ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Αθήνα, 25-09-2023
Αριθ. Πρωτ.: 2398

ΑΠΟΦΑΣΗ 30/2023

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε συνεδρίαση την 13-06-2023 σε συνέχεια των από 15/2/2022 και 12/4/2022 συνεδριάσεων, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Πρόεδρος της Αρχής, Κωνσταντίνος Μενουδάκος, τα τακτικά μέλη Κωνσταντίνος Λαμπρινουδάκης, ως εισηγητής, Χρήστος Καλλονιάτης, Αικατερίνη Ηλιάδου, καθώς και τα αναπληρωματικά μέλη Χρήστος Παπαθεοδώρου, Νικόλας Λίβος και Μαρία Ψάλλα, σε αντικατάσταση των τακτικών μελών Σπύρου Βλαχόπουλου, Χαράλαμπου Ανθόπουλου και Γρηγόριου Τσόλια, οι οποίοι, αν και κλήθηκαν νομίμως εγγράφως, δεν παρέστησαν λόγω κωλύματος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν, με εντολή του Προέδρου, οι ελεγκτές Φωτεινή Καρβέλα, Κωνσταντίνος Λιμνιώτης και Λεωνίδας Ρούσσος, ειδικοί επιστήμονες, ως βοηθοί εισηγητή και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Τμήματος Διοικητικών Υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Η Αρχή πραγματοποίησε στις 18/11/2019 έκτακτο επιτόπιο έλεγχο στον Οργανισμό Αστικών Συγκοινωνιών Αθηνών (ΟΑΣΑ) Α.Ε. (εφεξής «υπεύθυνος επεξεργασίας» ή ΟΑΣΑ) αναφορικά με την προστασία των προσωπικών δεδομένων που υφίστανται επεξεργασία στο πλαίσιο του Αυτόματου Συστήματος Συλλογής Κομίστρου (εφεξής ΑΣΣΚ), σύστημα το οποίο αναφέρεται και με τον όρο «ηλεκτρονικό εισιτήριο», υπό το πρίσμα των όσων η Αρχή είχε προδιαγράψει με την υπ’ αριθμ. 4/2017 Γνωμοδότησή της. Ειδικότερα, η Αρχή, με τη Γνωμοδότηση 4/2017, είχε εκφράσει γνώμη επί της επεξεργασίας την οποία θα

πραγματοποιούσε ο ΟΑΣΑ στο πλαίσιο του επικείμενου τότε συστήματος ηλεκτρονικού εισιτηρίου. Ήδη με την προηγούμενη υπ' αριθμ. 1/2017 Γνωμοδότηση η Αρχή είχε θέσει 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 (στα οποία δεδομένα συμπεριλαμβάνονται και δεδομένα ειδικών κατηγοριών, όπως αυτά που σχετίζονται με μετακινήσεις ΑΜΕΑ), να είναι σύμφωνη με τις επιταγές του σχετικού νομικού πλαισίου και να μη θίγει τα θεμελιώδη δικαιώματα και ελευθερίες των ατόμων. Η Αρχή, με τη νεότερη Γνωμοδότηση 4/2017, έκρινε ότι η νέα μορφή της εν λόγω επεξεργασίας, όπως την περιέγραφε ο ΟΑΣΑ, έχει εναρμονιστεί σε ικανοποιητικό βαθμό με τις προϋποθέσεις που είχε θέσει η Αρχή στη Γνωμοδότηση 1/2017. Ωστόσο, η Αρχή με τη Γνωμοδότηση 4/2017 έκρινε ότι ο ΟΑΣΑ, ως υπεύθυνος επεξεργασίας, θα πρέπει να προβεί σε κάποιες τροποποιήσεις, η αποτελεσματικότητα των οποίων πρέπει να τεκμαίρεται από μελέτη εκτίμησης αντικτύπου στην προστασία προσωπικών δεδομένων (εφεξής, ΕΑΠΔ) την οποία ο υπεύθυνος επεξεργασίας οφείλει να εκπονήσει και η οποία θα πρέπει να αποτυπώνεται σε εγκεκριμένο από τη διοίκηση του ΟΑΣΑ έγγραφο και να είναι διαθέσιμη έως τις 25 Μαΐου 2018 – ημερομηνία στην οποία θα ετίθετο σε εφαρμογή ο Γενικός Κανονισμός Προστασίας Δεδομένων (εφεξής, ΓΚΠΔ).

Ο ως άνω έλεγχος έγινε, με προηγούμενη ενημέρωση του υπευθύνου επεξεργασίας, στις εγκαταστάσεις του στη διεύθυνση Μετσόβου 115 στην Αθήνα, μετά από την υπ' αρ. πρωτ. Γ/ΕΞ/7873/14-11-2019 εντολή του Προέδρου της Αρχής. Ο έλεγχος προγραμματίστηκε προκειμένου να διαπιστωθεί η συμμόρφωση του υπευθύνου επεξεργασίας με τις απαιτήσεις που περιγράφηκαν στις ως άνω Γνωμοδοτήσεις της Αρχής, υπό το φως και του Γενικού Κανονισμού Προστασίας Δεδομένων αλλά και υπό το πρίσμα των εξής πρόσθετων στοιχείων τα οποία ήγειραν κατ' αρχάς ερωτήματα ως προς το αν διασφαλίζεται η ανωνυμία των μετακινήσεων (ζήτημα το οποίο έχει τεθεί στις ως άνω αναφερόμενες Γνωμοδοτήσεις της Αρχής):

i) Σχετικά δημοσιεύματα, κατά την περίοδο του ελέγχου, ανέφεραν ότι «έχουν καταγραφεί περιπτώσεις πολιτών που δηλώνουν άνεργοι και οι οποίοι καθημερινά πραγματοποιούν το ίδιο δρομολόγιο, και τις ίδιες ακριβώς ώρες, με τα μέσα μεταφοράς»[1].

[1] Βλ., ενδεικτικά, https://www.iefimerida.gr/ellada/xekina-safari-gia-anergoys-maimoy-se-sygkoinonies (ημερομηνία τελευταίας πρόσβασης: 16/6/2023)

ii) Δεν ήταν σαφής ο τρόπος με τον οποίο γίνεται από τον ΟΑΣΑ ο έλεγχος, κατά τη διαδικασία ανανέωσης ενός προσωποποιημένου ηλεκτρονικού εισιτηρίου ειδικής κατηγορίας από τον κάτοχό του μέσω ενός τερματικού, ως προς το αν ο κάτοχος του εισιτηρίου εξακολουθεί να υπάγεται στη συγκεκριμένη ειδική κατηγορία (δεδομένου ότι ο ΟΑΣΑ δεν τηρεί στοιχεία ονοματεπωνύμων, ούτε τηρεί αντιστοίχιση του αριθμού του ηλεκτρονικού εισιτηρίου με τον ΑΜΚΑ του κατόχου του).

Στο πλαίσιο του ελέγχου ζητήθηκε επίσης η ΕΑΠΔ στην οποία αναφέρεται η ανωτέρω Γνωμοδότηση 4/2017 της Αρχής. Περαιτέρω, η ομάδα ελέγχου ζήτησε πληροφορίες επί της επεξεργασίας μέσω του ΑΣΣΚ, ενώ επίσης ζήτησε και ένα σύνολο εγγράφων ως πειστήρια, τα οποία ο υπεύθυνος επεξεργασίας υπέβαλε ακολούθως στην Αρχή. Δεδομένου ότι η εκπόνηση της ΕΑΠΔ δεν είχε ολοκληρωθεί κατά τη στιγμή του επιτόπιου ελέγχου, ο υπεύθυνος επεξεργασίας ενημέρωσε ότι αυτή θα αποσταλεί στην Αρχή με την ολοκλήρωσή της. Η ΕΑΠΔ υποβλήθηκε μετέπειτα με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/9092/30-12-2019 έγγραφο, ενώ λίγες ημέρες νωρίτερα ο υπεύθυνος επεξεργασίας υπέβαλε στην Αρχή και άλλα συμπληρωματικά έγγραφα, σε συνέχεια των όσων είχε ζητήσει η ομάδα ελέγχου.

Ακολούθως, η ομάδα ελέγχου συνέταξε τα Πρακτικά του ελέγχου (εφεξής Πρακτικά), στα οποία καταγράφονται οι απαντήσεις/διευκρινίσεις του ελεγχόμενου φορέα, καθώς και επιτόπιες παρατηρήσεις της ομάδας ελέγχου. Τα Πρακτικά απεστάλησαν στον υπεύθυνο επεξεργασίας με μήνυμα ηλεκτρονικού ταχυδρομείου[2] την 01-06-2020 για υποβολή σχολίων ή/και παρατηρήσεων. Ο υπεύθυνος απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4340/23-06-2020 έγγραφο, με το οποίο παρείχε και συμπληρωματικά αρχεία. Ακολούθως, τα εν λόγω Πρακτικά οριστικοποιήθηκαν με το υπ' αριθμ. πρωτ. Γ/ΕΞ/7971/19-11-2020 έγγραφο. Στα Πρακτικά υπάρχει και αναλυτική περιγραφή του συνόλου των πειστηρίων που υποβλήθηκαν.

Εν συνεχεία, η ομάδα ελέγχου μελέτησε τα Πρακτικά σε συνδυασμό με τα πειστήρια που συλλέχθηκαν και υπέβαλε στην Αρχή το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/8221/30-11-2020 πόρισμα του ελέγχου. Το Πόρισμα συνοδεύεται από παράρτημα με τα πρακτικά του ελέγχου, το οποίο παράρτημα αποτελεί αναπόσπαστο μέρος του Πορίσματος.

Τα βασικά ευρήματα του ελέγχου, όπως αναλύονται στο πόρισμα, είναι τα εξής:

Εύρημα 1 - Μη έγκαιρη εκπόνηση ΕΑΠΔ: Η εκτίμηση αντικτύπου ως προς την προστασία

[2] Το σχετικό επισυναπτόμενο αρχείο εστάλη κρυπτογραφημένο, για την αποκρυπτογράφηση του οποίου διαβιβάστηκε το κλειδί αποκρυπτογράφησης στον ελεγχόμενο φορέα μέσω τηλεφωνικής επικοινωνίας.

προσωπικών δεδομένων δεν ήταν διαθέσιμη κατά τη στιγμή του ελέγχου, αλλά υποβλήθηκε τελικά στην Αρχή μετέπειτα, όπως προαναφέρθηκε, στις 30-12-2019.

Εύρημα 2 - Μη εμπεριστατωμένο περιεχόμενο εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων: Όπως αναλύεται στο πόρισμα του ελέγχου, η ΕΑΠΔ, η οποία υποβλήθηκε μετά τον έλεγχο, παρουσιάζει ασάφειες σε πολλά σημεία, δεν εξετάζει όλους τους κινδύνους ως προς την προστασία των προσωπικών δεδομένων, ενώ και οι κίνδυνοι που εξετάζονται, δεν φαίνεται ότι αποτιμώνται με τον δέοντα τρόπο. Επίσης, διαπιστώθηκε αναντιστοιχία μεταξύ της εκτίμησης αντικτύπου και του τεθέντος υπόψη της Αρχής αρχείου δραστηριοτήτων ως προς τις νομικές βάσεις της επεξεργασίας για τους διάφορους σκοπούς, η οποία δεν τεκμηριώνεται.

Εύρημα 3 - Χρόνος τήρησης των δεδομένων: Ο χρόνος τήρησης των δεδομένων στο πλαίσιο του ΑΣΣΚ δεν είχε καθοριστεί κατά τη στιγμή του ελέγχου. Μετά τον έλεγχο, επελέγη ως χρόνος τήρησης τα 20 έτη, για όλους ανεξαιρέτως τους σκοπούς του συστήματος, χωρίς διάκριση και χωρίς σχετική τεκμηρίωση.

Εύρημα 4 - Αρχείο δραστηριοτήτων επεξεργασίας: Οι σκοποί της εν λόγω επεξεργασίας δεν περιγράφονται στο αρχείο δραστηριοτήτων τόσο αναλυτικά όσο ο υπεύθυνος επεξεργασίας τους είχε περιγράψει αρχικώς στην Αρχή και όπως αυτοί περιγράφονται στις Γνωμοδοτήσεις 1/2017 και 4/2017 της Αρχής. Επίσης, δεν υπάρχει αντιστοιχία μεταξύ των σκοπών που περιγράφονται στο αρχείο δραστηριοτήτων και στη σχετική ενημέρωση η οποία παρεχόταν στα υποκείμενα των δεδομένων κατά την περίοδο εκείνη μέσω του διαδικτυακού τόπου του ΟΑΣΑ.

Στη συνέχεια, η Αρχή κάλεσε σε ακρόαση τον ΟΑΣΑ σε συνεδρίαση, μέσω τηλεδιάσκεψης, της Ολομέλειας της 10-12-2020 (βλ. κλήση με αριθ. πρωτ. Γ/ΕΞ/8295/2-12-2020) η οποία ωστόσο αναβλήθηκε. Με νεότερη κλήση (βλ. κλήση με αριθ. πρωτ. Γ/ΕΞΕ/279/04-02-2022) ο ΟΑΣΑ κλήθηκε σε συνεδρίαση της Ολομέλειας της Αρχής, μέσω τηλεδιάσκεψης, της 15-02-2022. Στη συνεδρίαση της 15-2-2022 παρέστησαν οι Α, Υπεύθυνος Προστασίας Δεδομένων του ΟΑΣΑ, Β, εκπρόσωπος για το ΑΣΣΚ, Γ, Σύμβουλος του ΟΑΣΑ σε θέματα προσωπικών δεδομένων, Δ, Σύμβουλος του ΟΑΣΑ σε θέματα προσωπικών δεδομένων, Αθανάσιος Μητρούσης, δικηγόρος του ΟΑΣΑ, και Ε, Υπεύθυνος Προστασίας Δεδομένων της αναδόχου εταιρείας HST. Μετά τη συνεδρίαση, ο ΟΑΣΑ έλαβε προθεσμία για υποβολή υπομνήματος, για την οποία ζήτησε μετέπειτα, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/3925/10-03-2022 αίτημά του, ολιγοήμερη παράταση, λόγω του ότι ειδικά για τη

λειτουργία του ΑΣΣΚ, ο ΟΑΣΑ απευθύνθηκε στην ανάδοχο του έργου Εταιρεία «HELLAS SMARTICKET Α.Ε.», η οποία ανέλαβε να εκπονήσει τεχνική έκθεση επί τη βάσει των παρατηρήσεων της Αρχής που διατυπώθηκαν κατά την ως άνω συνεδρίαση, δεν κατέστη όμως δυνατόν να ολοκληρωθεί έγκαιρα η σχετική έκθεση. Ακολούθως, ο ΟΑΣΑ υπέβαλε, εντός της νέας προθεσμίας που ετέθη, το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/4920/22-03-2022 υπόμνημα, όπως συμπληρώθηκε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/5320/28-03-2022 έγγραφο, το οποίο υποβλήθηκε τρεις (3) ημέρες μετά την παρέλευση της νέας προθεσμίας και περιλαμβάνει τη νέα ΕΑΠΔ, το νέο αρχείο δραστηριοτήτων επεξεργασίας του ΟΑΣΑ, καθώς επίσης και την προαναφερθείσα τεχνική έκθεση της αναδόχου εταιρείας.

Στο ανωτέρω υπόμνημα, με τα συμπληρωματικά του έγγραφα, αναφέρονται τα εξής σε σχέση με τα ως άνω αναφερόμενα ευρήματα του ελέγχου:

1) Για τη μη έγκαιρη εκπόνηση ΕΑΠΔ, ο ΟΑΣΑ αναφέρει ότι, σε συνέχεια της Γνωμοδότησης 4/2017 της Αρχής, απευθύνθηκε στην ανάδοχο του έργου «HELLAS SMART TICKET Α.Ε.» (εφεξής, HST) για την οργάνωση της ως άνω μελέτης, καθώς επίσης και ότι, κατά τη συγκεκριμένη χρονική περίοδο, η εμπειρία σχετικά με την εκπόνηση εκτίμησης αντικτύπου ήταν περιορισμένη. Στις 3/5/2018, η εν λόγω μελέτη ανατέθηκε στο Εργαστήριο Νομικής Πληροφορικής της Νομικής Σχολής του Πανεπιστημίου Αθηνών (εφεξής ΕΝΠ). Με την εν λόγω ανάθεση, κατέστη σαφές ότι υπήρχαν δυσκολίες, οι οποίες πήγαζαν από το ότι απαιτείτο χρόνος για την κατανόηση από το ΕΝΠ των δραστηριοτήτων επεξεργασίας του ΑΣΣΚ και, συναφώς, των σχετικών απαιτήσεων για τη συμμόρφωση με τη νομοθεσία, ότι δεν υπήρχαν εκείνη την περίοδο πρότυπα ή μεθοδολογίες για την εκπόνηση ΕΑΠΔ, καθώς επίσης και ότι ανέκυψαν δυσκολίες αποτελεσματικής άντλησης πληροφοριών από τους αναδόχους και υπεργολάβους του ΟΑΣΑ.
2) Για τα ζητήματα που άπτονται του περιεχομένου της ΕΑΠΔ, η οποία τελικά υποβλήθηκε, όπως προαναφέρθηκε, στις 30/12/2019, ο ΟΑΣΑ αναφέρει ότι η εν λόγω μελέτη έχει έκτοτε επικαιροποιηθεί. Αλλαγές έλαβαν χώρα: i) στις 10/6/2020, σε συνέχεια περιέλευσης στον ΟΑΣΑ του πορίσματος ελέγχου, ii) στις 10/2/2022, εν όψει της ακροαματικής διαδικασίας ενώπιον της Αρχής και iii) στις 15/03/2022, σε συνέχεια αυτής και μετά τις επικοινωνίες με την HST για την εκ μέρους της υποβολή τεχνικής έκθεσης σχετικά με την εξάλειψη -μέσω των υλοποιούμενων τεχνικών κατακερματισμού και των σχετικών μέτρων ασφαλείας- της πιθανότητας

ταυτοποίησης των κατόχων των προσωποποιημένων καρτών «ATHENA CARD». Ο ΟΑΣΑ αναφέρει ότι έχει λάβει υπόψιν του, για την εκπόνηση ΕΑΠΔ, τις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29, τις σχετικές Οδηγίες της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL), τις σχετικές Οδηγίες του Βρετανικού Γραφείου Προστασίας Δεδομένων (ICO), τις προτεινόμενες Μεθοδολογίες του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA), τις Γνωμοδοτήσεις 1/2017 και 4/2017 της Αρχής, καθώς και την υπ' αριθμ. 65/2018 Απόφαση της Αρχής. Για τα επιμέρους ζητήματα αναφορικά με την ΕΑΠΔ τα οποία θίγονται στο πόρισμα του ελέγχου, ο ΟΑΣΑ παραπέμπει σχετικώς, με το υπόμνημά του, σε συγκεκριμένες ενότητες εντός της νέας έκδοσης της ΕΑΠΔ.

3) Σχετικά με το χρόνο τήρησης των δεδομένων που υφίστανται επεξεργασία στο πλαίσιο του ΑΣΣΚ, ο ΟΑΣΑ αναφέρει στο υπόμνημά του ότι το αρχείο δραστηριοτήτων έχει επικαιροποιηθεί, αναφέροντας ειδικώς, για κάθε έναν από τους σκοπούς επεξεργασίας που εξυπηρετεί το ΑΣΣΚ, τους χρόνους τήρησης των δεδομένων που υφίστανται επεξεργασία εν όψει των σκοπών αυτών. Περαιτέρω, στην επικαιροποιημένη ΕΑΠΔ επιχειρείται η τεκμηρίωση της αναγκαιότητας και αναλογικότητας της τήρησης των δεδομένων για τα εν λόγω χρονικά διαστήματα. Ειδικώς, σε σχέση με την εικοσαετία, ως απώτατο χρονικό διάστημα τήρησης των δεδομένων, επισημαίνονται τα ακόλουθα: «*Ειδικώς τα δεδομένα (επανα)φόρτισης, επικύρωσης και, συναφώς, ελέγχου κομίστρου, έχει αποφασισθεί να τηρούνται για 20 έτη προς τον σκοπό της διασφάλισης της συμμόρφωσης του ΟΑΣΑ προς τις διατάξεις της φορολογικής νομοθεσίας. Συγκεκριμένα, ενόψει της εικοσαετούς παραγραφής που προβλέπεται για τις περιπτώσεις φοροδιαφυγής (άρ. 36 παρ. 3 του Ν. 4174/2013) - και παρά το γεγονός ότι τούτο δεν επηρεάζει κατ' αρχήν τον χρόνο διαφύλαξης των βιβλίων και στοιχείων για τα φορολογικά έτη από το 2014 και έπειτα- ο ΟΑΣΑ έκρινε σκόπιμη την τήρηση των συγκεκριμένων δεδομένων για είκοσι έτη από τη συλλογή τους. Προς τούτο, ελήφθη ιδίως υπ' όψιν το γεγονός πως οι υπό εξέταση λειτουργίες ((επανα)φόρτιση και επικύρωση) δεν απαιτούν την ταύτιση με φυσικό πρόσωπο (τον κάτοχο της προσωποιημένης κάρτας). Η δε ταυτοποίηση των επιβατών κατά τον έλεγχο κομίστρου πραγματοποιείται με μόνη την (φυσική) επίδειξη του στελέχους της προσωποποιημένης κάρτας.»* Συναφώς επίσης, όπως επίσης αναφέρεται στην επικαιροποιημένη ΕΑΠΔ η οποία υποβλήθηκε μετά την ακρόαση

του υπευθύνου επεξεργασίας στην Αρχή, «*ένας χρήστης είναι πιθανό να ζητήσει ανάλυση του ιστορικού των μετακινήσεών του - των συναλλαγών 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-συναλλαγή, η οποία, πάντως, είναι ενδιαφέρουσα και από φορολογικής απόψεως*».

4) Το περιεχόμενο του αρχείου δραστηριοτήτων επεξεργασίας είχε αρχικώς καθορισθεί επί τη βάσει των διατάξεων του Υπηρεσιακού Οργανισμού του ΟΑΣΑ (ΦΕΚ ΠΡΑ.Δ.Ι.Τ. 148/22-3-2019). Σε συνέχεια της περιέλευσης του πορίσματος του ελέγχου στον Οργανισμό, το αρχείο δραστηριοτήτων επεξεργασίας επικαιροποιήθηκε, ώστε οι σκοποί επεξεργασίας να περιγράφονται τόσο αναλυτικά όσο ο ΟΑΣΑ τους είχε αρχικώς περιγράψει στην Αρχή. Περαιτέρω, επικαιροποιήθηκε το περιεχόμενο της ενημέρωσης που παρέχεται στα υποκείμενα των δεδομένων μέσω του επίσημου δικτυακού τόπου του ΟΑΣΑ. Συγκεκριμένα, οι περιγραφόμενοι στο αρχείο δραστηριοτήτων επεξεργασίας σκοποί επεξεργασίας ομαδοποιήθηκαν σύμφωνα με το περιεχόμενο της Γνωμοδότησης 1/2017 και αποτυπώθηκαν στο κείμενο της Ενημέρωσης ως ακολούθως: «*α. Αποφυγή επιβίβασης σε μέσο μεταφοράς χωρίς την καταβολή του προβλεπόμενου κομίστρου. β. Παροχή νέων υπηρεσιών στο επιβατικό κοινό όπως i) έκδοση νέας κάρτας – σε περίπτωση απώλειας για οποιοδήποτε λόγο - με μεταφορά του υπολειπόμενου προ-πληρωμένου ποσού στη νέα κάρτα, ii) επανέκδοση κάρτας, iii) επαναφόρτιση προϊόντος δικτυακά μέσω της ιστοσελίδας εξυπηρέτησης πελατών. γ. Διευκόλυνση της διαδικασίας ελέγχου παραβάσεων και επιβολής προστίμου. δ. Παροχή δυνατότητας στον ΟΑΣΑ να εξάγει στατιστικές πληροφορίες που θα του επιτρέψουν να βελτιώσει τις υπηρεσίες που παρέχει -όπως αυτές περιγράφονται στο ιστορικό της παρούσας. ε. Παροχή δυνατότητας στον ΟΑΣΑ να γνωρίζει επακριβώς το πλήθος των μετακινήσεων για εκείνες τις κατηγορίες επιβατών για τους οποίους είναι υποχρεωμένοι οι Δημόσιοι Φορείς, υπό την εποπτεία των οποίων βρίσκονται οι εν λόγω δικαιούχοι, να αποζημιώνουν τον ΟΑΣΑ για το μεταφορικό έργο που παρέχει*». Περαιτέρω, η ως άνω ενημέρωση επικαιροποιήθηκε και ως προς τις αναφερόμενες σε αυτήν περιόδους τήρησης των δεδομένων. Η

επικαιροποιημένη ενημέρωση είχε προγραμματιστεί, όπως αναφέρεται στο υπόμνημα του ΟΑΣΑ, να αναρτηθεί στον επίσημο δικτυακό τόπο του ΟΑΣΑ μέχρι τα τέλη του Μαρτίου του 2022.

5) Περαιτέρω, ο ΟΑΣΑ στο υπόμνημά του, ως προς αν τα δεδομένα που τηρούνται στο ΑΣΣΚ είναι ανώνυμα, παραπέμπει στη Γνώμη 05/2014 της Ομάδας Εργασίας του άρθρου 29, στην οποία αναφέρεται ότι ανωνυμοποιημένα είναι τα δεδομένα που έχουν λάβει τέτοια μορφή ώστε να μην είναι δυνατή η εξακρίβωση της ταυτότητας του προσώπου στο οποίο αναφέρονται με «όλα» τα «πιθανά» και εύλογα «μέσα». Στην ίδια ως άνω Γνώμη γίνεται λόγος για συναρτήσεις κατατεμαχισμού (hash functions), οι οποίες τυποποιούνται ως «τεχνικές χρήσης ψευδωνύμου». Μεταξύ των εν λόγω συναρτήσεων περιγράφεται και αυτή του κατατεμαχισμού βάσει μυστικού κλειδιού. Εν προκειμένω, ο ΟΑΣΑ κατά τη λειτουργία του ΑΣΣΚ χρησιμοποιεί συνάρτηση κατατεμαχισμού βάσει οκταψήφιου αριθμού «PIN» (αποτελούμενου από οκτώ αριθμητικά ψηφία), ο οποίος επιλέγεται ελεύθερα από τον εκάστοτε κάτοχο προσωποποιημένης κάρτας και παραμένει μυστικός. Ο ΟΑΣΑ αναφέρει ότι, όπως επισημαίνει, συναφώς, η Ομάδα Εργασίας του άρθρου 29, αν και ο Υπεύθυνος Επεξεργασίας μπορεί να «*αναπαραγάγει τη συνάρτηση στο ιδιοχαρακτηριστικό με τη χρήση του μυστικού κλειδιού, (...), η αναπαραγωγή της είναι μακράν δυσκολότερη για τον πιθανό εισβολέα εάν δεν γνωρίζει το κλειδί, διότι ο αριθμός των πιθανών τιμών που πρέπει να δοκιμαστούν είναι αρκετά μεγάλος ώστε να καθίσταται πρακτικά αδύνατη η δοκιμή τους*». Ενόψει και των εφαρμοζόμενων μέτρων ασφαλείας, τα οποία αναλυτικώς περιγράφονται στην Ενότητα υπό 3.6. της επικαιροποιημένης ΕΑΠΔ, κατά τον ΟΑΣΑ πρέπει να γίνει δεκτό ότι η ταυτοποίηση των κατόχων των προσωποποιημένων καρτών καθίσταται σχεδόν αδύνατη σε κάθε περίπτωση, ιδίως για τρίτους «εισβολείς» - παραπέμποντας σχετικώς και στην Ενότητα υπό 5.1. της επικαιροποιημένης ΕΑΠΔ.

Η Αρχή, στη συνεδρίαση της 12/4/2022, έκρινε ότι ο ΟΑΣΑ δεν έχει τεκμηριώσει με το υπόμνημά του πλήρως –καίτοι του είχε ζητηθεί– την ανάγκη τήρησης των δεδομένων μετακινήσεων για είκοσι (20) έτη, και ως εκ τούτου ζήτησε με νεότερο έγγραφο περισσότερες πληροφορίες. Ειδικότερα, με το υπ' αριθμ. πρωτ. Γ/ΕΞΕ/1178/18-05-2022, η Αρχή ζήτησε από τον ΟΑΣΑ να διευκρινίσει τα εξής:

α) Πώς συνδέεται η τήρηση των δεδομένων επαναφόρτισης, επικύρωσης και

ελέγχου κομίστρου με τη φοροδιαφυγή και γενικότερα με τις διατάξεις της φορολογικής νομοθεσίας; (βλ. επικαιροποιημένη ΕΑΠΔ, σελ. 29).

β) Γιατί επελέγη ως χρόνος τήρησης των προαναφερθέντων δεδομένων η 20ετία, ενώ η συγκεκριμένη διάταξη (άρ. 36 παρ. 3 Ν. 4174/2013) προβλέπει 10ετή προθεσμία έκδοσης πράξης διοικητικού προσδιορισμού φόρου;

Με το ίδιο έγγραφο, η Αρχή επισήμανε ότι σε κάθε περίπτωση θα πρέπει να τεκμηριώνεται αναλυτικά ο λόγος επίκλησης της διάταξης του άρθρου 36 παρ. 3 ν. 4174/2013 καθώς και η επιλογή περί τήρησης των δεδομένων για είκοσι έτη.

Περαιτέρω, με το ίδιο έγγραφο, η Αρχή ζήτησε, πέραν των ως άνω -σχετικών με τη φορολογική νομοθεσία- ζητημάτων, να διευκρινιστεί αν το ενδεχόμενο ανωνυμοποίησης των δεδομένων επαναφόρτισης, επικύρωσης και ελέγχου κομίστρου (ήτοι διαγραφή του μοναδικού αριθμού της κάρτας, με διατήρηση των λοιπών πληροφοριών όπως κατηγορία δικαιούχου, σημεία και χρόνοι επικύρωσης κτλ.), σε σύντομο χρονικό διάστημα από τη δημιουργία τους, επηρεάζει δυσμενώς τους λοιπούς σκοπούς επεξεργασίας –και σε καταφατική περίπτωση, να τεκμηριωθεί σχετικά.

Ο ΟΑΣΑ δεν ανταποκρίθηκε στο εν λόγω έγγραφο, πέραν ενός ηλεκτρονικού μηνύματος του Υπευθύνου Προστασίας Δεδομένων του ΟΑΣΑ το οποίο εστάλη στις 30-8-2022 (αρ. πρωτ.: Γ/ΕΙΣ/3066/30-8-2022) και ανέφερε, μεταξύ άλλων, ότι θα υπήρχε απάντηση εντός 10 ημερών.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου και των διαμειφθέντων στην από 15-02-2022 συνεδρίαση, αφού άκουσε τον εισηγητή και τις διευκρινίσεις των βοηθών εισηγητή, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Σύμφωνα με τις διατάξεις των άρθρων 51 και 55 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (εφεξής, ΓΚΠΔ) και του άρθρου 9 του ν. 4624/2019 (ΦΕΚ Α΄ 137), η Αρχή έχει αρμοδιότητα να εποπτεύει την εφαρμογή των διατάξεων του ΓΚΠΔ, του νόμου

αυτού και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων.

2. Σύμφωνα με το άρθρο 4 στοιχ. 1 του ΓΚΠΔ, ως «δεδομένα προσωπικού χαρακτήρα» νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»), ενώ το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, αριθμός ταυτότητας, δεδομένα θέσης, επιγραμμικό αναγνωριστικό ταυτότητας ή ένας ή περισσότεροι παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

3. Ως ψευδωνυμοποίηση ορίζεται, κατά το άρθρο 4 στοιχ. 5 του ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Συναφώς στη σκέψη 26 του ΓΚΠΔ, αναφέρεται ότι «*τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο. Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας».*

4. Περαιτέρω, σύμφωνα με το άρθρο 4 στοιχ. 7 του ΓΚΠΔ, ως υπεύθυνος επεξεργασίας ορίζεται «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που,

μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα».

5. Σύμφωνα με το άρθρο 5 παρ. 1 του Γενικού Κανονισμού Προστασίας Δεδομένων, τα δεδομένα προσωπικού χαρακτήρα:

α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»),

β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς («περιορισμός του σκοπού»),

γ) είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»),

δ) είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»),

ε) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 του ΓΚΠΔ και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»),

στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

6. Περαιτέρω, σύμφωνα με την παρ. 2 του ιδίου άρθρου, «*ο υπεύθυνος επεξεργασίας φέρει*

την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»)». Η εισαγωγή της αρχής της λογοδοσίας μετατοπίζει το «βάρος της απόδειξης», όσον αφορά τη νομιμότητα της επεξεργασίας και τη συμμόρφωση με τον ΓΚΠΔ, από τις αρχές προστασίας δεδομένων στους ίδιους τους υπευθύνους επεξεργασίας ή τους εκτελούντες. Ο ΓΚΠΔ παρέχει στους υπευθύνους επεξεργασίας/εκτελούντες μια σειρά ρυθμιστικών μεθόδων και εργαλείων για τον σκοπό αυτό, όπως -μεταξύ άλλων- την τήρηση αρχείων δραστηριοτήτων επεξεργασίας, την εφαρμογή μέτρων ασφαλείας και την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων.

7. Εξάλλου, για να είναι σύννομη μία επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να έχει ως νομική βάση μία εξ αυτών που περιγράφονται στο άρθρο 6 του ΓΚΠΔ. Σύμφωνα με τη διάταξη του άρθρου 6 παρ. 1, «*η επεξεργασία είναι σύννομη, μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις (…) στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί*». Ωστόσο, όπως ορίζεται στο επόμενο εδάφιο της ίδιας διάταξης, η εν λόγω νομική βάση δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους. Όπως διευκρινίζει σχετικά η αιτιολογική σκέψη 47 του ΓΚΠΔ, ο δικαιολογητικός λόγος της απαγόρευσης εφαρμογής της νομικής βάσης αυτής στην επεξεργασία που κάνουν οι δημόσιες αρχές κατά την εκπλήρωση των καθηκόντων τους, έγκειται στην αρχή της νομιμότητας, δηλαδή στο γεγονός ότι, όσον αφορά τις δημόσιες αρχές, εναπόκειται στο νομοθέτη να παρέχει δια νόμου τη νομική βάση για την επεξεργασία στην οποία προβαίνουν.

8. Το άρθρο 4 του ν. 4624/2019 προβλέπει ότι «ως «δημόσιος φορέας» νοούνται οι δημόσιες αρχές, οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, τα νομικά πρόσωπα δημοσίου δικαίου, οι Ο.Τ.Α. πρώτου και δεύτερου βαθμού και τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό.»

9. Ο ΟΑΣΑ αποτελεί σύμφωνα με τον ιδρυτικό αυτού νόμο 2175/1993, νομικό πρόσωπο ιδιωτικού δικαίου και ειδικότερα δημόσια επιχείρηση κοινωφελούς χαρακτήρα με τη μορφή της ανώνυμης εταιρείας· εποπτεύεται από τον Υπουργό Μεταφορών και Επικοινωνιών και το μετοχικό του κεφάλαιο ανήκει στο Δημόσιο (βλ. ν. 2175/1993, άρ. 1, 2), ενώ ο πρόεδρος και ο διευθύνων σύμβουλος αυτού ορίζονται με κοινή απόφαση του Υπουργού Εθνικής Οικονομίας, Οικονομικών και του Υπουργού Μεταφορών και Επικοινωνιών (βλ. ν. 2175/1993, άρ. 2, παρ. 3).

10. Ο ΓΚΠΔ δεν ορίζει τι συνιστά «δημόσια αρχή ή δημόσιο φορέα»[3]. Η Ομάδα Εργασίας του άρθρου 29 στις Κατευθυντήριες Γραμμές σχετικά με τους υπευθύνους προστασίας δεδομένων (WP 243)[4], οι οποίες έχουν υιοθετηθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, εκτιμά ότι η έννοια αυτή πρέπει να προσδιορίζεται από τα εθνικά δίκαια, αλλά θεωρεί ότι η εκπλήρωση δημόσιου καθήκοντος και η άσκηση δημόσιας εξουσίας είναι δυνατή όχι μόνο από δημόσιες αρχές ή δημόσιους φορείς, αλλά και από άλλα φυσικά ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου, σε διάφορους τομείς που απορρέουν από την εθνική νομοθεσία κάθε κράτους μέλους, όπως οι υπηρεσίες δημόσιων μεταφορών, η ύδρευση και η παροχή ενέργειας, οι οδικές υποδομές, η δημόσια ραδιοτηλεόραση, η κατασκευή εργατικών κατοικιών, ή πειθαρχικά όργανα για νομοθετικά κατοχυρωμένα επαγγέλματα. Στις περιπτώσεις αυτές, τα υποκείμενα των δεδομένων είναι πιθανό να βρεθούν σε θέση που ομοιάζει πολύ με την επεξεργασία των δεδομένων τους από δημόσια αρχή ή δημόσιο φορέα. Συγκεκριμένα, είναι δυνατή η επεξεργασία δεδομένων για παρόμοιους σκοπούς και, ομοίως, τα φυσικά πρόσωπα έχουν συνήθως ελάχιστη ή καμία δυνατότητα επιλογής ως προς το εάν και το πώς θα υποβληθούν σε επεξεργασία τα δεδομένα τους. Η άποψη αυτή της Ομάδας Εργασίας του άρθρου 29 απηχεί και την κρατούσα οπτική της ελληνικής θεωρίας και νομολογίας, σύμφωνα με τις οποίες οι δημόσιες επιχειρήσεις που παρέχουν υπηρεσίες ζωτικής σημασίας για το κοινωνικό σύνολο, ασχέτως της μορφής τους ως νομικών προσώπων ιδιωτικού δικαίου, επιδιώκουν το δημόσιο σκοπό της διασφάλισης στο κοινωνικό σύνολο εκείνων των ζωτικών αγαθών και υπηρεσιών χωρίς τα οποία δεν

[3] Βλ. την έννοια “public authority or body” στις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του Άρθρου 29 για τον Υπεύθυνο Προστασίας Δεδομένων – διαθέσιμες στο σύνδεσμο https://ec.europa.eu/newsroom/article29/items/612048 .

[4] Βλ. δικτυακό σύνδεσμο ανωτέρω

υφίστανται οι ομαλοί όροι για την κατά τα σύγχρονα κριτήρια αξιοπρεπή διαβίωση του ανθρώπου και την ελεύθερη ανάπτυξη της προσωπικότητας και δραστηριότητας που εγγυάται το Σύνταγμα. Προκειμένου δε να διασφαλιστεί η διαφύλαξη των συνταγματικών εγγυήσεων που περιβάλλουν τις ζωτικής σημασίας παρεχόμενες υπηρεσίες (πχ δημόσιες συγκοινωνίες, ύδρευση, αποχέτευση κ.α.), το κράτος, δια της ρυθμιστικής εποπτείας και του ιδιοκτησιακού ελέγχου που ασκεί στις δημόσιες επιχειρήσεις, μετέχοντας κατά πλειοψηφία στο μετοχικό τους κεφάλαιο, χρησιμοποιεί εργαλεία του διοικητικού δικαίου που ουσιαστικά συνιστούν ενάσκηση δημόσιας εξουσίας[5].

11. Αναφορικά με την αρχή της διαφάνειας της επεξεργασίας, ο ΓΚΠΔ θέτει συγκεκριμένες υποχρεώσεις στους υπευθύνους επεξεργασίας ως προς την ενημέρωση που οφείλουν να παρέχουν στα υποκείμενα των δεδομένων. Ειδικότερα, σύμφωνα με το άρθρο 12 παρ. 1 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται στο άρθρο 13 – στο οποίο ορίζεται ειδικώς ότι «*όταν δεδομένα προσωπικού χαρακτήρα που αφορούν υποκείμενο των δεδομένων συλλέγονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες: α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας, β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση, γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία, δ) εάν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν (…)» (*βλ. παρ. 1 του άρθρου 13 του ΓΚΠΔ). Περαιτέρω, στην παρ. 2 του ιδίου άρθρου, προβλέπεται ότι «*εκτός από τις πληροφορίες που αναφέρονται στην παράγραφο 1, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων*

[5] Βλ. ΟλΣτΕ 190/2022, Πρακτ. Επεξεργασίας ΣτΕ 385/1995 και 608/1995 σε ΤοΣ 1996 σελ. 285 επ. Πρακτ. Επεξεργασίας ΣτΕ 38/1998 για τη μετατροπή των Οργανισμών Κεντρικής Αγοράς Αθηνών και Κεντρικής Αγοράς Θεσσαλονίκης σε ΝΠΙΔ.

προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων τις εξής επιπλέον πληροφορίες που είναι αναγκαίες για την εξασφάλιση θεμιτής και διαφανούς επεξεργασίας: α) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα (…)».

12. Το άρθρο 25 παρ. 1 του ΓΚΠΔ ορίζει την αρχή της προστασίας ήδη από το σχεδιασμό ως εξής: «*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 από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων*». Ειδικότερα δε ως προς την ασφάλεια της επεξεργασίας, στο άρθρο 32 παρ. 1 του ΓΚΠΔ ορίζεται ότι «*λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, (…)*».

13. Αναφορικά με την εκτίμηση αντικτύπου ως προς την προστασία δεδομένων, το άρθρο 35 του ΓΚΠΔ ορίζει 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. Περαιτέρω, η ΕΑΠΔ αποτελεί βασικό εργαλείο για την ικανοποίηση της αρχής της προστασίας των δεδομένων από το σχεδιασμό, όπως προσδιορίζεται στο άρθρο 25 παρ. 1 του ΓΚΠΔ (βλ. Απόφαση 50/2021 της Αρχής).

14. Η Αρχή κατήρτισε, βάσει του άρθρου 35 παρ. 4 του ΓΚΠΔ, κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια ΕΑΠΔ (βλ. Απόφαση 65/2018 της Αρχής). Σύμφωνα με την εν λόγω κατάλογο, απαιτείται εκπόνηση εκτίμησης αντικτύπου σε περίπτωση, μεταξύ άλλων, «*συστηματικής και σε μεγάλη κλίμακα επεξεργασίας για την παρακολούθηση, την παρατήρηση ή τον έλεγχο των φυσικών προσώπων με χρήση δεδομένων που συλλέγονται μέσω συστημάτων βιντεοεπιτήρησης ή μέσω δικτύων ή με οποιοδήποτε άλλο μέσο σε δημόσιο χώρο, δημοσίως προσβάσιμο χώρο ή ιδιωτικό χώρο προσιτό σε απεριόριστο αριθμό προσώπων. Περιλαμβάνει την παρακολούθηση των κινήσεων ή της τοποθεσίας/γεωγραφικής θέσης σε πραγματικό ή μη χρόνο ταυτοποιημένων ή ταυτοποιήσιμων φυσικών προσώπων. Σχετικά παραδείγματα είναι η χρήση καμερών σε εμπορικό κέντρο ή σε σταθμούς μέσων μαζικής μεταφοράς, ή η επεξεργασία δεδομένων θέσης των επιβατών σε αεροδρόμιο ή σε μέσα μαζικής μεταφοράς*».

15. Στη συγκεκριμένη περίπτωση, αναφορικά με την επεξεργασία δεδομένων μέσω του ΑΣΣΚ, ο ΟΑΣΑ αποτελεί τον υπεύθυνο επεξεργασίας κατά την έννοια του άρθρου 4 στοιχ. 7 του ΓΚΠΔ. Επισημαίνεται ότι, για τα προσωποποιημένα εισιτήρια, η επεξεργασία δεδομένων που πραγματοποιείται από το ΑΣΣΚ αναφορικά με τις κινήσεις του επιβατικού κοινού αποτελεί επεξεργασία προσωπικών και όχι ανώνυμων δεδομένων, παρά το ότι δεν τηρούνται ονοματεπώνυμα επιβατών. Και τούτο διότι στη βάση δεδομένων του ΑΣΣΚ αποθηκεύεται το «ψηφιακό αποτύπωμα» («hashed value») που προκύπτει από τον συνδυασμό του ΑΜΚΑ του επιβάτη (ή αριθμού διαβατηρίου ή άλλου επίσημου εγγράφου ταυτοποίησης) και του 8-ψήφιου κωδικού (PIN), καθώς και ο μήνας και έτος γέννησης αλλά και η ειδική κατηγορία του δικαιούχου. Συνεπώς, ο ΑΜΚΑ και ο 8-ψήφιος κωδικός που επιλέγει ο κάθε χρήστης, αποτελούν τις πληροφορίες εκείνες οι οποίες επιτρέπουν[6] την αντιστοίχιση του ΑΜΚΑ με το ψηφιακό αποτύπωμα – και άρα, την αναγνώριση (μέσω του ΑΜΚΑ) του επιβάτη που κατέχει κάρτα με συγκεκριμένο

[6] Καίτοι από το αποτύπωμα δεν μπορεί να εξαχθεί ο ΑΜΚΑ ή ο κωδικός, εν τούτοις για γνωστό ΑΜΚΑ και κωδικό μπορεί να γίνει ευχερώς επαλήθευση αν αυτά αντιστοιχούν ή όχι στο συγκεκριμένο ψηφιακό αποτύπωμα.

αριθμό, το οποίο κατ' επέκταση, επιτρέπει την αναγνώριση των μετακινήσεών του. Ο ΟΑΣΑ, ορθώς, δεν τηρεί τις εν λόγω πληροφορίες (βλ. και Γνωμοδοτήσεις 1/2017 και 4/2017 της Αρχής), κατ' εφαρμογή της αρχής της ελαχιστοποίησης των δεδομένων, σύμφωνα το άρθρο 5 παρ. 1 στοιχ. γ' του ΓΚΠΔ, αλλά και στο πλαίσιο των υποχρεώσεών του για προστασία των δεδομένων ήδη από το σχεδιασμό (άρθρο 25 του ΓΚΠΔ) και για ασφαλή επεξεργασία (άρθρο 32 του ΓΚΠΔ). Οι εν λόγω πληροφορίες είναι στην κατοχή μόνο του κάθε υποκειμένου των δεδομένων (κατόχου κάρτας) προκειμένου, όποτε το θελήσει (ιδίως σε περίπτωση απώλειας της κάρτας του) να αποδείξει ότι πράγματι κατείχε κάρτα με συγκεκριμένο αριθμό. Τούτο όμως δεν καθιστά τα δεδομένα ανώνυμα, αλλά ψευδωνυμοποιημένα, αφού τελικά υπάρχουν συμπληρωματικές πληροφορίες (στην κατοχή του ίδιου του υποκειμένου των δεδομένων) που επιτρέπουν την απόδοσή τους σε συγκεκριμένο φυσικό πρόσωπο. Εξάλλου, όπως αναλύεται στη συνέχεια, λαμβάνοντας υπόψη τα μέσα που μπορεί ευλόγως να χρησιμοποιήσει ο υπεύθυνος επεξεργασίας, δεν μπορεί να αποκλειστεί η δυνατότητα άρσης της ψευδωνυμοποίησης – ενώ εξάλλου, το γεγονός ότι ο ΟΑΣΑ, για τους λόγους που επικαλείται και οι οποίοι αναφέρθηκαν ήδη ανωτέρω, τηρεί τα δεδομένα μετακινήσεων για είκοσι (20) έτη, καταδεικνύει ότι τα εν λόγω δεδομένα δεν μπορούν να χαρακτηριστούν ως ανώνυμα.

16. Αναφορικά με την υλοποίηση της ΕΑΠΔ, ο ΟΑΣΑ επικαλείται για τους λόγους καθυστέρησης εκπόνησής της, μεταξύ άλλων, τη δυσκολία συγκέντρωσης πληροφοριών για το σύστημα από τους αναδόχους. Οι ανωτέρω όμως ισχυρισμοί, όπως προβάλλονται, δεν συνιστούν λόγο που δικαιολογεί την καθυστέρηση αυτή. Σημειώνεται ότι σύμφωνα με το άρθρο 28 του ΓΚΠΔ, «*η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας. Η εν λόγω σύμβαση ή άλλη νομική πράξη προβλέπει ειδικότερα ότι ο εκτελών την επεξεργασία: (…) στ) συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία (…)».* Ως εκ τούτου, ο υπεύθυνος

επεξεργασίας θα έπρεπε να λάβει τα κατάλληλα μέτρα προκειμένου να διασφαλίσει την έγκαιρη εκπόνηση της εκτίμησης αντικτύπου ως προς τα προσωπικά δεδομένα, αλλά και την υλοποίηση των όποιων διορθωτικών μέτρων ενδεχομένως κατεδείκνυε το αποτέλεσμα της μελέτης, χωρίς να μπορεί η υποχρέωση αυτή να αρθεί λόγω δυσκολιών που απορρέουν ως προς τη συλλογή στοιχείων από τους εκτελούντες την επεξεργασία.

17. Αναφορικά με το περιεχόμενο της επικαιροποιημένης ΕΑΠΔ, η οποία υποβλήθηκε μετά την ακρόαση του υπευθύνου επεξεργασίας ενώπιον της Αρχής, καίτοι είναι πράγματι βελτιωμένη σε σχέση με την αρχική της έκδοση (η οποία είχε υποβληθεί μετά τον επιτόπιο έλεγχο της Αρχής), παρατηρούνται τα εξής: Η νέα ΕΑΠΔ, αναφέρει ότι έχει ως βάση της τη σχετική μεθοδολογία της CNIL[7] (με γενική παραπομπή στον ιστότοπο της CNIL). Ωστόσο, δεν φαίνεται να υπάρχει απόλυτη συμφωνία με τα βήματα που περιγράφονται σε σχετικά εγχειρίδια της CNIL που είναι διαθέσιμα στο διαδικτυακό της τόπο. Τούτο από μόνο του δεν συνιστά μεν ελλιπή εκπόνηση ΕΑΠΔ, αφού δεν υπάρχει υποχρέωση υιοθέτησης, από τον υπεύθυνο επεξεργασίας, κάποιας συγκεκριμένης μεθοδολογίας, ωστόσο, εξακολουθούν να υπάρχουν κάποια σημεία ασαφή ή και ελλείψεις ως προς την προσέγγιση που τελικά ακολουθήθηκε για την αποτίμηση των κινδύνων. Τα σημεία αυτά μπορούν να συνοψιστούν ως εξής:

α. Μη σαφής τεκμηρίωση του τρόπου υπολογισμού του εκάστοτε κινδύνου που αποτελεί έλλειψη άμεσα συνυφασμένη με τη μη σαφή τεκμηρίωση του προσδιορισμού τόσο της πιθανότητας επέλευσης του κάθε κινδύνου όσο και των σχετικών συνεπειών από την επέλευσή του (αναλυτικότερη τεκμηρίωση δίνεται στο εμπιστευτικό παράρτημα της παρούσας).

β. Ως άμεση απόρροια του ανωτέρω, φαίνεται ότι, αν και πράγματι λαμβάνονται μέτρα αντιμετώπισης για διάφορους κινδύνους τα οποία είναι προς τη σωστή κατεύθυνση, υπάρχουν ακόμα περιθώρια λήψης πρόσθετων μέτρων, ιδίως ως προς την αντιμετώπιση του κινδύνου της μη εξουσιοδοτημένης αντιστοίχισης των μετακινήσεων ενός επιβάτη με τον ΑΜΚΑ αυτού (αναλυτικότερη τεκμηρίωση δίνεται στο εμπιστευτικό παράρτημα της παρούσας). Ως εκ τούτου, τίθεται εκ των πραγμάτων ζήτημα μη πλήρους συμμόρφωσης με την αρχή της προστασίας των δεδομένων ήδη από το

[7] Πρόκειται για την εποπτική Αρχή προστασίας δεδομένων της Γαλλίας

σχεδιασμό, βάσει του άρθρου 25 του ΓΚΠΔ.

γ. Δεν φαίνεται να έχει γίνει, εντός της ΕΑΠΔ, ορθή εκτίμηση της νομικής βάσης για τους διάφορους σκοπούς επεξεργασίας (τούτο αναλύεται περαιτέρω στη συνέχεια, στη Σκέψη 19)

δ. Η ΕΑΠΔ δεν εξετάζει ζητήματα που άπτονται της διαφάνειας της επεξεργασίας αλλά και των λοιπών δικαιωμάτων των υποκειμένων των δεδομένων. Γενικότερα, η ΕΑΠΔ εστιάζει κυρίως σε ζητήματα ασφάλειας της επεξεργασίας και όχι τόσο σε λοιπούς κινδύνους προστασίας δεδομένων (π.χ. δεν εξετάζεται αν οι συμβάσεις με εκτελούντες την επεξεργασία αντιμετωπίζουν τους διάφορους κινδύνους κ.α., ενώ δεν παρέχει επαρκή τεκμηρίωση ούτε για το ζήτημα του χρόνου τήρησης των δεδομένων, όπως περιγράφεται στη συνέχεια στη Σκέψη 18).

18. Αναφορικά με τους χρόνους τήρησης των δεδομένων για τους διάφορους σκοπούς επεξεργασίας, ο ΟΑΣΑ, ο οποίος δεν είχε προσδιορίσει χρόνους τήρησης των δεδομένων κατά τη χρονική στιγμή του επιτόπιου ελέγχου και, μετά τον έλεγχο, όρισε χρόνο τήρησης τα 20 έτη για όλα τα δεδομένα, ανεξαρτήτως των σκοπών επεξεργασίας, έχει προχωρήσει πλέον σε εξειδίκευση των χρόνων τήρησης για τους διάφορους σκοπούς επεξεργασίας δεδομένων –χωρίς να ισχύει πλέον το διάστημα της εικοσαετίας καθολικά για όλους τους σκοπούς. Ωστόσο, εν τέλει, φαίνεται ότι τα δεδομένα μετακινήσεων εξακολουθούν να τηρούνται για εικοσαετία, με το σκεπτικό ότι η τήρησή τους δικαιολογείται για φορολογικούς σκοπούς, «ενόψει –όπως αναφέρει ο ΟΑΣΑ στο υπόμνημά του- της εικοσαετούς παραγραφής που προβλέπεται για τις περιπτώσεις φοροδιαφυγής (άρ. 36 παρ. 3 του Ν. 4174/2013)». Τα παραδείγματα που αναφέρει δεν σχετίζονται με φορολογικές υποχρεώσεις του Οργανισμού αλλά με αιτήματα τα οποία μπορούν να υποβάλουν τα υποκείμενα των δεδομένων. Συγκεκριμένα, όπως αναφέρεται και στην επικαιροποιημένη ΕΑΠΔ, «*ένας χρήστης είναι πιθανό να ζητήσει ανάλυση του ιστορικού των μετακινήσεών του - των συναλλαγών 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-συναλλαγή, η οποία, πάντως, είναι*

ενδιαφέρουσα και από φορολογικής απόψεως». Όπως επισημάνθηκε και στο ιστορικό της παρούσας, ο ΟΑΣΑ δεν ανταποκρίθηκε σε νεότερο έγγραφο της Αρχής προκειμένου να παρέχει περισσότερες διευκρινίσεις επ' αυτού εξηγώντας, μεταξύ άλλων, γιατί επελέγη ως χρόνος τήρησης των προαναφερθέντων δεδομένων η 20ετία με επίκληση εικοσαετούς παραγραφής σε περιπτώσεις φοροδιαφυγής χωρίς επίκληση συγκεκριμένης διάταξης, ενώ η διάταξη του άρθρου 36 παρ. 3 ν. 4174/2013, σύμφωνα με την οποία ήταν δυνατή η έκδοση πράξης προσδιορισμού φόρου σε περιπτώσεις φοροδιαφυγής εντός είκοσι ετών και την οποία επικαλέστηκε ο ΟΑΣΑ, έχει αντικατασταθεί με το άρθρο 32 παρ. 2 του ν. 4646/2019, με το οποίο η προθεσμία για την έκδοση της πράξης προσδιορισμού φόρου ορίζεται σε δέκα έτη.

19. Ο ΟΑΣΑ, για διάφορους σκοπούς επεξεργασίας, αναφέρει ως νομική βάση της επεξεργασίας τη διάταξη του άρθρου 6 παρ. 1 στοιχ. στ' (τούτο ισχύει τόσο στην επικαιροποιημένη ΕΑΠΔ όσο και στο επικαιροποιημένο αρχείο δραστηριοτήτων επεξεργασίας, τα οποία υπέβαλε στην Αρχή σε συνέχεια των ευρημάτων του πορίσματος ελέγχου της Αρχής το οποίο του γνωστοποιήθηκε). Ωστόσο, για τους λόγους που εκτέθηκαν ανωτέρω, η εν λόγω νομική βάση δεν μπορεί να χρησιμοποιηθεί από τον ΟΑΣΑ, ο οποίος αποτελεί δημόσια επιχείρηση κοινωφελούς χαρακτήρα, που εποπτεύεται και ελέγχεται ιδιοκτησιακά από το κράτος. Άλλωστε η επίκληση από τον ΟΑΣΑ για ορισμένους σκοπούς επεξεργασίας ως νομικής βάσης της διάταξης του άρθρου 6 παρ. 1 στοιχ. ε' (επεξεργασία απαραίτητη για την εκπλήρωση καθήκοντος που σχετίζεται με την άσκηση δημόσιας εξουσίας που έχει ανατεθεί), επιρρωνύει την άποψη ότι ο ΟΑΣΑ, ως δημόσια επιχείρηση κοινωφελούς χαρακτήρα, εντάσσεται στην έννοια των «δημοσίων αρχών», κατά την έννοια του άρθρου 6 παρ. 1 τελευταίο εδάφιο, πέραν της αντίφασης που υπάρχει με την ταυτόχρονη επίκληση ως νομικής βάσης του άρθρου 6 παρ. 1 στοιχ. στ' .

Εξάλλου, πρέπει να σημειωθεί ότι η αναγνώριση και επιλογή της κατάλληλης νομικής βάσης εκ των προβλεπομένων στο άρθρο 6 παρ. 1 ΓΚΠΔ είναι στενά συνδεδεμένη με την αρχή της θεμιτής ή δίκαιης επεξεργασίας καθώς και με την αρχή του περιορισμού του σκοπού, ο δε υπεύθυνος επεξεργασίας οφείλει όχι μόνο να επιλέξει την κατάλληλη νομική βάση προ της έναρξης της επεξεργασίας, αλλά και να ενημερώσει, κατ' αρ. 13 παρ. 1 εδ. γ' και 14 παρ. 1 εδ. γ' ΓΚΠΔ, για την χρήση της το υποκείμενο των δεδομένων, καθώς η επιλογή της κάθε νομικής βάσης ασκεί έννομη επιρροή στην εφαρμογή των

δικαιωμάτων των υποκειμένων[8].

Επιπλέον, έκφραση της αρχής της νομιμότητας της επεξεργασίας είναι και η αρχή της διαφάνειας[9]. Δυνάμει του άρθρου 5 παρ. 1 στοιχ. α' ΓΚΠΔ, πέραν της απαίτησης τα δεδομένα να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία, η διαφάνεια περιλαμβάνεται ρητώς ως θεμελιώδης πτυχή αυτών των αρχών, συνδέεται δε εγγενώς τόσο με τη νομιμότητα όσο και με την αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας πρέπει να είναι πάντα σε θέση να αποδεικνύει ότι τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία με διαφάνεια όσον αφορά τα υποκείμενα των δεδομένων[10].

Συναφώς, δεν μπορεί μεν να αποκλεισθεί σε συγκεκριμένες περιπτώσεις το ενδεχόμενο παράλληλης – ταυτόχρονης εφαρμογής διαφορετικών νομικών βάσεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα, τούτο όμως είναι επιτρεπτό μόνο αν χρησιμοποιούνται στο σωστό πλαίσιο και ιδίως εφόσον εξυπηρετούν διαφορετικούς σκοπούς επεξεργασίας, ενώ για τον ίδιο σκοπό επεξεργασίας, ο υπεύθυνος επεξεργασίας πρέπει εξ αρχής να επιλέξει μία συγκεκριμένη νομική βάση, την πλέον κατάλληλη σε σχέση με τον συγκεκριμένο σκοπό. Κατ' αυτόν τον τρόπο, και τα υποκείμενα των δεδομένων γνωρίζουν επακριβώς, χωρίς να καταλείπεται αμφιβολία, την ορθή νομική βάση της εκάστοτε επεξεργασίας, ενώ και ο υπεύθυνος επεξεργασίας, ως προς το σκέλος αυτό, συμμορφώνεται με την αρχή της λογοδοσίας του άρθρου 5 παρ. 2 του ΓΚΠΔ, αφού, σύμφωνα με τη διάταξη αυτή, όπως προαναφέρθηκε, φέρει ο ίδιος το βάρος της επίκλησης και απόδειξης της νομιμότητας της επεξεργασίας, η οποία δεν προκύπτει, όταν παρουσιάζονται ταυτόχρονα δύο διαφορετικές νομικές βάσεις για τον ίδιο σκοπό επεξεργασίας.

20. Αναφορικά με την ενημέρωση των υποκειμένων των δεδομένων για τους σκοπούς επεξεργασίας, έχει επικαιροποιηθεί η ιστοσελίδα του ΟΑΣΑ σύμφωνα με όσα αναφέρει ο οργανισμός στο υπόμνημά του (τελευταία πρόσβαση στην ιστοσελίδα του ΟΑΣΑ: 9/6/2023). Ωστόσο, για τους εξής σκοπούς επεξεργασίας: α) να είναι δυνατή η μελέτη

[8] βλ. υπ' Αριθμ. 26/2019 Απόφαση της Αρχής

[9] Βλ. Αιτ. Σκ. 39, 60 ΓΚΠΔ. Βλ. επίσης ΔΕΕ C-496/17 σκ. 59 και ΔΕΕ C-201/14 σκ. 31-35 και ιδίως 34. Βλ. επίσης ενδεικτικά Αποφάσεις 50/2021, 35/2022, 43/2022 της Αρχής.

[10] Βλ. Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679 της Ο.Ε. του άρθρου 29 WP 260

ανωνυμοποιημένων στατιστικών δεδομένων από τον ΟΑΣΑ και από τρίτους, με τρόπο όμως που να μην δύνανται αυτοί να ταυτοποιήσουν το υποκείμενο των προσωπικών δεδομένων, β) να είναι δυνατή η διαχείριση των δικτυακών τόπων και της κάθε μορφής επικοινωνίας, γίνεται αναφορά, ως προς τις νομικές βάσεις για την επεξεργασία, σε τρεις νομικές βάσεις, αποτρέποντας με αυτόν τον τρόπο την ευχερή αναγνώριση της ορθής για τον κάθε σκοπό, σύμφωνα με όσα αναφέρονται ανωτέρω στη Σκέψη 19 - ενώ μία εκ των νομικών βάσεων είναι το έννομο συμφέρον του ΟΑΣΑ, η οποία, όπως προαναφέρθηκε, δεν μπορεί να έχει εφαρμογή στη συγκεκριμένη περίπτωση.

21. Συμπερασματικά, η Αρχή διαπιστώνει για τον ΟΑΣΑ τις κάτωθι παραβάσεις:

α. Παράβαση του άρθρου 5 παρ. 1 στοιχ. ε’ του ΓΚΠΔ αναφορικά με την αρχή του περιορισμού του χρόνου αποθήκευσης (βλ. ανωτέρω Σκέψη 18 της παρούσας, αλλά και το Εύρημα 3 του πορίσματος του ελέγχου).

β. Παράβαση του άρθρου 35 παρ. 1 του ΓΚΠΔ ως προς την εκπόνηση ΕΑΠΔ, αφού αυτή δεν είχε εκπονηθεί έγκαιρα (δεν ήταν διαθέσιμη κατά τη στιγμή του επιτόπιου ελέγχου – βλ. Εύρημα 1 του πορίσματος ελέγχου), ενώ και μετά την εκπόνησή της, αλλά ακόμα και μετά και τις διάφορες αναθεωρήσεις της, προκύπτει ότι δεν έχει εκπονηθεί κατά τρόπο τέτοιο ώστε να τεκμηριώνεται απόλυτα η αντιμετώπιση όλων των κινδύνων προστασίας δεδομένων (βλ. ανωτέρω Σκέψη 17). Περαιτέρω, και στην επικαιροποιημένη ΕΑΠΔ παρατηρείται προβληματική παράθεση των νομικών βάσεων (βλ. Σκέψη 17, σημείο γ’).

γ. Παράβαση του άρθρου 25 παρ. 1 του ΓΚΠΔ αναφορικά με την προστασία των δεδομένων ήδη από το σχεδιασμό, αφού, καίτοι έχουν πράγματι ληφθεί εκ σχεδιασμού μέτρα αντιμετώπισης διαφόρων κινδύνων, προκύπτει ότι υπάρχουν περιθώρια και για πρόσθετα μέτρα, για τα οποία δεν τεκμηριώνεται η μη αναγκαιότητα υλοποίησής τους τους (βλ. ανωτέρω Σκέψη 17, σημείο β’ αυτής).

δ. Παράβαση του άρθρου 30 παρ. 1 του ΓΚΠΔ αναφορικά με την ορθή τήρηση του αρχείου δραστηριοτήτων, αφού αυτό δεν ήταν ορθά συμπληρωμένο (υπήρχε ασάφεια στην περιγραφή των σκοπών επεξεργασίας, όπως περιγράφεται στο Εύρημα 4 του πορίσματος του ελέγχου).

Η ανωτέρω υπό στοιχ. δ’ παράβαση θεραπεύτηκε από τον υπεύθυνο επεξεργασίας, όπως προκύπτει από το υπόμνημα με τα συνοδευτικά αυτού έγγραφα που υποβλήθηκαν στην Αρχή μετά την ακρόασή του ενώπιον της Αρχής. Ωστόσο, στο

επικαιροποιημένο αρχείο δραστηριοτήτων παρατίθενται -καίτοι δεν υπάρχει η σχετική υποχρέωση από τις προβλέψεις του άρθρου 30 του ΓΚΠΔ– οι αντίστοιχες νομικές βάσεις για τους διάφορους σκοπούς επεξεργασίας, για τις οποίες προκύπτει ασάφεια σύμφωνα με τα όσα περιγράφονται ανωτέρω στη Σκέψη 19, κατά παράβαση του άρθρου 6 παρ. 1 του ΓΚΠΔ αλλά και στην ενημέρωση που παρέχεται στα υποκείμενα των δεδομένων μέσω της ιστοσελίδας του οργανισμού (βλ. Σκέψη 20). Ως εκ τούτου, η Αρχή επισημαίνει ότι ο ΟΑΣΑ θα πρέπει να προβεί στις κατάλληλες ενέργειες προκειμένου να είναι απόλυτα σαφές ποια είναι η ορθή νομική βάση για τον κάθε σκοπό επεξεργασίας που διενεργείται μέσω του ΑΣΣΚ, και τούτο θα πρέπει να παρέχεται ως ενημέρωση και στα υποκείμενα των δεδομένων.

22. Με βάση τα ανωτέρω, η Αρχή κρίνει ότι συντρέχει περίπτωση να ασκήσει τις κατά το άρθρο 58 παρ. 2 του ΓΚΠΔ διορθωτικές εξουσίες της σε σχέση με τις διαπιστωθείσες παραβάσεις.

23. Η Αρχή κρίνει περαιτέρω ότι πρέπει, με βάση τις περιστάσεις που διαπιστώθηκαν, να επιβληθεί, κατ' εφαρμογή της διάταξης του άρθρου 58 παρ. 2 εδ. θ' του ΓΚΠΔ, αποτελεσματικό, αναλογικό και αποτρεπτικό διοικητικό χρηματικό πρόστιμο κατ' άρθρο 83 του ΓΚΠΔ.

24. Περαιτέρω η Αρχή, έλαβε υπόψη τα κριτήρια επιμέτρησης του προστίμου που ορίζονται στο άρθρο 83 παρ. 2 του ΓΚΠΔ, τις παραγράφους 4 και 5 του ίδιου άρθρου που έχουν εφαρμογή στην παρούσα υπόθεση, το άρθρο 39 παρ. 1 και 2 του ν. 4624/2019 που αφορά την επιβολή διοικητικών κυρώσεων στους φορείς του δημόσιου τομέα, και τις Κατευθυντήριες γραμμές 4/2022 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων για τον υπολογισμό διοικητικών προστίμων για τους σκοπούς του Κανονισμού 2016/679, οι οποίες εγκρίθηκαν στις 24/5/2023[11], καθώς και τα πραγματικά δεδομένα της εξεταζόμενης υπόθεσης και ιδίως τα εξής:

i) Η διαπιστωθείσα παράβαση του άρθρου 5 παρ. 1 του ΓΚΠΔ υπάγεται, σύμφωνα με τις διατάξεις του άρθρου 83 παρ. 5 εδ. β' ΓΚΠΔ, στην ανώτερη προβλεπόμενη κατηγορία του συστήματος διαβάθμισης διοικητικών προστίμων («σημαντικές» παραβάσεις με μέγιστο ύψος 20.000.000 ευρώ).

[11] Βλ. https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf (τελευταία πρόσβαση: 16/6/2023)

ii) Η δραστηριότητα του υπευθύνου επεξεργασίας έχει μεγάλο εύρος, αφού αφορά το σύνολο του επιβατικού κοινού των μέσων μαζικής μεταφοράς της Αθήνας,

iii) Η δραστηριότητα σχετίζεται με τις κύριες δραστηριότητες του υπευθύνου επεξεργασίας.

iv) Η επεξεργασία αφορά μεν κυρίως «απλά» προσωπικά δεδομένα, αλλά αφορά επίσης και δεδομένα ειδικών κατηγοριών, όπως αυτά που σχετίζονται με μετακινήσεις ΑΜΕΑ.

v) Ο υπεύθυνος επεξεργασίας επέδειξε δυσχέρεια στη συνεργασία με την Αρχή ως προς το σκέλος της τεκμηρίωσης του χρόνου τήρησης των δεδομένων (παραβίαση του άρθρου 5 παρ. 1 στοιχ. ε'), παραλείποντας να παράσχει τις πληροφορίες που του ζητήθηκαν.

vi) Δεν προκύπτει υλική βλάβη για τα υποκείμενα των δεδομένων.

vii) Ο ΟΑΣΑ προέβη σε κάποιες διορθωτικές ενέργειες μετά τον επιτόπιο έλεγχο, σε σχέση με τον προσδιορισμό του χρόνου τήρησης των δεδομένων (αφού προ του επιτόπιου ελέγχου δεν είχαν προσδιοριστεί καθόλου οι χρόνοι τήρησης των δεδομένων για τους διάφορους σκοπούς επεξεργασίας).

viii) Τα πιο πρόσφατα διαθέσιμα στο Διαδίκτυο[12] στοιχεία για τα οικονομικά έσοδα και τον κύκλο εργασιών του υπευθύνου επεξεργασίας για το 2021.

25. Η Αρχή κρίνει ότι, με βάση τις περιστάσεις που διαπιστώθηκαν, οι κυρώσεις που αναφέρονται στο διατακτικό της απόφασης είναι το αποτελεσματικό, αναλογικό και αποτρεπτικό μέτρο τόσο προς αποκατάσταση της συμμόρφωσης, όσο και για την τιμωρία της παράνομης συμπεριφοράς.

[12] Διαθέσιμα στο σύνδεσμο https://oasa.b-cdn.net/wp-content/uploads/2022/10/ΜΟΝΟΣΕΛΙΔΟ-ΟΑΣΑ-31-12-2021-ΔΣ-ΤΕΛΙΚΟ.pdf (τελευταία πρόσβαση: 16/6/2023)

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή, λαμβάνοντας υπόψη τα παραπάνω:

α) Επιβάλλει, με βάση το άρθρο 58 παρ. 2 εδαφ. θ' του ΓΚΠΔ, πρόστιμο στην «Οργανισμό Αστικών Συγκοινωνιών Α.Ε.» συνολικού ύψους 50.000 ευρώ, για την παραβίαση του άρθρου 5 παρ. 2 στοιχ. ε' του Κανονισμού (ΕΕ) 2016/679.

β) Απευθύνει, με βάση το άρθρο 58 παρ. 2 β' του Κανονισμού (ΕΕ) 2016/679, επίπληξη στην «Οργανισμό Αστικών Συγκοινωνιών Α.Ε.» για τις παραβιάσεις της διατάξεων του άρθρου 25 παρ. 1 και του άρθρου 35 παρ. 1 του Κανονισμού (ΕΕ) 2016/679.

γ) Δίνει εντολή συμμόρφωσης στην «Οργανισμό Αστικών Συγκοινωνιών Α.Ε.», σύμφωνα με το άρθρο 58 παρ. 2 δ΄ του ΓΚΠΔ, προκειμένου να προσδιορίσει και να τεκμηριώσει, εντός ενός (1) μηνός, όλους τους χρόνους τήρησης των δεδομένων για τους διάφορους σκοπούς επεξεργασίας του ΑΣΣΚ. Σε περίπτωση κατά την οποία, μετά τον εν λόγω προσδιορισμό του χρόνου τήρησης, προκύψει ότι τηρούνται ήδη δεδομένα προσωπικού χαρακτήρα καθ' υπέρβαση του χρόνου αυτού, τότε θα πρέπει αμελλητί είτε να διαγράψει είτε να καταστήσει ανώνυμα τα δεδομένα αυτά, τεκμηριώνοντας σχετικά και ενημερώνοντας και την Αρχή. Η σχετική ενημέρωση για τους χρόνους διατήρησης των δεδομένων, για τους διάφορους σκοπούς επεξεργασίας, θα πρέπει να παρέχεται και στα υποκείμενα των δεδομένων. Σε κάθε περίπτωση, για τον προσδιορισμό του χρόνου τήρησης των δεδομένων, ο ΟΑΣΑ θα πρέπει να εξετάσει αν το ενδεχόμενο ανωνυμοποίησης των δεδομένων επαναφόρτισης, επικύρωσης και ελέγχου κομίστρου (ήτοι διαγραφή του μοναδικού αριθμού της κάρτας, με διατήρηση των λοιπών πληροφοριών όπως κατηγορία δικαιούχου, σημεία και χρόνοι επικύρωσης κτλ.), σε σύντομο χρονικό διάστημα από τη δημιουργία τους, επηρεάζει δυσμενώς τους λοιπούς σκοπούς επεξεργασίας με σχετική τεκμηρίωση σε καταφατική περίπτωση.

δ) Δίνει εντολή συμμόρφωσης στην «Οργανισμό Αστικών Συγκοινωνιών Α.Ε.», σύμφωνα με το άρθρο 58 παρ. 2 δ΄ του ΓΚΠΔ, προκειμένου, εντός τριών (3) μηνών, να αναθεωρηθεί η εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα σύμφωνα με τα όσα διαλαμβάνονται στην παρούσα, καθώς επίσης και να υλοποιηθούν στο πλαίσιο αυτό όποια πρόσθετα μέτρα

κριθεί, εκ του αποτελέσματος της αναθεώρησης αυτής, ότι είναι αναγκαία για την αντιμετώπιση των διαφόρων κινδύνων, λαμβάνοντας υπόψη τα όσα διαλαμβάνονται στη Σκέψη 17 της παρούσας.

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