ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 06-09-2013

Αριθ. Πρωτ.: Γ/ΕΞ/5733/06-09-2013

Α Π Ο Φ Α Σ Η ΑΡ. 100/2013

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος στην έδρα της την Τρίτη 23 Ιουλίου και ώρα 10:00 μετά από πρόσκληση του Προέδρου της, σε συνέχεια της από 2 Ιουλίου 2013 συνεδρίασης, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Γεώργιος Μπατζαλέξης, Αναπληρωτής Πρόεδρος, κωλυομένου του Προέδρου της Αρχής Πέτρου Χριστόφορου, και τα αναπληρωματικά μέλη της Αρχής Σπύρος Βλαχόπουλος, Γρηγόρης Λαζαράκος, ως εισηγητής, και Χαράλαμπος Ανθόπουλος, σε αντικατάσταση των τακτικών μελών Λεωνίδα Κοτσαλή, Αναστασίου – Ιωάννη Μεταξά και Δημητρίου Μπριόλα, αντίστοιχα, οι οποίοι αν και εκλήθησαν νομίμως εγγράφως δεν παρέστησαν λόγω κωλύματος. Παρόντες χωρίς δικαίωμα ψήφου ήταν οι Κωνσταντίνος Λιμνιώτης και Ιωάννης Λυκοτραφίτης, πληροφορικοί ελεγκτές, ως βοηθοί εισηγητή, και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η Γενική Γραμματεία Καταναλωτή (εφεξής ΓΓΚ) κοινοποίησε στην Αρχή, με το υπ' αριθμ. πρωτ. …-…./2012 έγγραφό της (αριθμ. πρωτ. Αρχής: Γ/ΕΙΣ/1134/16-02-2012), την καταγγελία που της υποβλήθηκε από τον Α στις 19-01-2012 αναφορικά με την τήρηση των δεδομένων της πιστωτικής του κάρτας από την εταιρεία Groupon Greece Μονοπρόσωπη

Εταιρεία Περιορισμένης Ευθύνης (εφεξής Groupon Ελλάδος), προκειμένου να την εξετάσει στο πλαίσιο των αρμοδιοτήτων της. Ειδικότερα, στην εν λόγω καταγγελία αναφέρεται ότι ο καταγγέλλων διαπίστωσε – κατά τη διαδικασία αγοράς κουπονιού μέσω του διαδικτυακού τόπου της εταιρείας www.groupon.gr - ότι ο αριθμός της πιστωτικής του κάρτας, το ονοματεπώνυμο κατόχου, αλλά και η ημερομηνία λήξης αυτής, ήταν αποθηκευμένα στη βάση δεδομένων της εταιρείας, αφού δεν χρειάστηκε να τα πληκτρολογήσει εκ νέου. Περαιτέρω, με το ως άνω σχετικό έγγραφο κοινοποιήθηκε στην Αρχή η από 19-01-2012 απάντηση που η εταιρεία απέστειλε μέσω ηλεκτρονικού ταχυδρομείου στον καταγγέλλοντα (η οποία απάντηση προωθήθηκε από τον ίδιο στη ΓΓΚ), με την οποία τον ενημέρωσε ότι προέβη στη διαγραφή όλων των δεδομένων των (δύο) πιστωτικών του καρτών.

Σημειώνεται ότι η ΓΓΚ κοινοποίησε επίσης στην Αρχή (αριθμ. πρωτ. Αρχής: Γ/ΕΙΣ/1767/08-03-2012) την υπ' αριθμ. πρωτ. …/.2012 επιστολή που απέστειλε στην εταιρεία προκειμένου να έχει τις απόψεις της, καθώς επίσης και την υπ' αριθμ. πρωτ. …/2012 απάντηση (αριθμ. πρωτ. Αρχής: Γ/ΕΙΣ/2622/09-04-2012) που έλαβε από την εταιρεία, όπου αναφέρεται ότι ικανοποιήθηκε το αίτημα του πελάτη για τη διαγραφή των στοιχείων των δύο πιστωτικών του καρτών από τη βάση δεδομένων της εταιρείας.

Η Αρχή, στο πλαίσιο εξέτασης της εν λόγω υπόθεσης, απέστειλε στην εταιρεία το υπ' αριθμ. πρωτ. Γ/ΕΞ/1134-1/08-03-2012 έγγραφο, με το οποίο ζητούσε μεταξύ άλλων διευκρινίσεις επί των διαδικασιών που ακολουθεί η Groupon Ελλάδος – ως προς την επεξεργασία προσωπικών δεδομένων των πελατών της - για την παροχή των διαδικτυακών της υπηρεσιών. Ακολούθως η Groupon Ελλάδος απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/3796/25-05-2012 έγγραφο, όπου αναφέρει μεταξύ άλλων ότι η επεξεργασία των προσωπικών δεδομένων των πελατών της έχει ανατεθεί στην εταιρεία Groupon GmbH, με έδρα το Βερολίνο, η οποία παρέχει υπηρεσίες αποθήκευσης – φιλοξενίας σε ασφαλή διακομιστή στη Γερμανία. Περαιτέρω, σύμφωνα με το ίδιο έγγραφο, οι υπηρεσίες ηλεκτρονικών πληρωμών (συμπεριλαμβανομένης της συλλογής δεδομένων πιστωτικών καρτών) έχουν ανατεθεί από την εταιρεία Groupon GmbH στην εταιρεία Adyen B.V. (εφεξής Adyen). Ειδικότερα, αναφέρεται ότι η Groupon GmbH δεν τηρεί δεδομένα πιστωτικών καρτών - πάρα μόνο ένα τυχαίο «κλειδί» (token) που παράγεται για κάθε πελάτη την πρώτη φορά που αυτός/αυτή πραγματοποιεί μια ηλεκτρονική αγορά. Το κλειδί αυτό στη συνέχεια διαβιβάζεται από την Groupon GmbH στην Adyen προκειμένου να γίνεται ανεύρεση των στοιχείων των πιστωτικών καρτών του πελάτη, κάθε φορά που αυτός/αυτή πραγματοποιεί κάποια νέα ηλεκτρονική αγορά. Η εταιρεία Adyen με τη σειρά της τηρεί για κάθε πελάτη, εκτός από το παραπάνω τυχαίο κλειδί, τον αριθμό της πιστωτικής κάρτας και την

ημερομηνία λήξης αυτής, αλλά όχι τον τριψήφιο αριθμό CVV/CVC/CCV (Card Verification Value/Card Validation Code/Card Code Verification) που βρίσκεται στο πίσω μέρος της κάρτας: ο αριθμός αυτός χρησιμοποιείται κατά την πρώτη συναλλαγή με τον πελάτη (οπότε και παράγεται το τυχαίο κλειδί) αλλά ουδέποτε αποθηκεύεται. Σημειώνεται επίσης στο ως άνω έγγραφο ότι τόσο η Groupon GmbH όσο και η εταιρεία Adyen συμμορφώνονται με το διεθνές πρότυπο ασφαλείας PCI-DSS (Payment Card Industry Data Security Standard).

Η εταιρεία απέστειλε επίσης στην Αρχή, με το ως άνω έγγραφο, τη σύμβαση με τη γερμανική εταιρεία Groupon GmbH. Επισημαίνεται ότι, σύμφωνα με τους όρους της σύμβασης, η επεξεργασία πραγματοποιείται εντός της Ομοσπονδιακής Δημοκρατίας της Γερμανίας ή κράτους εντός της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Οικονομικού Χώρου. Στο ίδιο έγγραφο επίσης επισυνάπτεται λίστα υπεργολάβων εταιρειών, όπου για την παροχή υπηρεσιών ηλεκτρονικών εισπράξεων (συμπεριλαμβανομένων της συλλογής/φιλοξενίας δεδομένων πιστωτικών καρτών) αναφέρονται, πέραν της Adyen, οι: α) Telephonica GmbH (φύλαξη των διακομιστών οι οποίοι τηρούν τα υπό επεξεργασία δεδομένα), β) Experian CheetahMail Deutchland GmbH (παροχή υπηρεσιών σχετικών με την αποστολή e-mail στους πελάτες).

Επιπρόσθετα, υποβλήθηκε στην Αρχή η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4692/03-07-2012 καταγγελία από τον Β σχετικά με αποστολή αζήτητης ηλεκτρονικής επικοινωνίας (spam) μέσω ηλεκτρονικού ταχυδρομείου από την Groupon Ελλάδος. Σημειώνεται ότι, βάσει της υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5646/23-08-2011 παλαιότερης καταγγελίας, η Αρχή έχει ήδη ενημερώσει την Groupon Ελλάδος, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/1534/01-03-2012 έγγραφο, σχετικά με τις προϋποθέσεις νομιμότητας που πρέπει να πληρούνται για την αποστολή διαφημιστικών μηνυμάτων.

Με την υπ' αριθμ. πρωτ. Γ/ΕΞ/4734/04-07-2012 εντολή του Προέδρου της Αρχής, διατάχθηκε η διενέργεια ελέγχου στη Groupon Ελλάδος. Ο έλεγχος πραγματοποιήθηκε στις 11-07-2012 στις εγκαταστάσεις της εταιρείας στην οδό Αιγιαλείας 54, στο Μαρούσι, από τους υπαλλήλους του Τμήματος Ελεγκτών της Γραμματείας της Αρχής Κωνσταντίνο Λιμνιώτη και Ιωάννη Λυκοτραφίτη (εφεξής «ομάδα ελέγχου»). Ο έλεγχος επικεντρώθηκε στα ζητήματα που σχετίζονται με τις ανωτέρω καταγγελίες, ήτοι α) στην επεξεργασία των προσωπικών δεδομένων των πελατών της Groupon Ελλάδος, και ειδικότερα στην επεξεργασία δεδομένων πιστωτικών καρτών και στην ασφάλεια των συναλλαγών, και β) στις διαδικασίες που ακολουθούνται προκειμένου να διασφαλίζεται η νόμιμη αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από την εταιρεία.

Κατά τον επιτόπιο έλεγχο, η ομάδα ελέγχου πραγματοποίησε συνεντεύξεις με διοικητικά

στελέχη της εταιρείας. Επίσης, στο πλαίσιο του ελέγχου, έγινε επίδειξη των εφαρμογών που χρησιμοποιούν οι υπάλληλοι της εταιρείας, και συγκεκριμένα του συστήματος διαχείρισης πελατών (περιλαμβάνει προσωπικά στοιχεία πελατών και στοιχεία για τις αγορές τους), καθώς και του συστήματος διαχείρισης στοιχείων πληρωμών των πελατών (μέσω ασφαλούς διαδικτυακής σύνδεσης με τους διακομιστές της Adyen). Περαιτέρω, έγινε επίδειξη της ιστοσελίδας που εμφανίζεται σε έναν εγγεγραμμένο και αυθεντικοποιημένο χρήστη όταν προβαίνει σε αγορά κάποιου κουπονιού. Αναφορικά με τα ανωτέρω, ζητήθηκε από τον υπεύθυνο επεξεργασίας να παραδώσει μια σειρά ηλεκτρονικών πειστηρίων (εφεξής Πειστήρια), τα οποία εμπεριέχουν αντιπροσωπευτικά δείγματα οθόνης (screenshots).

Μετά από την ολοκλήρωση του ελέγχου, η ομάδα ελέγχου συνέταξε τα Πρακτικά του ελέγχου (εφεξής Πρακτικά), στα οποία καταγράφονται οι απαντήσεις/διευκρινίσεις του υπεύθυνου επεξεργασίας, καθώς και επιτόπιες παρατηρήσεις της ομάδας ελέγχου. Το σχέδιο Πρακτικών εστάλη με το υπ' αριθμ. πρωτ. Γ/ΕΞ/4970/17-07-2012 έγγραφο της Αρχής στον υπεύθυνο επεξεργασίας για υποβολή σχολίων ή/και παρατηρήσεων. Με το ίδιο έγγραφο η Αρχή ζήτησε κάποιες συμπληρωματικές διευκρινίσεις αναφορικά με τις διαδικασίες που ακολουθούνται από την εταιρεία Adyen για τη διεκπεραίωση ηλεκτρονικών πληρωμών. Ο υπεύθυνος επεξεργασίας απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6415/10-10-2012 έγγραφο, οπότε και τα Πρακτικά – λαμβάνοντας υπόψη και τα σχόλια του υπεύθυνου επεξεργασίας – οριστικοποιήθηκαν με το με αρ. πρωτ. Γ/ΕΞ/6969/31-10-2012 έγγραφο της Αρχής.

Στη συνέχεια, η ομάδα ελέγχου μελέτησε τα Πρακτικά σε συνδυασμό με τα Πειστήρια και συνέταξε Πόρισμα, το οποίο υπέβαλε στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/146/11-01-2013 έγγραφο. Όπως διαπιστώνεται από το Πόρισμα και καταγράφεται στα ευρήματα:

- Οι πελάτες της Groupon δεν ενημερώνονται για το γεγονός ότι δεδομένα της πιστωτικής τους κάρτας τηρούνται από την εταιρεία Adyen.
- Οι πελάτες της Groupon δεν ενημερώνονται για το γεγονός ότι κανένα στοιχείο της πιστωτικής τους κάρτας (συμπεριλαμβανομένου του τριψήφιου αριθμού CVV/CVC/CCV) δεν θα τους ζητηθεί εκ νέου σε επόμενες αγορές τους. Σημειώνεται ότι, για την πραγματοποίηση μιας ηλεκτρονικής αφοράς, απαιτείται μόνο η σύνδεση στον ηλεκτρονικό λογαριασμό του πελάτη στην ιστοσελίδα του υπεύθυνου επεξεργασίας, χωρίς να πραγματοποιείται κανένας περαιτέρω έλεγχος (π.χ. επιβεβαίωση των στοιχείων της πιστωτικής κάρτας μέσω ελέγχου του τριψήφιου CCV/CVC/CCV). Ως εκ τούτου, ενδεχόμενη διαρροή του κωδικού πρόσβασης (που χρησιμοποιεί ένας πελάτης για τη σύνδεσή του στην ιστοσελίδα της εταιρείας) σε κάποιον τρίτο, θα επιτρέψει στον τελευταίο την

πραγματοποίηση αγοράς με χρέωση της πιστωτικής κάρτας του πελάτη, ακόμα και αν δεν γνωρίζει κανένα στοιχείο της πιστωτικής κάρτας.

- Ως άμεσο επακόλουθο των ανωτέρω, δεν λαμβάνεται από τους πελάτες η ρητή συγκατάθεσή τους για την ως άνω επεξεργασία (ήτοι την τήρηση στοιχείων της πιστωτικής τους κάρτας, καθώς και τη συνεπαγόμενη δυνατότητα πραγματοποίησης μελλοντικών αγορών βάσει αυτών).
- Ο υπεύθυνος επεξεργασίας πραγματοποιεί αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε άτομα που έχουν δηλώσει ρητά ότι δεν επιθυμούν τη λήψη τέτοιων μηνυμάτων.

Η εταιρεία Groupon Greece Μονοπρόσωπη Εταιρεία Περιορισμένης Ευθύνης κλήθηκε, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/4235/20-06-2013 έγγραφο της Αρχής, νομίμως σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 02-07-2013 για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει τις απόψεις της επί των καταγγελλομένων. Το ως άνω πόρισμα του ελέγχου επιδόθηκε επίσης στην εταιρεία, μαζί με την κλήση της από την Αρχή για ακρόαση. Στη συνεδρίαση της Αρχής, την 02-07-2013, παρέστησαν νομίμως, ως εκπρόσωποι της εταιρείας, ο Γ, ιδιοκτήτης αυτής, και η Αγγελική Γιαννακάκου, δικηγόρος Κατά την ακρόαση, οι εκπρόσωποι της εταιρείας, εξέθεσαν προφορικά τις απόψεις τους. Κατόπιν της ακρόασης, η εταιρεία κατέθεσε εμπροθέσμως σχετικό υπόμνημα με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4624/09-07-2013 έγγραφο, εκθέτοντας και εγγράφως τις απόψεις της. Στο υπόμνημά της η εταιρεία αναφέρει τα εξής:

α) Αναφορικά με την τήρηση των δεδομένων της κάρτας για μελλοντικές αγορές, έχει προστεθεί, στην ιστοσελίδα που εμφανίζεται στο χρήστη κατά την αγορά/πληρωμή, σχετικό κείμενο ενημέρωσης σε ήδη υπάρχον κείμενο για την αποδοχή των όρων χρήσης. Μέσω αυτού, ο χρήστης ενημερώνεται και συγκατατίθεται στην τήρηση των στοιχείων της πιστωτικής/χρεωστικής του κάρτας και για χρήση σε μελλοντικές αγορές μέσω επιλογής στο σχετικό κουτί ελέγχου («τικ» σε κουτάκι δίπλα στο κείμενο που είναι το ίδιο με την έκφραση αποδοχής των όρων χρήσης). Ειδικότερα, όπως προκύπτει και από το στιγμιότυπο οθόνης που επισυνάπτεται στο ως άνω υπόμνημα, στο κείμενο αυτό αναφέρεται το εξής: «*Βεβαιώνω ότι είμαι άνω των 18 ετών και ότι έχω διαβάσει και συμφωνώ με τους όρους χρήσης καθώς και με την τήρηση των ανωτέρω στοιχείων πληρωμής για χρήση σε μελλοντικές αγορές μου*».

Περαιτέρω, η εταιρεία διευκρινίζει ότι ακόμα κι αν υπάρξει περιστατικό παραβίασης του συνθηματικού πρόσβασης ενός χρήστη, αφενός δεν θα μπορεί να γίνει γενικευμένη χρήση των στοιχείων της κάρτας αυτού, παρά μόνο πραγματοποίηση αγορών με χρήση

της κάρτας μέσω της ιστοσελίδας της εταιρείας, αφετέρου στην περίπτωση αυτή ο κάτοχος της κάρτας θα μπορεί να αμφισβητήσει τη συναλλαγή και το αίτημά του θα γίνει αποδεκτό από την εταιρεία χωρίς καμία επιβάρυνση.

β) Αναφορικά με την αποστολή αζήτητης ηλεκτρονικής αλληλογραφίας, η εταιρεία από το Μάρτιο του 2013 έχει ανανεώσει το σύστημα εγγραφής/αποεγγραφής στο ενημερωτικό της δελτίο (newsletter), έτσι ώστε ο κάθε χρήστης να μπορεί να επιλέγει το είδος των ενημερωτικών δελτίων που θα λαμβάνει, καθώς επίσης και να ζητήσει να μη λαμβάνει κανένα. Περαιτέρω, δυνατότητα διαγραφής από τη λίστα παραληπτών ενημερωτικών δελτίων δίνεται και μέσω των σχετικών μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποστέλλονται στους χρήστες που τα έχουν αιτηθεί. Η εταιρεία, τέλος, διευκρινίζει ότι δεν έχει αποστείλει ποτέ διαφημιστικά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου σε άτομα που δεν έχουν δώσει τη συγκατάθεσή τους, ενώ το σχετικό πρόβλημα που υπήρχε παλαιότερα (αναφορικά με το γεγονός ότι, αν κάποιος πραγματοποιούσε μία αγορά μέσω της ιστοσελίδας της εταιρείας, τότε θα λάμβανε στο μέλλον διαφημιστικά μηνύματα, ακόμα και αν προ της αγοράς είχε δηλώσει ότι δεν επιθυμούσε τη λήψη αυτών) έχει διορθωθεί.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων, αφού αναγνώστηκαν τα πρακτικά της συνεδρίασης της 02/07/2013, άκουσε τον εισηγητή και τους βοηθούς εισηγητή, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Σύμφωνα με το άρθρο 5 παρ. 1 του ν. 2472/1997, η επεξεργασία δεδομένων προσωπικού χαρακτήρα (στα οποία συγκαταλέγονται και τα δεδομένα πιστωτικών καρτών) επιτρέπεται μόνο όταν το υποκείμενο έχει δώσει τη συγκατάθεσή του, εκτός εάν συντρέχει μία από τις προβλεπόμενες από την παράγραφο 2 του ιδίου άρθρου εξαιρέσεις, οπότε είναι νόμιμη η επεξεργασία και χωρίς τη συγκατάθεση του υποκειμένου. Σημειώνεται ότι, σύμφωνα με το άρθρο 2 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*».

Στη συγκεκριμένη περίπτωση, αναφορικά με την τήρηση στοιχείων των πιστωτικών καρτών των πελατών της εταιρείας και τη δυνατότητα που τους παρέχεται, ως εγγεγραμμένοι χρήστες, να πραγματοποιούν αγορές μέσω του διαδικτυακού τόπου της εταιρείας χωρίς να επανεισάγουν κάθε φορά τα στοιχεία της κάρτας τους, σημειώνεται ότι η πραγματοποίηση μίας αγοράς από κάποιον εγγεγραμμένο χρήστη δεν μπορεί να θεωρηθεί ως ελεύθερη, ρητή και ειδική βούλησή του για την εν λόγω επεξεργασία που εκφράζεται εν πλήρη επιγνώσει, διότι δεν έχει προηγουμένως ενημερωθεί για τα βασικά χαρακτηριστικά αυτής (βλ. και επόμενη Σκέψη 2). Συνεπώς, το σύννομο της εν λόγω επεξεργασίας θα πρέπει να κριθεί με βάση τη διάταξη του άρθρου 5 παρ. 2 στοιχ. ε) του ν. 2472/1997, αφού δεν συντρέχει άλλος λόγος επεξεργασίας από όσους αναφέρονται στο ίδιο άρθρο. Σύμφωνα με την εν λόγω διάταξη, κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς συγκατάθεση όταν «*η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας (…), και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών*». Ωστόσο, για τη συγκεκριμένη περίπτωση, επισημαίνεται ότι η εν λόγω επεξεργασία δεν είναι απολύτως αναγκαία για την πραγματοποίηση της αγοράς, αφού μπορεί να πραγματοποιηθεί και χωρίς αυτή. Κατά συνέπεια, λαμβάνοντας επίσης υπόψη και τους κινδύνους όπως αναλύονται στη συνέχεια στη Σκέψη 3, δεν πληρούνται οι προϋποθέσεις του άρθρου 5 παρ. 2 στοιχ. ε).

2. Σύμφωνα με το άρθρο 11 του ν. 2472/1997 ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει τα υποκείμενα των δεδομένων, με τρόπο πρόσφορο και σαφή, για τα βασικά χαρακτηριστικά της επεξεργασίας καθώς και για τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων τους.

Στη συγκεκριμένη περίπτωση, για το γεγονός ότι μετά την πρώτη αγορά που θα πραγματοποιήσει ένας πελάτης μέσω πιστωτικής/χρεωστικής κάρτας δεν θα του ζητηθεί στο μέλλον, σε επόμενη αγορά, η επανεισαγωγή των στοιχείων της κάρτας του, που αποτελεί βασικό χαρακτηριστικό της επεξεργασίας, δεν παρέχεται σαφής προηγούμενη ενημέρωση προς τους πελάτες/κατόχους των καρτών (πέραν μίας γενικής διατύπωσης στην Πολιτική Απορρήτου στο διαδικτυακό τόπο της εταιρείας, όπου αναφέρεται ότι «(…) *δυνάμεθα να διαθέσουμε τις προσωπικές πληροφορίες σας σε αντιπροσώπους και υπεργολάβους μας προκειμένου να διευκολυνθεί οποιαδήποτε χρήση των δεδομένων σας που αναφέρεται στην παρούσα Πολιτική. Για παράδειγμα, δυνάμεθα να χρησιμοποιήσουμε τρίτα μέρη να μας παρέχουν υπηρεσίες προώθησης προϊόντων ή υπηρεσίες εξυπηρέτησης πελατών ή να τις αποστείλουμε σε πάροχο πιστωτικών καρτών προκειμένου να επεξεργαστεί μία πληρωμή*») –

οπότε και, κατ' επέκταση, δεν ζητείται και η ρητή συγκατάθεσή τους για αυτή την επεξεργασία.

Όπως δήλωσε η εταιρεία στο υπ΄ αριθμ. πρωτ. Γ/ΕΙΣ/4624/09-07-2013 υπόμνημά της, πλέον έχει προστεθεί, στην ιστοσελίδα που εμφανίζεται στο χρήστη κατά την αγορά/πληρωμή, σχετικό κείμενο ενημέρωσης σε ήδη υπάρχον κείμενο για την αποδοχή των όρων χρήσης, μέσω του οποίου, ο χρήστης ενημερώνεται στην τήρηση των στοιχείων της πιστωτικής/χρεωστικής του κάρτας και για χρήση σε μελλοντικές αγορές.

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. Στο ίδιο άρθρο αναφέρεται ότι ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

Ειδικά για την ασφάλεια σε ηλεκτρονικές πληρωμές, σημείο αναφοράς αποτελεί το διεθνώς αναγνωρισμένο πρότυπο ασφαλείας Payment Card Industry Data Security Standard (PCI/DSS). Το PCI/DSS αναπτύχθηκε από το ανοιχτό παγκόσμιο forum Payment Card Industry Security Standards Council για να ενισχύσει την ασφάλεια των δεδομένων του κατόχου πιστωτικών καρτών μέσω της υιοθέτησης ενιαίων μέτρων ασφαλείας παγκοσμίως. Το πρότυπο αυτό απευθύνεται σε όλους τους φορείς που εμπλέκονται στην επεξεργασία πληρωμών με πιστωτική κάρτα, συμπεριλαμβανομένων των εμπόρων, των φορέων παροχής υπηρεσιών, καθώς και όλων των μερών που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα κατόχων καρτών[1]. Σημειώνεται ότι το πρότυπο PCI/DSS προβλέπει ότι ο τριψήφιος αριθμός ασφαλείας που βρίσκεται στο πίσω μέρος της κάρτας δεν πρέπει να αποθηκεύεται.

Η Αρχή κρίνει ότι η συμμόρφωση με το πρότυπο PCI/DSS αποτελεί απαραίτητη προϋπόθεση για την κατ' ελάχιστο εκπλήρωση των όρων του άρθρου 10 του ν. 2472/1997. Στη συγκεκριμένη περίπτωση, τόσο η Groupon GmbH όσο και η Adyen συμμορφώνονται με το ως άνω πρότυπο. Επίσης, σημειώνεται ότι η διαδικτυακή σύνδεση των εξουσιοδοτημένων υπαλλήλων της Groupon Ελλάδος με τους διακομιστές της Groupon GmbH και της Adyen

[1] https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

είναι κρυπτογραφημένη (χρήση πρωτοκόλλου HTTPS).

Ωστόσο, το γεγονός ότι, μετά την πρώτη αγορά που θα πραγματοποιήσει ένας χρήστης, δεν θα του ζητηθεί εκ νέου, σε καμία επόμενή του αγορά, να εισάγει τα στοιχεία της πιστωτικής του κάρτας (συμπεριλαμβανομένου μάλιστα και του τριψήφιου αριθμού ασφαλείας, ο οποίος – παρόλο που δεν αποθηκεύεται, σε συμμόρφωση με το PCI/DSS πρότυπο - δεν θα του ζητηθεί ξανά), αυξάνει τους κινδύνους ως προς την ασφάλεια της επεξεργασίας – ιδίως δε σε συνδυασμό με το ότι δεν παρέχεται από τον υπεύθυνο επεξεργασίας προς τους πελάτες σχετική ενημέρωση για αυτό. Και τούτο διότι ενδεχόμενη διαρροή του κωδικού πρόσβασης (συνθηματικού) που χρησιμοποιεί ένας χρήστης (για τη σύνδεσή του στο διαδικτυακό τόπο της εταιρείας) σε κάποιον τρίτο, θα επιτρέψει στον τελευταίο την πραγματοποίηση αγοράς με χρέωση της πιστωτικής κάρτας του πελάτη, ακόμα και αν δεν γνωρίζει κανένα στοιχείο της κάρτας αυτής.

4. Σύμφωνα με το άρθρο 11 παρ. 1 του ν. 3471/2006, όπως τροποποιήθηκε και ισχύει, η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς. Περαιτέρω, σύμφωνα με την παρ. 3 του ίδιου άρθρου, τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμα και όταν ο αποδέκτης δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό κατά τη συλλογή των στοιχείων επαφής, καθώς και σε κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.

Στη συγκεκριμένη περίπτωση, η Groupon Ελλάδος απέστελλε διαφημιστικά μηνύματα σε πελάτες που είχαν πραγματοποιήσει αγορά μέσω του διαδικτυακού τόπου της εταιρείας και είχαν δηλώσει ότι δεν επιθυμούν τη λήψη τέτοιων μηνυμάτων (είτε ρητά είτε μη επιλέγοντας κατά την αγορά το σχετικό πεδίο ελέγχου δήλωσης επιθυμίας λήψης μηνυμάτων), κατά παράβαση της ανωτέρω διάταξης και παρά το γεγονός ότι η Αρχή έχει ήδη ενημερώσει τον υπεύθυνο επεξεργασίας σχετικά με τις προϋποθέσεις νόμιμης προώθησης προϊόντων/υπηρεσιών με το υπ’ αριθμ. πρωτ. Γ/ΕΞ/1534/01-03-2012 έγγραφό της. Η εταιρεία, με το υπ΄ αριθμ. πρωτ. Γ/ΕΙΣ/4624/09-07-2013 υπόμνημά της, δηλώνει ότι πλέον η

πρακτική αυτή έχει εγκαταλειφθεί.

Συνεπώς η εταιρεία Groupon Greece παραβίασε τις διατάξεις των άρθρων 5, 10 και 11 του ν. 2472/1997 και του άρθρου 11 του ν. 3471/2006 και, λαμβάνοντας υπόψη και το άρθρο 13 του ν. 3471/2006, συντρέχουν οι προϋποθέσεις επιβολής σε βάρος της των κατ' άρθρο 21 παρ. 1 α και β΄ του ν. 2472/1997 διοικητικών κυρώσεων, λαμβανομένων υπόψη και των ανωτέρω ενεργειών στις οποίες προέβη προς αποκατάσταση της νομιμότητας και συμμόρφωση προς τις υποχρεώσεις που επιβάλλουν οι ανωτέρω διατάξεις.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

1) Επιβάλλει στη Groupon Greece Μονοπρόσωπη Εταιρεία Περιορισμένης Ευθύνης, πρόστιμο χιλίων πεντακοσίων Ευρώ (1.500€) για παραβίαση του άρθρου 11 του ν. 3471/2006.

2) Απευθύνει προειδοποίηση στην Groupon Greece Μονοπρόσωπη Εταιρεία Περιορισμένης Ευθύνης να προβεί στις κάτωθι ενέργειες, καθώς επίσης και να ενημερώσει σχετικά την Αρχή, αναφορικά με την εκπλήρωση των υποχρεώσεών της που τίθενται στα άρθρα 5, 10 και 11 του ν. 2472/1997:

- Να ζητά τη ρητή συγκατάθεση των πελατών της για την επεξεργασία δεδομένων των πιστωτικών/χρεωστικών τους καρτών, αναφορικά με την τήρηση δεδομένων της πιστωτικής τους κάρτας κατά τρόπο τέτοιο ώστε να παρέχεται η δυνατότητα στο να πραγματοποιούν αγορές χωρίς να χρειάζεται να επανεισάγουν τα στοιχεία των πιστωτικών τους καρτών. Προκειμένου η συγκατάθεση για αυτήν ακριβώς την επεξεργασία να είναι ελεύθερη, θα πρέπει να δίνεται στους χρήστες η δυνατότητα να επιλέξουν ρητώς εάν επιθυμούν να απολαύουν αυτής της υπηρεσίας ή αν αντίθετα επιθυμούν να εισάγουν, κάθε φορά που πραγματοποιούν μία νέα αγορά, τα στοιχεία της κάρτας τους. Ως εκ τούτου, η σχετική δήλωση συγκατάθεσης των χρηστών θα πρέπει να είναι διακριτή από άλλες δηλώσεις συγκατάθεσης (ήτοι να υπάρχει ξεχωριστό κείμενο το οποίο να περιγράφει σαφώς τη δυνατότητα τήρησης στοιχείων κάρτας για μελλοντικές αγορές), χωρίς να είναι υποχρεωτικό για το χρήστη, προκειμένου να πραγματοποιήσει κάποια αγορά, να επιλέξει το σχετικό πεδίο.

Τέλος, η Αρχή απευθύνει σύσταση στην Groupon Greece Μονοπρόσωπη Εταιρεία Περιορισμένης Ευθύνης να ενημερώνει με τρόπο πρόσφορο και σαφή τους πελάτες για τη

σημασία της επιλογής κωδικού πρόσβασης (συνθηματικού), και να εφαρμόζει επίσης κανόνες για να αποτρέπεται - κατά το δυνατόν - η επιλογή εύκολα προβλέψιμων συνθηματικών από τους χρήστες (π.χ. καθορισμός ελάχιστου επιτρεπτού μήκους, υποχρεωτική χρήση μη αλφαριθμητικών χαρακτήρων κτλ.).

Ο Αναπληρωτής Πρόεδρος	**Η γραμματέας**
Γεώργιος Μπατζαλέξης	**Ειρήνη Παπαγεωργοπούλου**