελλάδος την υπ' αριθμ. πρωτ. Γ/ΕΞ/6148/06-10-2016 επιστολή, με την οποία ζητήθηκαν οι απόψεις της επί της ανωτέρω παρατήρησης ως προς τα δεδομένα πρόσφατων κινήσεων/συναλλαγών

που μεταδίδονται ανέπαφα. Με το ίδιο έγγραφο η Αρχή ρώτησε αν τα εν λόγω χαρακτηριστικά της κάρτας (δηλαδή τα δεδομένα που τηρούνται και αποστέλλονται ανέπαφα) είναι εις γνώσιν των Τραπεζικών Ιδρυμάτων που συνεργάζονται με την MasterCard για την έκδοση καρτών, καθώς επίσης και αν υπάρχει διαφοροποίηση στην υλοποίηση των καρτών που παρέχονται από ελληνικά Τραπεζικά Ιδρύματα σε σχέση με άλλα κράτη. Τέλος, η Αρχή ζήτησε να υποβληθεί η προαναφερθείσα μελέτη εκτίμησης στην ιδιωτικότητα που έχει διενεργηθεί από τη MasterCard για τις εν λόγω ανέπαφες κάρτες.

Σε απάντηση του ως άνω εγγράφου, η Mastercard (εγκατάσταση Ελλάδος) απέστειλε στην Αρχή το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/180/12-01-2017 έγγραφο, στο οποίο αναφέρει, μεταξύ άλλων, τα εξής:

α) Η Mastercard δεν εκδίδει κάρτες πληρωμών σε κατόχους καρτών. Στην Ελλάδα, όπως και σε άλλες αγορές παγκοσμίως, οι κάρτες εκδίδονται από τραπεζικά και χρηματοπιστωτικά ιδρύματα, τα οποία και λαμβάνουν αποφάσεις σχετικά με την υλοποίηση και λειτουργία των καρτών και άλλων προϊόντων πληρωμών στην αγορά.

β) Η χρήση της τεχνολογίας ανέπαφων συναλλαγών είναι στη διακριτική ευχέρεια των εκδοτών. Οι εκδότες είναι οι υπεύθυνοι επεξεργασίας προσωπικών δεδομένων και είναι επιφορτισμένοι με το να συνάπτουν άμεση οικονομική σχέση με τους καταναλωτές/κατόχους καρτών. Οι εκδότες στη σχέση αυτή καθορίζουν, μεταξύ άλλων, τον τύπο της κάρτας πληρωμής που εκδίδεται για κάθε κάτοχο κάρτας, καθώς και τα σχετικά τεχνικά χαρακτηριστικά της κάρτας.

γ) Η Mastercard παρέχει στους πελάτες της, τραπεζικά και χρηματοπιστωτικά ιδρύματα, τη βασική υποδομή της τεχνολογίας ανέπαφων συναλλαγών, καθώς και όλες τις σχετικές πληροφορίες που είναι απαραίτητο να εξετάζονται από τους εκδότες πριν την υλοποίηση κάθε προϊόντος. Κάθε εκδότης έχει τη διακριτική ευχέρεια να προχωρά στην επιλογή των τεχνικών χαρακτηριστικών των καρτών ανέπαφων συναλλαγών που παρέχει στους πελάτες του. Ως εκ τούτου, οι εκδότες μόνο είναι σε θέση να παρέχουν λεπτομερείς πληροφορίες σχετικά με την εκάστοτε υλοποίηση και τα τεχνικά χαρακτηριστικά των προϊόντων πληρωμών που παρέχουν.

δ) Οι βασικές κατηγορίες προσωπικών δεδομένων που τηρούνται στο chip της κάρτας και είναι αναγνώσιμες ανέπαφα είναι ο προσωπικός αριθμός λογαριασμού[4] (απαραίτητος ώστε να ταυτοποιεί τον εκδότη και συγκεκριμένο λογαριασμό του κατόχου

[4] Πρόκειται για τον αριθμό της κάρτας, ο οποίος ονομάζεται και "Primary Account Number (PAN)".

της κάρτας που είναι συνδεδεμένος με την κάρτα ανέπαφων πληρωμών) και η ημερομηνία λήξης της κάρτας (απαραίτητη ώστε να διαπιστώνεται η ημερομηνία πέραν της οποίας δεν μπορεί πλέον να χρησιμοποιηθεί η κάρτα). Επίσης, τηρούνται δεδομένα τρίτων μόνο αν υποστηρίζεται από τον εκδότη. Το πεδίο αυτό μπορεί να χρησιμοποιηθεί από τους εκδότες για την αποθήκευση πληροφοριών που αφορούν τον τύπο της συσκευής ή προσωπικά δεδομένα όπως τον αριθμό προγράμματος επιβράβευσης πελατών. Η Mastercard συνιστά ρητά στους εκδότες να μην εισάγουν προσωπικά δεδομένα σε αυτό το πεδίο. Τέλος, τηρείται αρχείο καταγραφής συναλλαγών (transaction logs) μόνο εάν υποστηρίζεται από τον εκδότη. Το αρχείο αυτό μπορεί να περιλαμβάνει: i) Εγκριθέν ποσό συναλλαγής, κωδικό νομίσματος συναλλαγής και ημερομηνία συναλλαγής. Τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν από τους εκδότες στο πλαίσιο επίλυσης διαφορών που αφορούν συναλλαγές, καθώς επίσης και για την παροχή πληροφοριών σε κατόχους των καρτών σε ό,τι αφορά τις πρόσφατες κινήσεις της κάρτας τους. ii) Δεδομένα τα οποία παρέχονται από εμπόρους όταν είναι απαραίτητα για τον υπολογισμό του χρεωθέντος ποσού – για παράδειγμα, η τοποθεσία ή/και ο χρόνος ορισμένης συναλλαγής για τον υπολογισμό ναύλου στις περιπτώσεις συγκοινωνιών/μεταφορών.

Ως προς το αρχείο καταγραφής συναλλαγών, οι εκδότες έχουν τη διακριτική ευχέρεια να αποφασίζουν: 1) αν αυτό είναι απαραίτητο, 2) πόσες συναλλαγές θα καταγράφονται (με ελάχιστες τις 10, αν ο εκδότης έχει επιλέξει να υποστηρίζει το εν λόγω χαρακτηριστικό), 3) να καταστήσουν το αρχείο καταγραφής συναλλαγών απρόσιτο ανάγνωσης από τις συσκευές ανάγνωσης ανέπαφων καρτών.

ε) Όλες οι πληροφορίες που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της τεχνολογίας ανέπαφων πληρωμών είναι γνωστές στους εκδότες. Βάσει των πληροφοριών αυτών, οι εκδότες είναι σε θέση να καθορίζουν την υλοποίηση και λειτουργία της εν λόγω τεχνολογίας που παρέχουν στους πελάτες τους. Δεν προβλέπονται εξειδικευμένα τεχνικά χαρακτηριστικά της τεχνολογίας αυτής στην Ελλάδα – λειτουργεί βάσει παγκόσμιων τεχνικών απαιτήσεων.

στ) Η μελέτη εκτίμησης αντικτύπου στην ιδιωτικότητα που διενεργήθηκε από τη Mastercard – και επισυνάπτεται στο ως άνω έγγραφο της Mastercard – έλαβε υπόψη τον προαιρετικό χαρακτήρα της λειτουργίας ανέπαφων πληρωμών, συμπεριλαμβανομένης της δυνατότητας εκ των υστέρων απενεργοποίησης της λειτουργίας της. Ειδικότερα, η μελέτη επικινδυνότητας περιγράφει διάφορες εναλλακτικές λύσεις που προσφέρονται από τη Mastercard στους εκδότες ώστε να αποφασίζουν τον τρόπο που επιθυμούν να επιτρέπουν στους πελάτες τους να ασκούν το δικαίωμά τους να αρνηθούν τη χρήση της ανέπαφης

λειτουργίας εκ των προτέρων ή αργότερα.

Επίσης, η Αρχή, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/4942/27-06-2017 έγγραφό της, ζήτησε σχετικώς τις απόψεις και από τη VISA Hellas (εταιρεία με την οποία είναι συμβεβλημένη η Τράπεζα Πειραιώς, την οποία αφορά η δεύτερη καταγγελία), ιδίως ως προς το είδος των δεδομένων και τα λοιπά χαρακτηριστικά της επεξεργασίας που πραγματοποιείται μέσω της τεχνολογίας ανέπαφων συναλλαγών, ως προς τα ζητήματα αν η Visa υποχρεώνει τους εκδότες (τραπεζικά ιδρύματα) στη χορήγηση αποκλειστικά ανέπαφων καρτών στους πελάτες τους, αν υπάρχει η τεχνολογική δυνατότητα, σε μία εκδοθείσα ανέπαφη κάρτα, να απενεργοποιηθεί το χαρακτηριστικό εκείνο που προσδίδει τη δυνατότητα των ανέπαφων συναλλαγών έτσι ώστε να λειτουργεί η κάρτα ως συμβατική (ήτοι μη ανέπαφη) και –σε καταφατική περίπτωση– αν αυτή η απενεργοποίηση δύναται να πραγματοποιείται από τους εκδότες (Τραπεζικά Ιδρύματα), καθώς επίσης και αν έχει διενεργηθεί, για την εν λόγω επεξεργασία, εκτίμηση επιπτώσεων στην προστασία προσωπικών δεδομένων. Η Visa Hellas απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6719/19-09-2017 έγγραφο στο οποίο αναφέρει, μεταξύ άλλων, ότι για την τεχνολογία αυτή έχουν υιοθετηθεί διεθνή πρότυπα ασφάλειας (τα οποία και κατονομάζει), καθώς επίσης και ότι, προς το παρόν, η Visa δεν απαιτεί από τους εκδότες καρτών στην Ελλάδα να διασφαλίζουν ότι οι κάρτες που εκδίδουν είναι ανέπαφες. Σχετικές απαιτήσεις έχουν τεθεί σε ορισμένες ευρωπαϊκές χώρες και η Ελλάδα πρόκειται να συμπεριληφθεί σε αυτές σύντομα. Επίσης, οι προδιαγραφές της Visa επιτρέπουν στους εκδότες να ρυθμίζουν τις παραμέτρους των καρτών, οι οποίες μπορούν να ενεργοποιήσουν ή να απενεργοποιήσουν την ανέπαφη δυνατότητα συναλλαγής κατά τη διάρκεια του κύκλου ζωής της κάρτας. Επίσης η Visa έχει εκπονήσει εκτίμηση επιπτώσεων στην προστασία προσωπικών δεδομένων, την οποία και υπέβαλε στην Αρχή με το ως άνω έγγραφό της.

Τέλος, η Αρχή, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/4943/27-06-2017 έγγραφό της, ζήτησε σχετικές πληροφορίες επί ανέπαφων καρτών από το σύνολο των Πιστωτικών Ιδρυμάτων που λειτουργούν στην Ελλάδα με έδρα στην Ελλάδα[5] και, συγκεκριμένα από τις: i) ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε., ii) ΑΛΦΑ ΤΡΑΠΕΖΑ Α.Ε., iii) ATTICA BANK, ΑΝΩΝΥΜΗ ΤΡΑΠΕΖΙΚΗ ΕΤΑΙΡΕΙΑ, iv) ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ Α.Ε., v) ΤΡΑΠΕΖΑ EUROBANK ERGASIAS Α.Ε., vi) ΕΠΕΝΔΥΤΙΚΗ ΤΡΑΠΕΖΑ ΕΛΛΑΔΟΣ Α.Ε., vii) AEGEAN BALTIC BANK A.T.E., viii) CREDICOM CONSUMER FINANCE ΤΡΑΠΕΖΑ Α.Ε., ix) ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΧΑΝΙΩΝ ΣΥΝ.Π.Ε., x)

[5] Σύμφωνα με τη σχετική λίστα, ημερομηνίας Απριλίου 2017, από το διαδικτυακό τόπο της Τράπεζας της Ελλάδας.

ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΗΠΕΙΡΟΥ ΣΥΝ.ΠΕ., xi) ΠΑΓΚΡΗΤΙΑ ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΣΥΝ.ΠΕ., xii) ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ Ν. ΕΒΡΟΥ ΣΥΝ.Π.Ε., xiii) ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΚΑΡΔΙΤΣΑΣ ΣΥΝ.Π.Ε., xiv) ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΘΕΣΣΑΛΙΑΣ ΣΥΝ.Π.Ε., xv) ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΠΙΕΡΙΑΣ - ΟΛΥΜΠΙΑΚΗ ΠΙΣΤΗ ΣΥΝ.Π.Ε., xvi) ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΔΡΑΜΑΣ ΣΥΝ.Π.Ε., xvii) ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΣΕΡΡΩΝ ΣΥΝ.Π.Ε.

Από τα ως άνω Ιδρύματα, τα υπό στοιχ. iii, viii, ix, x, xii, xiii, xiv, xv και xvi απάντησαν ότι δεν παρέχουν στους πελάτες τους προϊόντα αυτής της τεχνολογίας[6]. Η ΕΠΕΝΔΥΤΙΚΗ ΤΡΑΠΕΖΑ ΕΛΛΑΔΟΣ Α.Ε. (στοιχ. vi), με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6089/16-08-2017 έγγραφό της, αναφέρει ότι διαθέτει κάρτες για ανέπαφες συναλλαγές στους πελάτες της, έχοντας συμβληθεί σχετικώς με το διεθνή οργανισμό Mastercard, ακολουθώντας τα πρότυπα που ορίζει ο οργανισμός αυτός. Δεν παρέχεται η δυνατότητα της εκ των υστέρων απενεργοποίησης της ανέπαφης λειτουργικότητας ούτε παρέχεται στους πελάτες της η δυνατότητα να λάβουν κάρτα χωρίς αυτήν την τεχνολογία. Επίσης η Τράπεζα αναφέρει ότι το όριο για την πραγματοποίηση ανέπαφων συναλλαγών είναι αθροιστικά 25 Ευρώ σε τρεις (3) διαδοχικές ανέπαφες συναλλαγές, πέραν του οποίου είναι υποχρεωτική η χρήση PIN.

Η AEGEAN BALTIC BANK A.T.E. (στοιχ. vii), με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/7488/17-10-2017 έγγραφό της, αναφέρει ότι εκδίδει χρεωστικές κάρτες για τους πελάτες της οι οποίες μπορούν να πραγματοποιούν και ανέπαφες συναλλαγές, έχοντας συμβληθεί σχετικώς με το διεθνή οργανισμό Visa. Η Τράπεζα αναφέρει ότι τα δεδομένα που τηρούνται στο chip των καρτών είναι δεδομένα που αφορούν στοιχεία του πελάτη που γνωστοποιεί κατά την αίτησή του για χορήγηση κάρτας καθώς και δεδομένα που αφορούν τη λειτουργία της κάρτας, ενώ κάποια εξ αυτών μπορούν να αναγνωσθούν ανέπαφα (π.χ. ονοματεπώνυμο, αριθμός κάρτας, ημερομηνία λήξης αυτής) μέσω κατάλληλης συσκευής-«αναγνώστη». Η προσωποποίηση των δεδομένων στην κάρτα πραγματοποιείται σύμφωνα με τα πρότυπα και τις οδηγίες του οργανισμού Visa. Εφόσον πελάτης της Τράπεζας εκφράσει ειδική αντίρρηση, δεν παρέχεται η δυνατότητα να λάβει κάρτα αυτής της τεχνολογίας, ενώ υπάρχει η δυνατότητα, πάντα κατόπιν γραπτής οδηγίας του πελάτη, να παραμετροποιηθεί εκ των υστέρων η λειτουργικότητα της κάρτας αυτού με αποτέλεσμα να

[6] Με τα υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5479/18-07-2017, Γ/ΕΙΣ/5348/13-07-2017, Γ/ΕΙΣ/5254/10-07-2017, Γ/ΕΙΣ/5329/12-07-2017, Γ/ΕΙΣ/5357/13-07-2017, Γ/ΕΙΣ/5289/11-07-2017, Γ/ΕΙΣ/5376/14-07-2017, Γ/ΕΙΣ/5363/13-07-2017 και Γ/ΕΙΣ/6768/21-09-2017 έγγραφα αντιστοίχως

μην επιτρέπει την πραγματοποίηση ανέπαφων συναλλαγών. Ο λόγος που η Τράπεζα δεν δίνει εξ αρχής τη δυνατότητα έκδοσης καρτών μη ανέπαφων συναλλαγών είναι αφενός το κόστος και αφετέρου η εναρμόνιση με τον ευρύτερο εγχώριο και διεθνή ανταγωνισμό στο χώρο των καρτών.

Τα λοιπά ιδρύματα δεν απάντησαν στο ως άνω έγγραφο της Αρχής, πέραν της Τράπεζας Πειραιώς (στοιχ. iv), η οποία με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5949/07-08-2017 έγγραφό της ουσιαστικά επανέλαβε συνοπτικά τα όσα είχε πει σχετικώς με το προηγούμενο έγγραφό της. Η Αρχή απέστειλε ειδικώς υπόμνηση στις ΑΛΦΑ ΤΡΑΠΕΖΑ Α.Ε. (στοιχ. ii) και ΤΡΑΠΕΖΑ EUROBANK ERGASIAS Α.Ε. (στοιχ. v) με τα υπ' αριθμ. πρωτ. Γ/ΕΞ/276/12-01-2018 και Γ/ΕΞ/275/12-01-2018 έγγραφά της, στα οποία επίσης δεν έλαβε απάντηση.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων, αφού άκουσε τον εισηγητή και τις διευκρινίσεις του βοηθού εισηγητή, ο οποίος στη συνέχεια αποχώρησε πριν από τη διάσκεψη και τη λήψη απόφασης, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ 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». Ως εκ τούτου, σημειώνεται ότι τα δεδομένα χρεωστικών ή/και πιστωτικών καρτών, όπως ο αριθμός της κάρτας και η ημερομηνία λήξης αυτής, αποτελούν δεδομένα προσωπικού χαρακτήρα.

   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, ενώ ως εκτελών την επεξεργασία ορίζεται οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας (φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός).

Στις εν λόγω περιπτώσεις, τόσο η Εθνική Τράπεζα της Ελλάδας (για την πρώτη περίπτωση) όσο και Τράπεζα Πειραιώς Α.Ε. (για τη δεύτερη περίπτωση) αποτελούν τον υπεύθυνο επεξεργασίας, αφού παρέχουν στους πελάτες τους ένα τραπεζικό προϊόν (χρεωστική κάρτα για ανέπαφες συναλλαγές), μέσω του οποίου επεξεργάζονται προσωπικά δεδομένα αυτών - στο πλαίσιο πραγματοποίησης χρεώσεων του τραπεζικού λογαριασμού του κάθε πελάτη βάσει των συναλλαγών που πραγματοποιεί με χρήση της κάρτας - και για το οποίο προϊόν η κάθε Τράπεζα έχει επιλέξει το σκοπό και τον τρόπο της επεξεργασίας.

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. 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[7].

   Λαμβάνοντας υπόψη τους κινδύνους που συνεπάγεται η επεξεργασία δεδομένων χρεωστικών καρτών, ιδίως σε περίπτωση τυχαίας ή παράνομης πρόσβασης ή διάδοσης, προκύπτει ότι, για την περίπτωση αυτή, ο υπεύθυνος επεξεργασίας θα πρέπει να λάβει μέτρα που να εξασφαλίζουν υψηλό επίπεδο ασφαλείας.

4. Σύμφωνα με το αρ. 11 παρ. 1 του ν. 2472/1997 ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει με τρόπο πρόσφορο και σαφή τα υποκείμενα των δεδομένων κατ' ελάχιστο για την ταυτότητά του, το σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, καθώς και για την ύπαρξη του δικαιώματος πρόσβασης (όπως αυτό προβλέπεται στο άρθρο 12 του ν. 2472/1997).

5. Στη συγκεκριμένη περίπτωση, τόσο η Εθνική Τράπεζα όσο και η Τράπεζα Πειραιώς αντικατέστησαν τις χρεωστικές κάρτες των καταγγελλόντων πελατών τους με νέες,

[7] Εξάλλου, και στο άρθρο 32 του Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ο οποίος θα τεθεί σε εφαρμογή στα Κράτη Μέλη στις 25 Μαΐου 2018, αναφέρεται ότι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, 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, 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 (...)*». Στο ίδιο άρθρο αναφέρεται ότι 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. Περαιτέρω, στο άρθρο 35 του Κανονισμού αναφέρεται ότι όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

οι οποίες διαφέρουν από τις προηγούμενες στο ότι διαθέτουν τεχνολογία για ανέπαφες συναλλαγές (όπως αυτή έχει περιγραφεί ανωτέρω). Η αντικατάσταση των καρτών, και στις δύο περιπτώσεις, ήταν υποχρεωτική – δηλαδή δεν δόθηκε η δυνατότητα στους καταγγέλλοντες πελάτες τους να αποκτήσουν νέα κάρτα όμοιας τεχνολογίας με αυτή της παλαιάς τους κάρτας (ήτοι χωρίς δυνατότητα ανέπαφων συναλλαγών). Και στις δύο περιπτώσεις φαίνεται ότι με τη λήψη της νέας κάρτας υπήρξε σαφής ενημέρωση από την κάθε Τράπεζα προς τον πελάτη της για το ότι πρόκειται για κάρτα με τεχνολογία που υποστηρίζει ανέπαφες συναλλαγές – χωρίς όμως αναλυτική ενημέρωση για τα επιμέρους χαρακτηριστικά της εν λόγω επεξεργασίας, όπως το ποια δεδομένα μεταδίδονται ανέπαφα ή ποια δεδομένα τηρούνται στο chip της κάρτας. Η νέα τεχνολογία, όπως επισημαίνουν και οι δύο Τράπεζες στα υπομνήματά τους προς την Αρχή, παρέχει το πλεονέκτημα ότι πραγματοποιούνται, με τη χρήση αυτής, πιο εύκολα και γρήγορα οι συναλλαγές αξίας μέχρι 25 Ευρώ (αφού δεν χρειάζεται να εισάγει ο κάτοχός της το PIN αυτής, ούτε αυτή να τοποθετηθεί στην υποδοχή κάποιας τερματικής συσκευής-αναγνώστη).

6. Ως προς την ασφάλεια της επεξεργασίας, η χρήση της νέας κάρτας εγείρει κατ' αρχάς τους εξής κινδύνους, οι οποίοι κίνδυνοι δεν υπήρχαν με την παλαιότερη τεχνολογία χρεωστικών καρτών:

   α) Εάν η κάρτα έρθει στα χέρια κακόβουλου τρίτου (π.χ. απώλεια από τον κάτοχό της), τότε αυτός θα μπορεί, χωρίς τη γνώση του PIN αυτής, να πραγματοποιεί σειρά αγορών, αξίας μέχρι 25 Ευρώ εκάστη.

   β) Δεδομένου ότι μία τέτοια κάρτα μπορεί να εκπέμψει, μέσω ραδιοκυμάτων υψηλής συχνότητας[8], προσωπικά δεδομένα όπως τον αριθμό αυτής και την ημερομηνία λήξης της, υπάρχει η δυνατότητα σε κάποιον που διαθέτει συσκευή ανάγνωσης αυτών των σημάτων και βρεθεί στην εμβέλειά τους, να τα καταγράψει.

Για την αξιολόγηση των εν λόγω κινδύνων, σε σχέση με τα σχετικά μέτρα ασφάλειας που έχουν ληφθεί, σημειώνονται τα εξής:

α) Και οι δύο Τράπεζες αναφέρουν ότι τυχόν δόλιες συναλλαγές μπορούν να αμφισβητηθούν από τον κάτοχο της κάρτας με την ίδια διαδικασία που ακολουθείται και στις συναλλαγές με πιστωτικές ή χρεωστικές κάρτες με χρήση PIN, καθώς επίσης και ότι ο κάτοχος της κάρτας έχει σε κάθε περίπτωση την

[8] Πληροφορίες για την τεχνολογία NFC, αλλά και γενικότερα για την τεχνολογία RFID, υπάρχουν στο σύνδεσμο http://nfc-forum.org/.

ευθύνη ασφαλούς φύλαξής της. Περαιτέρω, και οι δύο Τράπεζες παρακολουθούν σε εικοσιτετράωρη βάση όλες τις κινήσεις των καρτών στο πλαίσιο πρόληψης και αποφυγής απάτης.

Θα πρέπει επίσης να ληφθεί υπόψη, κατά την αξιολόγηση του εν λόγω κινδύνου, ότι τυχόν κλοπή ή υπεξαίρεση της κάρτας, ανεξάρτητα του αν η κάρτα φέρει τεχνολογία ανέπαφων συναλλαγών ή όχι, δύναται σε κάθε περίπτωση να επιφέρει εξαιρετικά δυσμενείς συνέπειες για τον κάτοχο αυτής: για παράδειγμα, θα μπορεί οποιοσδήποτε κακόβουλος, ο οποίος έχει την κάρτα στην κατοχή του, να πραγματοποιήσει αγορές προϊόντων ή υπηρεσιών μέσω Διαδικτύου οικονομικής αξίας όχι περιορισμένης στα 25 Ευρώ αλλά μέχρι το ανώτερο επιτρεπτό χρηματικό όριο που έχει τεθεί για τη συγκεκριμένη κάρτα.

Συνεπώς, αναφορικά με τον εν λόγω κίνδυνο, πρέπει να γίνει δεκτό ότι δεν πρόκειται κατ' αρχάς για κίνδυνο μεγαλύτερης έντασης από το γενικότερο κίνδυνο απώλειας ή κλοπής οποιασδήποτε άλλης κάρτας. Πρέπει ωστόσο να συνυπολογιστεί ότι η κακόβουλη χρήση της ως ανέπαφη κάρτα, για αγορές αξίας μέχρι 25 Ευρώ, είναι πιο εύκολο να πραγματοποιηθεί σε σχέση με την κακόβουλη χρήση της για αγορές μέσω Διαδικτύου.

β) Οι Τράπεζες δεν αναφέρουν, για τον εν λόγω κίνδυνο, συγκεκριμένα μέτρα που έχουν λάβει για την αντιμετώπισή του. Η Εθνική Τράπεζα αναφέρει ότι τα μόνα δεδομένα που μεταδίδονται με ραδιοκύματα, σε μη κρυπτογραφημένη μορφή, είναι ο αριθμός της κάρτας και η ημερομηνία λήξης αυτής (δηλαδή όχι το ονοματεπώνυμο του κατόχου, ούτε ο τριψήφιος αριθμός ασφαλείας CCV/CVV), ενώ η Τράπεζα Πειραιώς δεν παρέχει αναλυτικές πληροφορίες. Ωστόσο, λαμβάνοντας υπόψη και τη σχετική απάντηση της Visa Hellas, γίνεται χρήση της ίδιας τεχνολογίας και πρόκειται για ίδιες περιπτώσεις – άρα, τα ίδια δεδομένα (ήτοι ο αριθμός της κάρτας και η ημερομηνία λήξης αυτής) είναι αυτά που μεταδίδονται σε όλες τις περιπτώσεις με ραδιοκύματα και όχι περισσότερα.

Ο ανωτέρω κίνδυνος δεν μπορεί να θεωρηθεί ως εξαιρετικά χαμηλής πιθανότητας επέλευσης: και τούτο διότι, παρά το γεγονός ότι για να καταγράψει κανείς τα ραδιοκύματα που εκπέμπει η κάρτα θα πρέπει να βρεθεί σε πολύ κοντινή απόσταση (της τάξης των 5 έως 8 cm), εν τούτοις η καταγραφή αυτή μπορεί να γίνει με κατάλληλο εξοπλισμό που δεν είναι δαπανηρός ή με επίσης χαμηλού κόστους

λογισμικό που μπορεί να εγκατασταθεί σε «έξυπνες» κινητές συσκευές[9] – εξάλλου, με αντίστοιχο λογισμικό κατέστη εφικτός ο έλεγχος των μεταδιδόμενων δεδομένων από ελεγκτές της Αρχής. Η μη κρυπτογράφηση των μεταδιδόμενων δεδομένων επιτρέπει δυνητικά την πραγματοποίηση μίας τέτοιας καταγραφής. Ο εν λόγω κίνδυνος μπορεί να επιφέρει, σε περίπτωση υλοποίησης της σχετικής απειλής, την εξής συνέπεια: Έχοντας κάποιος κακόβουλος γνώση του αριθμού της κάρτας και της ημερομηνίας λήξης αυτής, μπορεί να επιχειρήσει να πραγματοποιήσει αγορά προϊόντος μέσω Διαδικτύου με χρέωση/πίστωση στον τραπεζικό λογαριασμό με τον οποίο είναι συνδεδεμένη η κάρτα, η αγορά δε αυτή ενδέχεται να ολοκληρωθεί επιτυχώς εφόσον το σχετικό ηλεκτρονικό κατάστημα δεν εφαρμόζει τα δέοντα μέτρα ασφάλειας (όπως το να απαιτεί από το χρήστη και την εισαγωγή του τριψήφιου κωδικού ασφαλείας CCV/CVV[10]). Ως εκ τούτου, καθίσταται σαφές ότι για τον εν λόγω κίνδυνο δεν μπορεί να θεωρηθεί ότι οι συνέπειες που δύναται επιφέρει στα δικαιώματα και στις ελευθερίες των φυσικών προσώπων είναι χαμηλής σοβαρότητας.

Σημειώνεται ότι στη σχετική μελέτη αντικτύπου στην ιδιωτικότητα που εκπόνησε η Mastercard για την τεχνολογία ανέπαφων συναλλαγών και την οποία υπέβαλε στην Αρχή, ο ως άνω κίνδυνος πράγματι αναγνωρίζεται ως υπαρκτός. Ως μέτρα αντιμετώπισης του εν λόγω κινδύνου, αναφέρονται: i) δεν αποστέλλεται το ονοματεπώνυμο του κατόχου της κάρτας ούτε ο τριψήφιος κωδικός ασφαλείας CCV/CVV, ii) για την ανέπαφη ανάγνωση των δεδομένων, η συσκευή-αναγνώστης πρέπει να βρεθεί σε πολύ κοντινή απόσταση με την κάρτα, iii) παρέχεται η δυνατότητα απενεργοποίησης της δυνατότητας ανέπαφων συναλλαγών, αν το επιλέξει σχετικά ο εκδότης (Τραπεζικό Ίδρυμα), iv) υπάρχει η δυνατότητα τοποθέτησης της κάρτας σε ειδική θήκη ("data protection sleeve") η οποία δεν επιτρέπει σε καμία συσκευή-αναγνώστη να «διαβάσει» ανέπαφα δεδομένα της κάρτας. Από τα ανωτέρω, και με βάση τα στοιχεία του φακέλου της υπόθεσης, προκύπτει ότι τα Τραπεζικά Ιδρύματα –εν προκειμένω, η Εθνική Τράπεζα και η Τράπεζα Πειραιώς τις οποίες αφορούν οι υπό εξέταση καταγγελίες– ως εκδότες, δεν

[9] Βλ. ενδεικτικά περιγραφή μίας τέτοιας επίθεσης στο http://securityaffairs.co/wordpress/37667/hacking/nfc-attack-credit-card.html, καθώς επίσης και ενδεικτική αναφορά σε Android λογισμικό που μπορεί να διαβάσει τέτοια δεδομένα στο http://www.androidauthority.com/android-app-steal-credit-card-info-nfc-96823/ (τελευταία πρόσβαση: 23/4/2018).

[10] Ενδεικτική τέτοια περίπτωση – βλ. https://www.independent.co.uk/news-14-1/contactless-payment-card-theft-how-is-the-data-stolen-and-what-can-i-do-to-protect-myself-10409319.html καθώς και https://www.theguardian.com/money/2015/jul/23/contactless-card-is-too-easy-says-which (τελευταία πρόσβαση: 23/4/2018).

έχουν επιλέξει τα υπό στοιχ. iii) και iv) μέτρα για την αντιμετώπιση του εν λόγω κινδύνου.

Η μελέτη εκτίμησης επιπτώσεων που εκπόνησε η Visa ως προς την προστασία των προσωπικών δεδομένων και την οποία υπέβαλε στην Αρχή, αναφορικά με τον εν λόγω κίνδυνο χαρακτηρίζει τα δεδομένα που αποστέλλονται ανέπαφα (ήτοι τον αριθμό της κάρτας και την ημερομηνία λήξης αυτής) ως ψευδωνυμοποιημένα δεδομένα[11], υπό την έννοια ότι από μόνα τους δεν επαρκούν για την ταυτοποίηση του προσώπου χωρίς τη χρήση συμπληρωματικών πληροφοριών, οι οποίες πληροφορίες βρίσκονται στα συστήματα της Τράπεζας. Η Visa επίσης αναφέρει ότι για τη συλλογή αυτών των δεδομένων θα πρέπει η συλλογή-«αναγνώστης» να βρεθεί πολύ κοντά, σε απόσταση λίγων εκατοστών, με την κάρτα, καθώς επίσης και ότι με τα δεδομένα αυτά δεν μπορεί κάποιος κακόβουλος να πραγματοποιήσει ηλεκτρονικές πληρωμές διότι τα ηλεκτρονικά καταστήματα διαθέτουν και άλλες δικλείδες ασφαλείας (όπως, π.χ., με το να ζητάνε και τον αριθμό CVV της κάρτας). Σε κάθε περίπτωση άλλωστε, και η Visa αναφέρει ότι οι εκδότες (δηλαδή τα πιστωτικά ιδρύματα) μπορούν οποτεδήποτε να απενεργοποιήσουν την ανέπαφη λειτουργία μιας κάρτας.

Πρέπει επίσης να σημειωθεί ότι ήδη τουλάχιστον μία εκ των Τραπεζών, και συγκεκριμένα η AEGEAN BALTIC BANK A.T.E., όπως αναφέρει στο έγγραφό της που μνημονεύεται στο ιστορικό της παρούσας, παρέχει στους πελάτες της τη δυνατότητα της εκ των υστέρων απενεργοποίησης από μία ανέπαφη κάρτα της δυνατότητας ανέπαφων συναλλαγών.

7. Τέλος, για την περίπτωση καρτών της Mastercard, υπάρχει η δυνατότητα αποθήκευσης στην κάρτα του πρόσφατου ιστορικού συναλλαγών, καθώς επίσης και δυνατότητα ανέπαφης ανάγνωσης αυτών. Τα συγκεκριμένα δεδομένα σαφώς δεν είναι απολύτως απαραίτητα για τη βασική λειτουργικότητα για την οποία προορίζεται μία χρεωστική κάρτα και, ως εκ τούτου, δεν θα πρέπει εξ ορισμού να τηρούνται[12] – πολλώ δε μάλλω χωρίς ρητή προς τούτο ενημέρωση, όπως φαίνεται ότι

[11] Κάνοντας ειδική μνεία στον ορισμό της ψευδωνυμοποίησης του Κανονισμού (ΕΕ) 679/2016.

[12] Σημειώνεται εξάλλου ότι σύμφωνα με το άρ. 25 παρ. 2 του Κανονισμού (ΕΕ) 2016/679, ο οποίος τίθεται σε εφαρμογή από τις 25 Μαΐου 2018, 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.

ισχύει στην περίπτωση της Εθνικής Τράπεζας. Σημειώνεται επίσης ότι η τήρηση αυτών των δεδομένων –η οποία δεν είναι υποχρεωτική βάσει των προδιαγραφών που έχει θέσει η Mastercard– εγείρει ζητήματα προστασίας προσωπικών δεδομένων αφού από τις κινήσεις της κάρτας μπορεί να δημιουργηθεί προφίλ του κατόχου της ως προς τις καταναλωτικές του συνήθειες.

Συνεπώς, ενόψει των κινδύνων, των πιθανοτήτων εμφάνισής τους και της σοβαρότητάς τους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η συγκεκριμένη επεξεργασία (τήρηση ιστορικού συναλλαγών στην κάρτα) δεν εμπίπτει σε καμία εκ των εξαιρέσεων του άρθρου 5 παρ. 2 του ν. 2472/1997 και, συνεπώς, η μοναδική νομική βάση για την πραγματοποίηση αυτής της επεξεργασίας μέσω των εν λόγω καρτών είναι η συγκατάθεση των υποκειμένων των δεδομένων (πελατών της κάθε Τράπεζας που είναι κάτοχοι των καρτών).

8. Επίσης, ως προς τον κίνδυνο κακόβουλης ανέπαφης ανάγνωσης των δεδομένων «αριθμός κάρτας–ημερομηνία λήξης αυτής», όπως περιγράφεται στη Σκέψη 6 της παρούσας, οι Τράπεζες πρέπει –ως μέσο αντιμετώπισης του κινδύνου αυτού– να παρέχουν είτε τη δυνατότητα απενεργοποίησης της ανέπαφης λειτουργίας ή, εναλλακτικώς, τη χορήγηση νέας κάρτας χωρίς ανέπαφη λειτουργία, εφόσον ο πελάτης δεν επιθυμεί να έχει κάρτα με δυνατότητα ανέπαφων συναλλαγών.
9. Ενόψει των ανωτέρω, και λαμβάνοντας υπόψη και τις διεθνείς προδιαγραφές που ακολουθούνται αναφορικά με τις ανέπαφες χρεωστικές ή/και πιστωτικές κάρτες, οι εκδότες των πιστωτικών καρτών οφείλουν να λάβουν τα κατάλληλα μέτρα προκειμένου να εξασφαλίζουν τα εξής:

   α) Εφόσον ο πελάτης δηλώσει ότι δεν επιθυμεί να έχει κάρτα με δυνατότητα πραγματοποίησης ανέπαφων συναλλαγών, να παρέχεται η δυνατότητα απενεργοποίησης της ανέπαφης λειτουργίας της κάρτας είτε η χορήγηση νέας, μη ανέπαφης κάρτας.

   β) Εφόσον σε κάρτα που έχει χορηγηθεί σε πελάτη είναι ενεργοποιημένη η δυνατότητα τήρησης ιστορικού συναλλαγών στο chip αυτής χωρίς να έχει δώσει την ειδική προς τούτο συγκατάθεσή του, θα πρέπει ο πελάτης να ενημερωθεί σχετικώς με κάθε πρόσφορο τρόπο (π.χ. μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, μέσω μηνύματος κατά τη σύνδεσή του σε προσωποποιημένες ηλεκτρονικές υπηρεσίες του υπεύθυνου επεξεργασίας, μέσω ταχυδρομικής επιστολής, κτλ.) ως προς την επεξεργασία αυτή, παρέχοντάς του τη δυνατότητα διακοπής της επεξεργασίας αυτής. Περαιτέρω, σε κάθε νέα έκδοση/χορήγηση κάρτας, το εν λόγω χαρακτηριστικό θα

πρέπει να είναι εξ αρχής απενεργοποιημένο, και να ενεργοποιείται μόνο αν υπάρχει ειδική προς τούτο συγκατάθεση του πελάτη, εφόσον έχει προηγουμένως σχετικώς ενημερωθεί για την επεξεργασία αυτή.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων απευθύνει, σύμφωνα με το άρ. 19 παρ. γ΄ του ν. 2472/1997, σύσταση στην Εθνική Τράπεζα της Ελλάδος ΑΕ, καθώς επίσης και στην Τράπεζα Πειραιώς ΑΕ, να προβούν, ως υπεύθυνοι επεξεργασίας κατά την έννοια του άρ. 2 στοιχ. ζ' του ν. 2472/1997, στις κατάλληλες ενέργειες σύμφωνα με τα όσα περιγράφονται στη Σκέψη 9 της παρούσας.

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