Αθήνα, 04-08-2017
Αριθ. Πρωτ. Γ/ΕΞ/5929/04-08-2017

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Γ Ν Ω Μ Ο Δ Ο Τ Η Σ Η 4/2017

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε στην έδρα της τη Δευτέρα 17.07.2017 και ώρα 10:00 σε έκτακτη συνεδρίαση, 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, Σπυρίδων Βλαχόπουλος, Κωνσταντίνος Λαμπρινουδάκης, ως εισηγητής, Χαράλαμπος Ανθόπουλος και Ελένη Μαρτσούκου, επίσης ως εισηγήτρια. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, η Φ. Καρβέλα, δικηγόρος-νομική ελέγκτρια και ο Κ. Λιμνιώτης, πληροφορικός ελεγκτής, ως βοηθοί εισηγητών, οι οποίοι παρέσχαν διευκρινίσεις και αποχώρησαν πριν από τη διάσκεψη και τη λήψη απόφασης, ενώ απουσίαζε, λόγω κωλύματος, ο βοηθός εισηγητών Λεωνίδας Ρούσσος. Επίσης παρέστη, με εντολή Προέδρου, η Γεωργία Παλαιολόγου, υπάλληλος του Διοικητικού-Οικονομικού Τμήματος της Αρχής, ως γραμματέας.

Η Αρχή συνεδρίασε προκειμένου να γνωμοδοτήσει, σύμφωνα με το άρθρο 19 παρ. 1 στοιχ. θ΄ του ν. 2472/1997, επί της υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/1570/02-06-2017 γνωστοποίησης επεξεργασίας προσωπικών δεδομένων –όπως αυτή συμπληρώθηκε– που υπέβαλε ο Οργανισμός Αστικών Συγκοινωνιών Αθηνών Α.Ε. (εφεξής ΟΑΣΑ ή υπεύθυνος επεξεργασίας, κατά την έννοια του άρ. 2 στοιχ. ζ΄ του ν. 2472/1997), σε συνέχεια της υπ' αριθμ. 1/2017 Γνωμοδότησης της Αρχής, στο πλαίσιο του νέου

Αυτομάτου Συστήματος Συλλογής Κομίστρου (εφεξής ΑΣΣΚ) στο οποίο γίνεται αναφορά και με τον όρο «ηλεκτρονικό εισιτήριο». Με την ως άνω γνωστοποίηση ο ΟΑΣΑ ανακάλεσε την υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/2139/15-09-2016 γνωστοποίηση επεξεργασίας προσωπικών δεδομένων επί της οποίας η Αρχή είχε εκδώσει την ως άνω Γνωμοδότηση, υποβάλλοντας νέα τροποποιημένη γνωστοποίηση και δηλώνοντας ότι ουδέποτε τέθηκε σε λειτουργία το ΑΣΣΚ με τις αναφερόμενες στην προηγούμενη γνωστοποίηση ρυθμίσεις.

Σύμφωνα με τη νέα γνωστοποίηση του ΟΑΣΑ, το ΑΣΣΚ θα υποστηρίζει δύο μέσα κομίστρου υπό τη μορφή ηλεκτρονικών «έξυπνων καρτών», τα οποία είναι:

- «Πολλαπλό»: Έξυπνη κάρτα χωρίς επαφή (Contactless Smart Card-SC) στην οποία θα αποθηκεύονται κόμιστρα μικρής αξίας (εισιτήρια)
- «Κάρτα»: Έξυπνη Κάρτα χωρίς επαφή (Contactless Smart Card - SC) με μικροεπεξεργαστή η οποία θα υλοποιεί διάφορα προϊόντα κομίστρου, για παράδειγμα: τα προϊόντα απεριορίστων διαδρομών, μεγάλης διάρκειας ή μεγάλης αποθηκευμένης αξίας.

Όπως επισημαίνει ο ΟΑΣΑ στην ως άνω γνωστοποίησή του, «η Κάρτα δύναται να είναι είτε απρόσωπη είτε προσωποποιημένη. Στην κάρτα θα αποθηκεύεται χρηματική αξία (stored value), εισιτήρια ή κάρτες απεριορίστων διαδρομών. Οι απρόσωπες Κάρτες και τα Πολλαπλά εισιτήρια αποτελούν τη συντριπτική πλειοψηφία (άνω του 90%) των μέσων κομίστρου που θα διακινούνται στο ΑΣΣΚ, ενώ η προσωποποιημένη Κάρτα θα υποκαταστήσει κυρίως τις υφιστάμενες μηνιαίες, τριμηνιαίες, εξαμηνιαίες, ετήσιες κάρτες και ελευθέρας».

Η σχεδίαση του νέου συστήματος που υποστηρίζει τη λειτουργία του ΑΣΣΚ θεωρεί ως βασική οντότητα την κάρτα και όχι τον επιβάτη. Ως εκ τούτου, όλες οι λειτουργίες του συστήματος (ήτοι έκδοση, φόρτιση και επικύρωση) χρησιμοποιούν ως μοναδικό στοιχείο καταχώρισης και επεξεργασίας τον αριθμό της κάρτας (οποιουδήποτε τύπου) και όχι τα στοιχεία του επιβάτη. Επιπλέον, προκειμένου να εκτελεστεί οποιαδήποτε συναλλαγή φόρτισης ή επικύρωσης, δεν απαιτείται ταύτιση με φυσικό πρόσωπο (κάτοχο προσωποποιημένης κάρτας). Το σύστημα μπορεί να διαχειρίζεται κατά τρόπο ενιαίο τόσο τις προσωποποιημένες όσο και τις ανώνυμες κάρτες. Η ανάγκη συστημικής αντιστοίχισης της κάρτας με φυσικό πρόσωπο προκύπτει αποκλειστικά

από την ανάγκη υλοποίησης των διαδικασιών:
α) αντικατάστασης απολεσθείσας κάρτας με ταυτόχρονη μεταφορά του υπολοίπου στη νέα κάρτα και ακύρωσης της παλαιάς
β) αμφισβήτησης των χρεώσεων.
Όπως επισημαίνει ο ΟΑΣΑ, η μεταφορά υπολοίπου αποτελεί ένα από τα βασικότερα πλεονεκτήματα του νέου συστήματος σε σύγκριση με το προηγούμενο που δεν μπορούσε να την υποστηρίξει και διασφαλίζει τη μη απώλεια των πληρωμένων από τον επιβάτη δικαιωμάτων (προϊόντων κομίστρου ή/και χρηματική αξία) ενώ η ακύρωση της απολεσθείσας κάρτας είναι μια δυνατότητα που περιορίζει την απώλεια εσόδων του οργανισμού (καθιστώντας άμεσα μη αξιοποιήσιμη την απολεσθείσα κάρτα).

Για την έκδοση κάρτας απεριορίστων διαδρομών των χρηστών του ΑΣΣΚ, ο ΟΑΣΑ επιλέγει τη χρήση κρυπτογραφικού αλγορίθμου κατακερματισμού (hashing) των προσωπικών δεδομένων των χρηστών. Κάθε καταγραφή δεδομένων κίνησης των προσωποποιημένων καρτών δεν θα παραπέμπει σε συγκεκριμένο πρόσωπο αλλά σε ένα «ψηφιακό αποτύπωμα» (hash value) όπως αυτό υπολογίζεται από τη συνάρτηση κατακερματισμού. Το ψηφιακό αποτύπωμα θα προκύπτει από το συνδυασμό του ΑΜΚΑ και ενός 4-ψήφιου κωδικού ασφαλείας (για Έλληνες πολίτες) ή του αριθμού διαβατηρίου και ενός 4-ψήφιου κωδικού ασφαλείας (για αλλοδαπούς). Ο 4-ψήφιος κωδικός ασφαλείας θα καταχωρίζεται (πληκτρολογείται) από τον επιβάτη κατά τη διαδικασία προσωποποίησης και θα απαιτείται προκειμένου να ανακτηθούν τα στοιχεία της κάρτας (σε περίπτωση απώλειας). Ο κωδικός αυτός θα είναι γνωστός μόνο στον επιβάτη και ο συνδυασμός του με τον ΑΜΚΑ για την παραγωγή του μη αναστρέψιμου ψηφιακού αποτυπώματος εξασφαλίζει ότι ούτε χρήστες με γνώση της δομής του συστήματος και διαβαθμισμένη πρόσβαση στα δεδομένα αυτού θα είναι σε θέση να προσδιορίσουν την αντιστοιχία αριθμού κάρτας με τον ΑΜΚΑ (και κατά συνέπεια την ταυτότητα) του επιβάτη.

Για τις ειδικές κατηγορίες χρηστών (δηλαδή ανέργους, φοιτητές, ΑΜΕΑ κ.λπ.), επειδή η κάρτα έχει περαιτέρω έκπτωση και πρέπει να αποκλειστεί η περίπτωση έκδοσης περισσοτέρων καρτών ανά άτομο, πέραν της ως άνω διαδικασίας και επεξεργασίας, θα τηρείται ένα αρχείο δεδομένων με μόνο στοιχείο τον ΑΜΚΑ του χρήστη και την ημερομηνία λήξης του ειδικού δικαιώματος (π.χ. χρόνος ανεργίας,

λήξη θητείας κ.λπ.). Στο αρχείο αυτό δεν θα υφίσταται άλλη πληροφορία ούτε θα μπορεί να πραγματοποιείται διασύνδεσή του με άλλο αρχείο. Σκοπός του θα είναι μόνον η παρεμπόδιση χρήσης του ίδιου ΑΜΚΑ για έκδοση δεύτερης κάρτας ειδικής κατηγορίας. Επομένως, για τον ΟΑΣΑ αρκεί η καταχώριση του αριθμού ΑΜΚΑ προκειμένου να μην είναι δυνατόν ο ήδη χρήστης/νόμιμος κάτοχος κάρτας να προβεί σε έκδοση περισσοτέρων (πολλαπλασιασμό της). Με βάση τα ανωτέρω, ο ΟΑΣΑ τηρεί αρχείο προσωπικών δεδομένων με το συγκεκριμένο περιεχόμενο και για το συγκεκριμένο σκοπό και προβαίνει μόνο στην απολύτως απαραίτητη επεξεργασία του δεδομένου, δηλαδή του ΑΜΚΑ, μόνο για τον σκοπό της αποτροπής χρήσης του ίδιου ΑΜΚΑ για έκδοση δεύτερης κάρτας ειδικών κατηγοριών.

Η διαδικασία της έκδοσης της κάρτας δεν απαιτεί οποιαδήποτε αποθήκευση προσωπικών δεδομένων σε τοπικό (Τερματικό Έκδοσης Καρτών – ΤΕΚ) ή κεντρικό επίπεδο πλην της καταχώρισης του ΑΜΚΑ για τις ειδικές κατηγορίες. Επομένως, ο σκοπός του ΟΑΣΑ να παρέχει ένα ηλεκτρονικό σύστημα έκδοσης και χρήσης εισιτηρίου πραγματοποιείται χωρίς τη δυνατότητα αντιστοίχισης των κινήσεων της κάρτας με τον χρήστη της και τηρείται μόνο το δεδομένο του ΑΜΚΑ με ημερομηνία λήξης του δικαιώματος για τις ειδικές κατηγορίες χωρίς οποιαδήποτε αντιστοίχιση με άλλη πληροφορία. Το αρχείο κίνησης/συναλλαγής των καρτών και των ανωνύμων κομίστρων είναι ως εκ τούτου –κατά τον ΟΑΣΑ– ανωνυμοποιημένο και δεν υφίσταται οποιαδήποτε δυνατότητα προσωποποίησης της διαδρομής χωρίς τη συμβολή του χρήστη της κάρτας.

Ειδικότερα, για την έκδοση προσωποποιημένης κάρτας από Τερματικό Έκδοσης Καρτών (ΤΕΚ) απαιτείται η προσκόμιση επίσημου εγγράφου που να προσδιορίζει τον αριθμό ΑΜΚΑ του επιβάτη, καθώς και της αστυνομικής του ταυτότητας. Εναλλακτικά, για αλλοδαπούς, απαιτείται η προσκόμιση έγκυρου διαβατηρίου. Εφόσον ο επιβάτης ανήκει σε ειδική κατηγορία, οφείλει να προσκομίσει και έγγραφο απόδειξης του δικαιώματός του. Ο εκδότης οφείλει να εισάγει στην εφαρμογή του ΤΕΚ τον ΑΜΚΑ, το όνομα, το επώνυμο καθώς και τον μήνα και έτος γέννησης και την ειδική κατηγορία κομίστρου εφόσον υπάρχει[1]. Εν συνεχεία ο εκδότης προχωρά

[1] Ο ΟΑΣΑ αναφέρει ότι, όταν και εφόσον υπάρξει διασύνδεση με το Web Service της ΗΔΙΚΑ, η άντληση δεδομένων πέραν του ΑΜΚΑ, ήτοι όνομα, επώνυμο, μήνας & έτος γέννησης θα γίνεται αυτόματα.

σε επιβεβαίωση της ταυτότητας του επιβάτη (μέσω της αστυνομικής ταυτότητας) ο οποίος και καλείται να εισάγει τον 4-ψήφιο κωδικό ασφαλείας. Για τους αλλοδαπούς, ο εκδότης οφείλει να εισάγει το όνομα, το επώνυμο και τον αριθμό διαβατηρίου στη φόρμα της εφαρμογής του ΤΕΚ και να ζητήσει από τον επιβάτη να εισάγει τον 4-ψήφιο κωδικό ασφαλείας. Τέλος, ο εκδότης προχωρά σε λήψη φωτογραφίας του επιβάτη (μέσω της φωτογραφικής μηχανής που διαθέτει το ΤΕΚ ή μέσω σάρωσης προεκτυπωμένης φωτογραφίας) και έκδοση της προσωποποιημένης κάρτας. Κατά τη διαδικασία έκδοσης της κάρτας το σύστημα παράγει και αποθηκεύει στη βάση δεδομένων το «ψηφιακό αποτύπωμα» (hashed value) που προκύπτει από τον συνδυασμό ΑΜΚΑ (ή αριθμού διαβατηρίου) και 4-ψήφιου κωδικού, καθώς και τον μήνα και έτος γέννησης αλλά και την ειδική κατηγορία του κομίστρου. Ο μήνας και έτος γέννησης αλλά και η ειδική κατηγορία του κομίστρου αποθηκεύονται επίσης στη μνήμη της έξυπνης κάρτας. Το λοιπά στοιχεία (όνομα, επώνυμο και φωτογραφία) εκτυπώνονται στην επιφάνεια της κάρτας και δεν αποθηκεύονται πουθενά ούτε στο ΤΕΚ ούτε και στο κεντρικό σύστημα του ΑΣΣΚ. Σε περίπτωση έκδοσης κάρτας ειδικής κατηγορίας αποθηκεύεται σε ξεχωριστό αρχείο δεδομένων μόνο ο αριθμός ΑΜΚΑ και η ημερομηνία λήξης του δικαιώματος.

Η διαδικασία έκδοσης κάρτας με χρήση της Web εφαρμογής διαφοροποιείται μόνο ως προς τη μέθοδο εισαγωγής των στοιχείων στην εφαρμογή του ΤΕΚ: Συγκεκριμένα, ο επιβάτης εισάγει στο σχετικό ιστότοπο του ΟΑΣΑ (portal) τον ΑΜΚΑ, το όνομα και το επώνυμό του[2]. Εν συνεχεία, η εφαρμογή ζητά από τον επιβάτη να εισάγει τον 4-ψήφιο κωδικό ασφαλείας και παράγει έναν εκτυπώσιμο κωδικό άμεσης απόκρισης (Quick Response QR Code). Ο επιβάτης προσκομίζει το εκτυπωμένο QR Code στο ΤΕΚ προκειμένου να μεταφερθούν τα στοιχεία στην εφαρμογή μέσω σάρωσης. Η διασταύρωση των στοιχείων με χρήση της αστυνομικής ταυτότητας καθώς και η λήψη φωτογραφίας ακολουθούν την ίδια λογική. Αν πρόκειται περί ειδικής κατηγορίας, ο χρήστης προσθέτει αυτό το δεδομένο σε ειδική θέση στην οθόνη του υπολογιστή του ώστε όταν προσέλθει στο ΤΕΚ με τον κωδικό QR και προ της έκδοσης της κάρτας να καταχωριστεί στο ειδικό αρχείο ο ΑΜΚΑ και η λήξη του δικαιώματος. Η μέθοδος αυτή δεν διαφέρει σε τίποτα ως προς τα στοιχεία που αποθηκεύονται ή εκτυπώνονται.

Σε περίπτωση απώλειας προσωποποιημένης έξυπνης κάρτας, ο νόμιμος κάτοχος

[2] Και για αυτήν την περίπτωση γίνεται ειδική μνεία στη δυνατότητα διασύνδεσης με την ΗΔΙΚΑ.

οφείλει να προσκομίσει στο εκδοτήριο ένα επίσημο έγγραφο που να προσδιορίζει τον ΑΜΚΑ του καθώς και την αστυνομική του ταυτότητα (ή αντίστοιχα έγκυρο διαβατήριο για τους αλλοδαπούς). Ο εκδότης εισάγει στην εφαρμογή του ΤΕΚ τον ΑΜΚΑ (ή τον αριθμό διαβατηρίου) και ζητά από τον επιβάτη να εισάγει τον 4ψήφιο κωδικό. Η εφαρμογή συνδυάζει τα δύο αυτά στοιχεία και παράγει ένα ψηφιακό αποτύπωμα (hashed value). Στην περίπτωση ταύτισης με αποθηκευμένο στη βάση δεδομένων ψηφιακό αποτύπωμα που συσχετίζεται με ενεργή έξυπνη κάρτα, ο εκδότης έχει τη δυνατότητα να προχωρήσει σε έκδοση νέας κάρτας με ταυτόχρονη μεταφορά του υπολοίπου και ακύρωση (blacklisting) της παλαιάς. Κανένα επιπλέον στοιχείο του επιβάτη δεν απαιτείται και δεν αποθηκεύεται κατά τη διαδικασία αυτή.

Συγκεντρωτικά, τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας προκειμένου να εκδοθεί η προσωποποιημένη κάρτα απεριορίστων διαδρομών ή/και ειδικών κατηγοριών μειωμένου κομίστρου, με βάση τα όσα αναφέρει ο ΟΑΣΑ στην ως άνω γνωστοποίησή του, περιγράφονται ως εξής:

α) Στην επιφάνεια της κάρτας θα εκτυπώνονται το όνομα, το επώνυμο και η φωτογραφία του κατόχου. Τα στοιχεία αυτά αφορούν μόνο τον φυσικό έλεγχο, δηλαδή τη φυσική ταυτοποίηση κατά τον έλεγχο του επιβάτη, γεγονός ιδιαιτέρως σημαντικό κυρίως στην περίπτωση κατά την οποία η κάρτα είναι εκπτωτική.

β) Στον μικροεπεξεργαστή (chip) της κάρτας θα αποθηκεύεται ο μήνας και το έτος γέννησης του κατόχου της αλλά και η κατηγορία στην οποία αυτός εμπίπτει. Ο μήνας και το έτος γέννησης απαιτούνται ως προσδιοριστικά θεμελίωσης ή μη του δικαιώματος καταβολής μειωμένου κομίστρου βάσει ηλικίας (παιδιά και νέοι κάτω των 18, ενήλικες, ενήλικες άνω των 65). Στο μικροεπεξεργαστή διατηρούνται επίσης οι έξι τελευταίες κινήσεις-συναλλαγές οι οποίες είναι απολύτως απαραίτητες για τη χρέωση της κάρτας. Τις κινήσεις αυτές έχει καταγράψει και το κεντρικό σύστημα βάσης. Από τον μικροεπεξεργαστή της κάρτας διαγράφονται οι κινήσεις μόνο όταν εγγραφούν νέες επί αυτών. Οι τελευταίες έξι κινήσεις δεν μπορούν να διαγραφούν από τον μικροεπεξεργαστή.

γ) Στο κεντρικό σύστημα τηρούνται ο ΑΜΚΑ, ο μήνας και το έτος γέννησης, το «ψηφιακό αποτύπωμα» (hashed value) του ΑΜΚΑ με τον 4-ψήφιο κωδικό όπως περιεγράφηκε ανωτέρω και η κατηγορία του χρήστη. Ήδη προαναφέρθηκε ότι ο ΑΜΚΑ καταχωρίζεται σε εντελώς ανεξάρτητο αρχείο χωρίς καμία περαιτέρω πληροφορία πλην αυτής της λήξεως του δικαιώματος και αφορά μόνο και αδιακρίτως

στις ειδικές κατηγορίες προκειμένου να μην υπάρξει περίπτωση πολλαπλής έκδοσης κάρτας αφού υπάρχει δικαίωμα έκδοσης μίας και μόνο ειδικής κατηγορίας κάρτας και το δικαίωμα αυτό ανήκει σε έναν και μόνο δικαιούχο (π.χ. φοιτητής).

Η αυθεντικοποίηση του υποκειμένου γίνεται με τη χρήση φωτογραφίας και στοιχείων ονόματος και επωνύμου τα οποία αναγράφονται μόνο επί της κάρτας. Η συμπληρωματική επίδειξη ταυτότητας βοηθά στην αυθεντικοποίηση του υποκειμένου ως του νομίμου κατόχου της κάρτας. Ο ελεγκτής κομίστρου μπορεί να ζητήσει περαιτέρω εξακρίβωση στοιχείων ειδικής κατηγορίας, δηλαδή αιτιολόγηση της ένταξης σε ειδικής κατηγορίας μετακίνησης. Οι αντίστοιχοι φορείς προμηθεύουν τους δικαιούχους με σχετικά έγγραφα πιστοποίησης των δικαιωμάτων μετακίνησης (π.χ. κάρτες ανεργίας). Περαιτέρω, στα σημεία επικύρωσης, η αυθεντικοποίηση μέσω έξυπνης κάρτας πραγματοποιείται στις πύλες εισόδου και εξόδου και στα σημεία επικύρωσης των οδικών μέσων.

Επιπροσθέτως, ο ΟΑΣΑ επαναφέρει με την ως άνω νέα γνωστοποίηση το αίτημα που είχε θέσει και στην αρχική του γνωστοποίηση σχετικά με την επαλήθευση και ορθότητα των δεδομένων που χορηγεί ο χρήστης μέσω διαδικτυακής υπηρεσίας (web service) της ΗΔΙΚΑ καθώς είναι απαραίτητη η επαλήθευση αυτών για την αποφυγή λαθών κατά την πληκτρολόγηση και ταυτοποίηση. Η βάση της ΗΔΙΚΑ θεωρείται ακριβής και σε κάθε περίπτωση συσχετίζει τον ΑΜΚΑ με τα απαραίτητα για επεξεργασία προσωπικά δεδομένα του υποκειμένου. Η χρήση της βάσεως της ΗΔΙΚΑ εξυπηρετεί μόνο την επαλήθευση εκείνων των προσωπικών δεδομένων που είναι απαραίτητα για την ταυτοποίηση των χρηστών. Καμία περαιτέρω επεξεργασία των δεδομένων της βάσης δεν γίνεται, η δε πληκτρολόγηση του ΑΜΚΑ στην οθόνη του εκδοτηρίου δεν επιτρέπει στον χειριστή την άντληση δεδομένων εκ της βάσεως. Το σχετικό web service της ΗΔΙΚΑ που μνημονεύει ο ΟΑΣΑ ονομάζεται AMKA2dataLight.

Ο ΟΑΣΑ επίσης στην ως άνω γνωστοποίησή του περιγράφει το πλαίσιο ασφαλείας των πληροφοριών του, αναφέροντας, μεταξύ άλλων, ότι διαθέτει και συνεχώς εξελίσσει πολιτική ασφάλειας πληροφοριών αλλά και σχέδιο ασφάλειας. Επιπροσθέτως περιγράφονται οι διαδικασίες άσκησης των δικαιωμάτων πρόσβασης και αντίρρησης από την πλευρά των υποκειμένων των δεδομένων και αναφέρεται ότι

οποιαδήποτε πληροφορία επί του μικροεπεξεργαστή της κάρτας απεριορίστων διαδρομών διατηρείται ως καθαρό κείμενο διότι η κάρτα είναι εξ ορισμού ασφαλής χώρος φύλαξης/αποθήκευσης δεδομένων.

Ο ΟΑΣΑ, εν κατακλείδι, συμπεραίνει ότι κατοχυρώνει τη δυνατότητα των επιβατών σε πλήρως ανωνυμοποιημένη χρήση των αστικών συγκοινωνιών και σε περίπτωση ειδικών προϊόντων εξασφαλίζει την ανωνυμία του χρήστη μέσω συστήματος αλγορίθμου κατακερματισμού (hashing).

Τέλος, ο ΟΑΣΑ γνωστοποιεί στην Αρχή και τη δημιουργία ενός νέου αρχείου προσωπικών δεδομένων το οποίο ουδεμία σχέση έχει με το μεταφορικό έργο ή με οποιοδήποτε άλλο αρχείο του ΟΑΣΑ και λειτουργεί αυτόνομα. Το αρχείο αυτό έχει ως σκοπό την επικοινωνία του ΟΑΣΑ με όσους επιθυμούν να ενημερώνονται για νέα προϊόντα, προσφορές και ειδικά ή έκτακτα νέα που αφορούν στις αστικές συγκοινωνίες. Στο αρχείο αυτό εγγράφονται ηλεκτρονικά όσοι επιθυμούν να λαμβάνουν ενημέρωση για τις δράσεις και προσφορές του ΟΑΣΑ. Η διαδικασία καταχώρισης των δεδομένων γίνεται βάσει της Οδηγίας 2/2011 της Αρχής. Ο χρήστης στη σχετική ηλεκτρονική σελίδα καταχωρεί το όνομα, το επώνυμο, την ηλεκτρονική ή ταχυδρομική διεύθυνση ή τον αριθμό κινητού τηλεφώνου. Στην ίδια σελίδα μπορεί να ασκεί ψηφιακά το δικαίωμα αντίρρησης και διαγραφής από τη λίστα των πελατών/ενδιαφερομένων. Ο πελάτης μπορεί να είναι χρήστης οποιουδήποτε προϊόντος και οποιασδήποτε κατηγορίας. Το ενδιαφέρον και ο σκοπός του ΟΑΣΑ στην τήρηση αυτού του αρχείου είναι να ωθεί μέσω προσφορών τους χρήστες στη χρήση των μέσων μαζικής μεταφοράς και στην προτίμηση αυτών για ενδεχόμενες δράσεις τους (όπως π.χ. προσφορά ή δωρεάν μετάβαση ή έκπτωση σε όλους τους κατόχους προσωποποιημένων καρτών για συγκεκριμένες εκδηλώσεις, παραστάσεις κ.λπ.). Οι ενημερώσεις αυτές δεν έχουν προσωπικό αλλά μαζικό χαρακτήρα και στη βάση δεδομένων δεν καταχωρούνται συγκεκριμένα χαρακτηριστικά των πελατών.

Κατόπιν της ως άνω νέας γνωστοποίησης, η Αρχή απέστειλε στον ΟΑΣΑ το υπ' αριθμ. πρωτ. ΓΝ/ΕΞ/1570-1/15-06-2017 έγγραφο, με το οποίο ζήτησε την παροχή συμπληρωματικών διευκρινίσεων επί κάποιων ειδικών θεμάτων. Ο ΟΑΣΑ απάντησε με το υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/1894/30-06-2017 έγγραφο. Λόγω της ανάγκης

αποσαφήνισης κάποιων από τα ζητήματα της ως άνω επιστολής, η Αρχή απέστειλε νέα επιστολή με ερωτήματα με το υπ' αριθμ. πρωτ. ΓΝ/ΕΞ/1570-2/3-07-2017 έγγραφο, στο οποίο ο ΟΑΣΑ απάντησε με το υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/2020/10-07-2017 έγγραφο. Από τα έγγραφα αυτά προκύπτουν τα εξής:

α) Ο μήνας και το έτος γέννησης τηρούνται για όλους ανεξαιρέτως τους κατόχους προσωποποιημένων καρτών και αφορούν στη μετάπτωση της κάρτας σε άλλη κατηγορία με βάση την ηλικία (χωρίς αναφορά στην πλήρη ημερομηνία αλλά μόνο στο μήνα και έτος γεννήσεως). Η πληροφορία αυτή είναι απαραίτητη για την εφαρμογή όλων των πολιτικών κομίστρου που συναρτώνται με την ηλικία του επιβάτη (όπως περιγράφονται αναλυτικά στη συνέχεια). Η έναρξη και λήξη του εκπτωτικού δικαιώματος αφορά άτομα που πλησιάζουν για παράδειγμα την ηλικία των 18 ή των 65 ετών. Ο ΟΑΣΑ δεν μπορεί να γνωρίζει για πόσο διάστημα θα διατηρήσει ο χρήστης την κάρτα του, επομένως η αυτόματη μετάπτωση μπορεί να συμβεί σε μικρό ή μεγάλο χρονικό διάστημα. Για τον λόγο αυτό ο ΟΑΣΑ έχει επιλέξει να μην τηρεί την πλήρη ημερομηνία γεννήσεως αλλά μόνο μήνα/έτος ώστε να είναι αδύνατον να ταυτοποιηθεί κάποιος χρήστης από την ημερομηνία γεννήσεως και συγχρόνως να επιτυγχάνεται ο σκοπός της αυτόματης μετάπτωσης στην επόμενη κατηγορία χωρίς απώλεια εσόδων του οργανισμού ή απώλεια δικαιωμάτων των χρηστών. Πέραν της εφαρμογής των υπαρχουσών πολιτικών κομίστρου, το έτος γεννήσεως των επιβατών αποτελεί και ένα από τα στοιχεία που δύνανται να χρησιμοποιηθούν για στατιστική επεξεργασία των δεδομένων μετακίνησης και εξαγωγή συμπερασμάτων για τη χρήση των μέσων από διαφορετικές ηλικιακές ομάδες. Η επεξεργασία αυτή είναι καθαρά στατιστική επί μεγάλου όγκου ανώνυμων δεδομένων και σε καμία περίπτωση δεν προσδιορίζει στοιχεία μετακίνησης μεμονωμένων ατόμων.

Συγκεκριμένα, οι δικαιούχοι μετακίνησης με μειωμένους τύπους κομίστρου λόγω ηλικίας είναι οι εξής: i) άτομα άνω των 65 ετών, ii) νέοι 7 έως 18 ετών, iii) φοιτητές Ανώτατων Εκπαιδευτικών Ιδρυμάτων της αλλοδαπής (μέχρι τα 25 έτη), iv) Μαθητές άνω των 18 ετών, v) Σπουδαστές Δημόσιων Ι.Ε.Κ. (μέχρι τα 22 έτη).

Όπως ήδη έχει αναφερθεί παραπάνω, ο ΑΜΚΑ τηρείται επιπρόσθετα για τους δικαιούχους μη σχετικού με την ηλικία εκπτωτικού δικαιώματος (ανέργους, ΑΜΕΑ, φοιτητές κ.λπ.), σε ανεξάρτητο πίνακα της βάσης δεδομένων μαζί με την ημερομηνία λήξης δικαιώματος για την οποία θα τηρείται μόνο ο μήνας και το έτος. Μεταξύ του πίνακα αυτού και του πίνακα στον οποίο καταχωρίζονται οι κάρτες με τα δεδομένα

που αναφέρονται παραπάνω δεν υπάρχει κανένα κοινό πεδίο (κλειδί) που να επιτρέπει συσχέτιση των στοιχείων.

β) Η πληροφορία της ημερομηνίας λήξης του δικαιώματος βρίσκεται και στον ως άνω ανεξάρτητο πίνακα όπου τηρούνται οι ΑΜΚΑ αλλά και στον πίνακα με τα στοιχεία των καρτών. Όμως αυτή η πληροφορία δεν συνιστά κλειδί συσχέτισης γιατί, όπως εξηγείται στη συνέχεια, η ημερομηνία λήξης του δικαιώματος περιορίζεται μόνο σε μήνα και έτος και είναι ίδια για μεγάλες ομάδες χρηστών. Η πληροφορία της λήξης του δικαιώματος συναρτάται με την ανάγκη γνώσης του ΟΑΣΑ για τη μετάπτωση της ειδικής κατηγορίας κάρτας σε κανονική κατηγορία μετά τη λήξη του δικαιώματος. Ο ΑΜΚΑ διαγράφεται από τον πίνακα μετά τη μετάπτωση σε κανονική κατηγορία.

Ως προς τις ημερομηνίες λήξης του δικαιώματος, ο ΟΑΣΑ αναφέρει ότι τα δικαιώματα μειωμένου κομίστρου προσδιορίζονται κάθε φορά με κοινή υπουργική απόφαση και στη συνέχεια τα δικαιώματα χορηγούνται με συμβάσεις μεταξύ του ΟΑΣΑ και των εκάστοτε δικαιούχων οργανισμών. Οι ημερομηνίες λήξης των δικαιωμάτων είναι συνήθως η 31^{η} Δεκεμβρίου εκάστου έτους ή η ημερομηνία λήξης του χρόνου φοίτησης, θητείας κ.λπ. Πρόκειται δηλαδή για δεδομένα μαζικά και όχι για συγκεκριμένες ημερομηνίες λήξεως που εξατομικεύουν το κάθε υποκείμενο. Επομένως τέτοια δεδομένα όπως π.χ. η λήξη εξαμήνου φοίτησης ή η λήξη της θητείας δεν μπορούν να οδηγήσουν σε ταυτοποίηση επιβάτη διότι είναι, κατά τους ισχυρισμούς του ΟΑΣΑ, ίδια για πολύ μεγάλες ομάδες δικαιούχων. Ο ΟΑΣΑ εξέτασε την περίπτωση να μην τηρεί αναλυτικά την ημερομηνία λήξης δικαιώματος αλλά μόνο τον μήνα και έτος λήξης αυτού και κατέληξε στην αποδοχή της χρήσης μόνο αυτής της πληροφορίας.

γ) Κατά τον έλεγχο της κάρτας από ελεγκτή, τα δεδομένα που είναι αποθηκευμένα στο chip της κάρτας και επί της κάρτας διαβάζονται τοπικά με χρήση της ειδικής συσκευής ελέγχου χωρίς να γίνεται ανταλλαγή στοιχείων με το κεντρικό σύστημα. Στο chip της κάρτας βρίσκεται αποθηκευμένος ο μήνας και το έτος γέννησης και η κατηγορία της κάρτας (πολλαπλών διαδρομών, ΑΜΕΑ, άνεργος, φοιτητής κ.λπ.). Επίσης αποθηκεύονται οι έξι τελευταίες κινήσεις, ο αριθμός της κάρτας καθώς και το υπόλοιπο ποσό στην περίπτωση της ύπαρξης αποθηκευμένης αξίας.

δ) Οι τελευταίες έξι κινήσεις της κάρτας (ώρες επικύρωσης και σταθμοί/στάσεις) καταγράφονται σε όλες τις κάρτες (προσωποποιημένες και μη) όπως και στα πολλαπλά εισιτήρια. Οι ώρες επικύρωσης, οι σταθμοί/στάσεις και ο αριθμός όλων

των καρτών τηρούνται και στη βάση δεδομένων. Σημειώνεται ότι δεν είναι γνωστή η ταυτότητα του επιβάτη παρά μόνο ο αριθμός της κάρτας. Το ακριβές ιστορικό των μετακινήσεων είναι απαραίτητο για τον υπολογισμό του κομίστρου βάσει της επικύρωσης επιβίβασης ή της επικύρωσης αποβίβασης. Παραδείγματος χάριν, το σύστημα χρησιμοποιεί τα προαναφερθέντα δεδομένα για να υπολογίσει εάν η κάρτα κυκλοφορεί εντός του χρονικού ορίου των 90 λεπτών ή εάν τα έχει υπερβεί καθώς και για να υπολογίσει εάν η κάρτα έχει υπερβεί ή όχι το μέγιστο αριθμό μετεπιβιβάσεων εντός του επιτρεπόμενου χρονικού ορίου. Επίσης, το σύστημα εφαρμόζει μέγιστη επιτρεπόμενη ημερήσια χρέωση (fare cap) στα προϊόντα Πολλαπλών Διαδρομών (Count Based Ticket) και Αποθηκευμένης Αξίας. Δηλαδή, εάν εντός μίας ημέρας η αξία του αθροίσματος των κομίστρων φτάσει την καθορισμένη μέγιστη ημερήσια χρέωση, το σύστημα σταματάει πλέον να αφαιρεί διαδρομές/αξία από την κάρτα για την αποφυγή φαινομένων υπερβολικής χρέωσης. Οι προαναφερθείσες λειτουργίες απαιτούν την τήρηση του ιστορικού μετακινήσεων στην κάρτα για την ορθή υλοποίησή τους.

Η τήρηση των δεδομένων κίνησης της κάρτας δεν αφορά σε δεδομένα κίνησης «επιβατών» καθώς τα δεδομένα αυτά έχουν ψευδωνυμοποιηθεί με τη χρήση ανεπίστρεπτου ψηφιακού αποτυπώματος (hashed value). Επομένως, τα δεδομένα κίνησης που τηρούνται δεν αναφέρονται σε υποκείμενα αλλά σε αριθμούς καρτών. Αν υφίσταται υπόλοιπο στην κάρτα τότε το μεταφορικό δικαίωμα παραμένει ενεργό και δεν υπάρχει σε αυτήν την περίπτωση λόγος διαγραφής της κάρτας. Αν το υπόλοιπο της κάρτας είναι μηδενικό, τότε τα δεδομένα κίνησης διατηρούνται για δύο έτη. Περαιτέρω, ο χρήστης είναι πιθανό να ζητήσει ανάλυση του ιστορικού των μετακινήσεών του. Παραδείγματος χάριν, εάν ένας επιβάτης παραπονεθεί για υπερβολική χρέωση κατά την επικύρωση της κάρτας του σε σταθμό ή όχημα, ο έλεγχος του ιστορικού μετακινήσεων είναι αναγκαίος για την επιβεβαίωση ή μη των ισχυρισμών του επιβάτη και εν τέλει την επίλυση του προβλήματος. Εξάλλου ο χρήστης μπορεί να θεωρήσει ότι δικαιούται να αμφισβητήσει το τυχόν μηδενικό υπόλοιπο της κάρτας του ή οποιαδήποτε χρέωση έγινε εντός της τελευταίας πενταετίας (οπότε παραγράφεται και το δικαίωμα εξ αδικοπραξίας).

Προκειμένου να μην διατηρούνται στο αρχείο του ΟΑΣΑ εκατομμύρια κινήσεις καρτών, ο ΟΑΣΑ διαγράφει τα δεδομένα κινήσεων προ της παρόδου της πενταετίας, δηλαδή με το τέλος της διετίας αχρησίας της κάρτας μηδενικού υπολοίπου. Η διετία θεωρείται εύλογος χρόνος διατήρησης ιστορικού κινήσεων της κάρτας και για

στατιστικούς σκοπούς. Ο ΟΑΣΑ αναλαμβάνει την υποχρέωση, αν τυχόν εμφανισθούν αμφισβητήσεις κινήσεων που υπερβαίνουν τη διετία, να τις χειριστεί κατά περίπτωση. Σε κάθε περίπτωση, τα δεδομένα κινήσεων που τηρούνται αφορούν σε κινήσεις καρτών, όχι υποκειμένων, οι οποίες συνδυάζονται με μη αντιστρεφόμενες τιμές συνάρτησης κατακερματισμού («ψηφιακά αποτυπώματα»).

ε) Τα δεδομένα που θα λαμβάνονται από την υπηρεσία της ΗΔΙΚΑ θα χρησιμοποιούνται μόνο για αυτόματη επαλήθευση των χορηγούμενων από το υποκείμενο δεδομένων. Τα δεδομένα δεν καταχωρίζονται σε αρχείο του ΟΑΣΑ. Στο αρχείο του ΟΑΣΑ καταχωρίζεται μόνο η τιμή της συνάρτησης κατακερματισμού (hash code), ο αριθμός της κάρτας και ο μήνας και το έτος γέννησης. Το όνομα και το επώνυμο του επιβάτη χρησιμοποιούνται μόνο για την εκτύπωση της κάρτας και δεν καταχωρίζονται.

στ) Η χρήση 4ψήφιου κωδικού ασφαλείας υιοθετήθηκε, έναντι της δυνατότητας χρήσης οποιουδήποτε αλφαριθμητικού ανεξαρτήτου μήκους εν είδει συνθηματικού, αφενός μεν διότι είναι κάτι στο οποίο το κοινό είναι εξοικειωμένο (pin πιστωτικών/χρεωστικών καρτών, κωδικός sim κινητών τηλεφώνων) αφετέρου δε διότι δύναται να εισαχθεί από τον επιβάτη με χρήση ασύρματου numpad κατά τη διαδικασία έκδοσης της κάρτας στο ΤΕΚ. Ο τελευταίος περιορισμός δεν υφίσταται φυσικά κατά τη διαδικασία καταχώρισης των στοιχείων μέσω του portal και δημιουργίας του QR code. Η χρήση όμως αλφαριθμητικών κωδικών θα αύξανε τη πιθανότητα απώλειάς τους με αρνητικές συνέπειες στη διαδικασία αντικατάστασης καρτών με μεταφορά υπολοίπου.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου, αφού άκουσε τους εισηγητές και τις διευκρινίσεις των βοηθών εισηγητών οι οποίοι στην συνέχεια αποχώρησαν, κατόπιν διεξοδικής συζήτησης, εκδίδει την ακόλουθη

Γ Ν Ω Μ Ο Δ Ο Τ Η Σ Η

1. Η Αρχή είναι αρμόδια σύμφωνα με το άρθρο 19 παρ. 1 στοιχ. θ΄ του ν. 2472/1997 να *«γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα»*. Η γνωμοδοτική αρμοδιότητα της Αρχής δεν περιορίζεται μόνο στους τομείς που ρυθμίζονται από την Οδηγία 95/46/ΕΚ

αλλά καταλαμβάνει όλα τα θέματα που αφορούν στην επεξεργασία και προστασία των προσωπικών δεδομένων.

2. Ήδη με την υπ' αριθμ. 1/2017 Γνωμοδότηση η Αρχή έθεσε το σύνολο των προϋποθέσεων που πρέπει να πληρούνται ώστε η επεξεργασία προσωπικών δεδομένων στο πλαίσιο ενός ηλεκτρονικού συστήματος για τις μετακινήσεις που γίνονται με μέσα μαζικής μεταφοράς να είναι σύμφωνη με τις επιταγές του σχετικού νομικού πλαισίου και να μη θίγει τα θεμελιώδη δικαιώματα και ελευθερίες των ατόμων. Όπως επεσήμανε, μεταξύ άλλων, η Αρχή στην ως άνω Γνωμοδότηση, οι σκοποί που δήλωσε ο ΟΑΣΑ για την εν λόγω επεξεργασία είναι καθορισμένοι, σαφείς, θεμιτοί και νόμιμοι ενώ η επίτευξή τους χωρίς τη χρήση ηλεκτρονικού εισιτηρίου είναι εξαιρετικά δυσχερής με την υπάρχουσα έγχαρτη μορφή των εισιτηρίων για τα μέσα μαζικής μεταφοράς που τελούν υπό την εποπτεία του ΟΑΣΑ (βλ. Γνωμοδότηση 1/2017, Σκέψη 6). Ωστόσο, όπως επίσης αναφέρεται στην ως άνω Γνωμοδότηση, για την επίτευξη των σκοπών αυτών η εν λόγω επεξεργασία προσωπικών δεδομένων είναι εμφανώς διαφορετικής «έντασης» (τήρηση ηλεκτρονικής βάσης δεδομένων, χρήση microchip ανέπαφης *contactless* τεχνολογίας, τήρηση μεγάλου εύρους προσωπικών δεδομένων κτλ.) σε σχέση με την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί μέχρι τώρα ο ΟΑΣΑ στο πλαίσιο της παροχής των υπηρεσιών του στο επιβατικό κοινό. Επιπλέον, η αιτούμενη επεξεργασία θα είναι υποχρεωτική και θα αφορά μεγάλο πλήθος υποκειμένων των δεδομένων, οπότε και καθίσταται αναγκαίο, κατά τον σχεδιασμό του ηλεκτρονικού συστήματος, να διασφαλίζεται ότι πληρούνται οι αναγκαίες προϋποθέσεις για την αντιμετώπιση των κινδύνων ως προς την προστασία των προσωπικών δεδομένων («προστασία των δεδομένων ήδη από τον σχεδιασμό», βλ. Γνωμοδότηση 1/2017, Σκέψη 7).

Περαιτέρω, η Αρχή ρητώς επεσήμανε ότι ο κύριος κίνδυνος που ελλοχεύει, ως προς την προστασία των προσωπικών δεδομένων, στο πλαίσιο ενός συστήματος προσωποποιημένων ηλεκτρονικών εισιτηρίων, συνίσταται στο ότι η χρήση ενός τέτοιου συστήματος μπορεί να συνεπάγεται τη συλλογή δεδομένων σχετικά με τις διαδρομές που πραγματοποιεί ο εκάστοτε επιβάτης με αποτέλεσμα να θίγεται υπέρμετρα η ελευθερία κίνησης ή κυκλοφορίας της οποίας αναπόσπαστο μέρος αποτελεί το δικαίωμα της ανώνυμης μετακίνησης (βλ. Γνωμοδότηση 1/2017, Σκέψη 8). Ο κίνδυνος αυτός ήταν υπαρκτός με βάση την αρχική μορφή του συστήματος που περιέγραφε ο ΟΑΣΑ στην αρχική του γνωστοποίηση. Συναφώς, ο υπεύθυνος

επεξεργασίας ούτε τεκμηρίωσε την αναγκαιότητα της επεξεργασίας του συνόλου των προσωπικών δεδομένων τα οποία θα υφίσταντο επεξεργασία σύμφωνα με το αρχικό σύστημα ούτε κατέδειξε ότι εξέτασε εναλλακτικές τεχνικές λύσεις που αφενός μεν θα επετύγχαναν εξίσου τους επιδιωκόμενους σκοπούς αφετέρου δε θα εξασφάλιζαν την προστασία της ιδιωτικότητας των χρηστών (βλ. Γνωμοδότηση 1/2017, Σκέψη 9).

3. Η υπό εξέταση νέα γνωστοποίηση, όπως περιγράφεται στο ιστορικό της παρούσας, έχει εναρμονιστεί σε ικανοποιητικό βαθμό με τις προϋποθέσεις που έθεσε η Αρχή στη Γνωμοδότηση 1/2017. Συγκεκριμένα, όπως συνάγεται από το ιστορικό της παρούσας, ο υπεύθυνος επεξεργασίας έχει περιορίσει το σύνολο των προσωπικών δεδομένων που συλλέγει και επεξεργάζεται εν όψει των επιδιωκόμενων σκοπών ενώ έχει επίσης προβεί σε νέα συνολική σχεδίαση του συστήματος. Προκύπτει επίσης ότι για το σύστημα ΗΛΕΚΤΡΟΝΙΚΟ ΕΙΣΙΤΗΡΙΟ τέθηκε πλέον ως σχεδιαστικός στόχος η αντιμετώπιση των κινδύνων για την προστασία των προσωπικών δεδομένων που περιέγραψε η Αρχή στη Γνωμοδότηση 1/2017. Σε συμμόρφωση με την προαναφερόμενη Γνωμοδότηση, η νέα γνωστοποίηση, μεταξύ άλλων, προβλέπει τη δημιουργία ψηφιακού αποτυπώματος με την εισαγωγή κωδικού που θα γνωρίζει μόνο ο χρήστης. Η νέα γνωστοποίηση εξάλλου περιέχει όλες τις πληροφορίες που προσδιορίζονται στο άρ. 6 του ν. 2472/1997.

4. Επιπροσθέτως, η Αρχή κρίνει ότι η αξιοποίηση της διαδικτυακής υπηρεσίας της ΗΔΙΚΑ για τον σκοπό της ακρίβειας των προσωπικών δεδομένων (όνομα, επώνυμο, μήνας και έτος γέννησης), όπως περιγράφεται από τον ΟΑΣΑ στη νέα γνωστοποίησή του, δεν προσκρούει στις θεμελιώδεις αρχές της προστασίας προσωπικών δεδομένων αφού μια τέτοια επεξεργασία γίνεται για σαφή, θεμιτό και νόμιμο σκοπό και δεν έχει ως αποτέλεσμα τη συλλογή, από πλευράς ΟΑΣΑ, περισσότερων προσωπικών δεδομένων από όσα απαιτούνται για την επίτευξη των επιδιωκόμενων σκοπών του – δεδομένου άλλωστε ότι ο ΟΑΣΑ θα συλλέγει τα ίδια ακριβώς δεδομένα ακόμα και χωρίς την αξιοποίηση της διαδικτυακής υπηρεσίας της ΗΔΙΚΑ. Αυτονόητο είναι ότι η εν λόγω διαδικτυακή υπηρεσία δεν θα πρέπει να παρέχει καμία άλλη πληροφορία προς τον ΟΑΣΑ, πέραν των όσων ρητώς προσδιορίζονται ανωτέρω, καθώς επίσης και ότι ο ΟΑΣΑ οφείλει ως υπεύθυνος επεξεργασίας να λαμβάνει πάντα τα πλέον ενδεδειγμένα μέτρα για την ασφάλεια της επεξεργασίας στο πλαίσιο της εν λόγω διαδικτυακής υπηρεσίας.

5. Περαιτέρω, η Αρχή κρίνει ότι, ιδίως ως προς τον κίνδυνο της συστημικής αντιστοίχισης του αριθμού της κάρτας με τον κάτοχό της, η οποία τελικά θα

ισοδυναμούσε με γνώση του ιστορικού όλων των μετακινήσεων για συγκεκριμένο επιβάτη –κάτι που αντίκειται στις προϋποθέσεις που έθεσε η Αρχή στη Γνωμοδότηση 1/2017– ο υπεύθυνος επεξεργασίας θα πρέπει να εξετάσει προσεγγίσεις προς βελτίωση του συστήματος. Τούτο διότι με το περιγραφόμενο σύστημα ο κίνδυνος αυτός περιορίζεται μεν σημαντικά αλλά φαίνεται ότι δεν εξαλείφεται πλήρως ιδίως λόγω της τήρησης, για συγκεκριμένους έστω χρήστες, του ΑΜΚΑ. Σημειώνεται ότι η Αρχή στη Γνωμοδότηση 1/2017 είχε ρητώς επισημάνει ότι ο υπεύθυνος επεξεργασίας θα πρέπει να διασφαλίσει ότι από το σύνολο της τηρούμενης πληροφορίας, ακόμα και αν αυτή είναι διαμοιρασμένη σε ανεξάρτητα υποσυστήματα, δεν θα πρέπει να είναι εφικτή η εξαγωγή πλήρους πληροφόρησης για τις ακριβείς διαδρομές που πραγματοποιεί ο κάθε επιβάτης έτσι ώστε να διασφαλίζεται το δικαίωμα της ανώνυμης μετακίνησης (βλ. Σκέψη 9 αυτής). Εντούτοις το νέο σύστημα παρέχει αυτήν την, έστω και απομακρυσμένη πρακτικά, δυνατότητα επειδή, όπως περιγράφεται αναλυτικά στη συνέχεια, δεν αποκλείει τη διασύνδεση πληροφοριών που τηρούνται μεν σε ανεξάρτητους πίνακες της βάσης δεδομένων, ωστόσο μέσω της κατάλληλης μεταξύ τους διασύνδεσης μπορεί να δημιουργήσουν προφίλ μετακινήσεων συγκεκριμένου επιβάτη/συγκεκριμένων επιβατών:

i) Για δοθέν ΑΜΚΑ που εμφανίζεται στον ανεξάρτητο πίνακα, καταγραφή του μήνα και έτους λήξης δικαιώματος της αντίστοιχης κάρτας.

ii) Αναζήτηση της ανωτέρω τιμής «μήνας/έτος λήξης δικαιώματος» στον κεντρικό πίνακα της βάσης. Όπως αναφέρει ο ΟΑΣΑ, πολλοί χρήστες –άρα, πολλές καταχωρίσεις στον κεντρικό αυτό πίνακα– θα έχουν κοινή τιμή σε αυτό το πεδίο (π.χ. θα είναι για πολλούς η 31η Δεκεμβρίου του τρέχοντος κάθε φορά έτους) και, ως εκ τούτου, η αναζήτηση αυτή θα έχει ως αποτέλεσμα πολλές –και όχι αποκλειστικά μία– καταχωρίσεις (δηλαδή πολλούς διαφορετικούς χρήστες, ένας μόνο εκ των οποίων θα αντιστοιχεί στον δοθέντα ΑΜΚΑ).

iii) Λαμβάνοντας υπόψη ότι ο ΑΜΚΑ περιέχει τον μήνα και το έτος γέννησης, από το σύνολο των πολλών αυτών χρηστών μπορούν να εξαιρεθούν εκείνοι για τους οποίους ο μήνας και το έτος γέννησης –που τηρούνται στον κεντρικό πίνακα– δεν αντιστοιχεί στην αρχική τιμή του ΑΜΚΑ που επελέγη.

Η ανωτέρω περιγραφείσα διαδικασία καταδεικνύει ότι δεν μπορεί να αποκλειστεί το ενδεχόμενο, για κάποιες έστω τιμές του ΑΜΚΑ, να προσδιοριστεί μονοσήμαντα το ποια είναι η κάρτα που αντιστοιχεί σε κάθε έναν από τους χρήστες με τις εν λόγω τιμές του ΑΜΚΑ – δηλαδή τελικά να αναγνωριστούν οι κάτοχοι συγκεκριμένων καρτών.

Ως εκ τούτου, για την αντιμετώπιση και του ανωτέρω κινδύνου, ο υπεύθυνος επεξεργασίας θα πρέπει να εξετάσει την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία ώστε να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. Ενδεικτικά, θα μπορούσε να εξεταστεί να μην τηρείται ο ΑΜΚΑ σε αυτούσια μορφή αλλά αντ' αυτού να τηρείται ένα μη αναστρέψιμο ψηφιακό αποτύπωμα (hashed value) του ΑΜΚΑ[3].

Συναφώς με τον ανωτέρω κίνδυνο, ο υπεύθυνος επεξεργασίας θα πρέπει να επιτρέπει στους χρήστες, για τον υπολογισμό του «ψηφιακού αποτυπώματος» που περιγράφεται στο ιστορικό της παρούσας, να επιλέγουν οποιοδήποτε συνθηματικό επιθυμούν και όχι να περιορίζονται σε τετραψήφιο κωδικό. Και τούτο διότι ο τετραψήφιος κωδικός συνεπάγεται ότι για κάθε ΑΜΚΑ, μόνο 10.000 πιθανές τιμές ψηφιακού αποτυπώματος[4] μπορούν να προκύψουν – αριθμός τέτοιος που τελικά επιτρέπει υπολογιστικά τον έλεγχο για το εάν μία δοθείσα τιμή του ΑΜΚΑ αντιστοιχεί σε κάποια από τις κάρτες που τηρούνται στον κεντρικό πίνακα της βάσης.

6. Η Αρχή στη Γνωμοδότηση 1/2017 (βλ. Σκέψη 11 αυτής) επεσήμανε ότι, λαμβάνοντας υπόψη τα χαρακτηριστικά της επεξεργασίας, σκόπιμο είναι ο ΟΑΣΑ, ως υπεύθυνος επεξεργασίας, να προβεί στην εκπόνηση μελέτης εκτίμησης επιπτώσεων στην προστασία προσωπικών δεδομένων, προκειμένου να καταδειχτούν και να αντιμετωπιστούν όλα τα ζητήματα που εγείρονται ως προς την προστασία των δεδομένων, καθώς επίσης και να ληφθούν τα απαραίτητα μέτρα. Δεδομένου ότι δεν υποβλήθηκε στην Αρχή μια τέτοια μελέτη εκτίμησης επιπτώσεων, η Αρχή επαναφέρει την ανάγκη εκπόνησης μιας τέτοιας μελέτης η οποία θα πρέπει να περιέχει τουλάχιστον[5]: α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους

[3] Π.χ. μια κατακερματισμένη τιμή της τριπλέτας «ΑΜΚΑ-Επώνυμο-Όνομα» τα οποία παρέχονται από τη διαδικτυακή υπηρεσία της ΗΔΙΚΑ.

[4] Όσο είναι και το σύνολο όλων των διαφορετικών τετραψήφιων κωδικών.

[5] Υπό το πρίσμα των όσων αναφέρονται και στο άρθρο 35 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.

επιδιωκόμενους σκοπούς, γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας (όπως ανωνυμοποίηση ή/και ψευδωνυμοποίηση), ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα.

7. Τέλος, ως προς το νέο (σε σχέση με την παλαιότερη γνωστοποίηση) αρχείο που γνωστοποίησε ο ΟΑΣΑ για τους σκοπούς της ενημέρωσης –όσων επιθυμούν– για τις προσφορές του Οργανισμού κ.λπ., κρίνεται ότι αυτό δεν προσκρούει στις διατάξεις του ν. 2472/1997. Αυτονόητο είναι ότι, και για αυτό το αρχείο, θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα ασφάλειας σύμφωνα με το άρ. 10 ν. 2472/1997.

8. Λαμβάνοντας υπόψη όλα τα ανωτέρω, η Αρχή γνωμοδοτεί θετικά για το νέο σύστημα αναφορικά με την περιγραφόμενη επεξεργασία προσωπικών δεδομένων συμπεριλαμβανομένης της κατάλληλης αξιοποίησης της διαδικτυακής υπηρεσίας της ΗΔΙΚΑ όπως αναφέρεται στη Σκέψη 4 της παρούσας. Ωστόσο, ο υπεύθυνος επεξεργασίας θα πρέπει αμελλητί να προβεί σε κατάλληλες τροποποιήσεις του συστήματος, σύμφωνα με τα όσα διαλαμβάνονται στη Σκέψη 5 της παρούσας. Περαιτέρω, η αποτελεσματικότητα των σχετικών τροποποιήσεων θα πρέπει να τεκμαίρεται από μελέτη εκτίμησης επιπτώσεων στην προστασία προσωπικών δεδομένων την οποία ο υπεύθυνος επεξεργασίας οφείλει να εκπονήσει σύμφωνα με τα όσα διαλαμβάνονται στη Σκέψη 6 της παρούσας. Η μελέτη αυτή θα πρέπει να αποτυπώνεται σε εγκεκριμένο από τη διοίκηση του ΟΑΣΑ έγγραφο και να είναι διαθέσιμη έως τις 25 Μαΐου 2018.

Ο Πρόεδρος **Η Γραμματέας**

Κωνσταντίνος Μενουδάκος **Γεωργία Παλαιολόγου**