



**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ**

Αθήνα, 04-01-2019

Αριθ. Πρωτ.: Γ/ΕΞ/45/04-01-2019

Α Π Ο Φ Α Σ Η ΑΡ. 77/2018

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την 22-05-2018, σε συνέχεια της από 17-07-2017 τακτικής συνεδρίασής 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 Αντώνιος Συμβώνης, Σπυρίδων Βλαχόπουλος, ως εισηγητής, Κωνσταντίνος Λαμπρινουδάκης, επίσης ως εισηγητής, Χαράλαμπος Ανθόπουλος και Ελένη Μαρτσούκου, καθώς επίσης και το αναπληρωματικό μέλος της Αρχής Γεώργιος Νούσκαλης, σε αντικατάσταση του τακτικού μέλους Κωνσταντίνου Χριστοδούλου ο οποίος, εάν και εκλήθη νομίμως και εγγράφως, δεν προσήλθε λόγω κωλύματος. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, η Ε. Μαραγκού, δικηγόρος-νομική ελέγκτρια και οι Γ. Ρουσόπουλος και Κ. Λιμνιώτης, πληροφορικοί ελεγκτές, ως βοηθοί εισηγητών. Επίσης παρέστη, με εντολή Προέδρου, η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του Διοικητικού – Οικονομικού Τμήματος της Αρχής, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Υποβλήθηκε στην Αρχή το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/823/02-02-2017 ερώτημα του Συλλόγου Δικαστικών Υπαλλήλων Διοικητικών Δικαστηρίων Αθήνας, αναφορικά με το ζήτημα κατά πόσο είναι νόμιμη η υποχρεωτική και διαρκής χρήση για υπηρεσιακό σκοπό

των στοιχείων αυθεντικοποίησης που αποδίδονται σε φυσικά πρόσωπα για ιδιωτικό τους σκοπό – και, ειδικότερα για την χρήση από αυτά, ως φορολογουμένους, των ηλεκτρονικών υπηρεσιών του Υπουργείου Οικονομικών και της Ανεξάρτητης Αρχής Δημοσίων Εσόδων. Συγκεκριμένα, τα ως άνω αναφερόμενα στοιχεία πιστοποίησης ζητούνται υποχρεωτικώς για την πιστοποίηση των αρμοδίων υπαλλήλων για τη δέσμευση ηλεκτρονικών παραβόλων (e-παραβόλο), στο πλαίσιο της πιλοτικής εφαρμογής του μέτρου στο Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και ειδικότερα στο Διοικητικό Εφετείο Αθηνών. Στο ως άνω ερώτημά του ο Σύλλογος αναφέρει ότι δεν μπορούν να αξιολογηθούν οι κίνδυνοι που μπορεί να ενέχει η υποχρεωτική χρήση των προσωπικών διαπιστευτηρίων του συστήματος TAXISNET για υπηρεσιακούς σκοπούς.

Στο πλαίσιο εξέτασης της υπόθεσης, η Αρχή, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/823-1/4-4/2017 έγγραφό της, ζήτησε τις απόψεις των εμπλεκόμενων φορέων – ήτοι της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Διοικητικής Υποστήριξης του Υπουργείου Οικονομικών (εφεξής ΓΓΠΣ), της Ανεξάρτητης Αρχής Δημοσίων Εσόδων (εφεξής ΑΑΔΕ) και του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων (εφεξής ΥΔΔΑΔ).

Η ΑΑΔΕ απάντησε με το υπ' αριθμ. πρωτ. ΔΗΛΕΔ Β 1069020 ΕΞ 2017/5-5-2017 έγγραφό της (αρ. πρωτ. Αρχής Γ/ΕΙΣ/3743/11-05-2017). Σε αυτό αναφέρει ότι τα διαπιστευτήρια TAXISNET αποδίδονται σε φυσικά πρόσωπα με σκοπό τη χρήση εκ μέρους τους των πληροφοριακών συστημάτων της ΑΑΔΕ και των επιμέρους εφαρμογών αυτών. Περαιτέρω, αναφέρει ότι αποτελεί διεθνή πρακτική να αποδίδονται μοναδικά διαπιστευτήρια σε ένα φυσικό πρόσωπο και στη συνέχεια να του αποδίδονται ρόλοι και δικαιώματα στις διάφορες εφαρμογές. Τα διαπιστευτήρια αυτά είναι μοναδικά, είτε πρόκειται για ιδιωτικές υποθέσεις, είτε για υπηρεσιακές (οπότε και η αρμόδια υπηρεσία πρέπει να του αποδώσει αυτή τη δυνατότητα). Ο κάθε χρήστης επιλέγει κάθε φορά τον αντίστοιχο ρόλο με τον οποίο εισέρχεται στο σύστημα.

Η ΑΑΔΕ υποστηρίζει επίσης ότι η απόδοση πολλαπλών διαπιστευτηρίων ανά εφαρμογή, θα οδηγήσει σε σημαντικά προβλήματα τόσο για την υπηρεσία (π.χ. αύξηση διαχειριστικού κόστους, δυσκολία στην παρακολούθηση και έλεγχο ορθής χρήσης των εφαρμογών) όσο και στους χρήστες (π.χ. ανάγκη διατήρησης πολλαπλών διαπιστευτηρίων, πολλαπλή προσωπική παρουσία για την απόδοση των κωδικών). Τέλος, επισημαίνει ότι κατά τη χρήση της εφαρμογής του ηλεκτρονικού παραβόλου γίνεται κρυπτογράφηση της επικοινωνίας και έχουν ληφθεί κατάλληλα τεχνικά μέτρα ασφάλειας.

Η ΓΓΠΣ απάντησε με το υπ' αριθμ. πρωτ. Δ.Σ.Α.Ε. 4011392 ΕΞ 2017 έγγραφό της

(αρ. πρωτ. Αρχής Γ/ΕΙΣ/4538/09-06-2017). Σε αυτό αναφέρει ότι μέσω του μηχανισμού αυθεντικοποίησης του TAXISNET ακολουθείται ισχυρή διαδικασία απόδοσης ατομικών διαπιστευτηρίων σε φυσικά πρόσωπα, με τη χρήση των οποίων επιτυγχάνεται η ταυτοποίηση του φυσικού προσώπου που συνδέεται σε ένα Πληροφοριακό Σύστημα και εν συνεχεία προσδιορίζεται ο ρόλος του βάσει του τρόπου λειτουργίας του εκάστοτε Πληροφοριακού Συστήματος. Με βάση την ως άνω λογική ο υπάλληλος, εφόσον εξουσιοδοτηθεί (ήτοι εφόσον του αποδοθεί από το φορέα του ο συγκεκριμένος ρόλος) ενεργεί ως εκπρόσωπος του φορέα του. Τούτο αναφέρεται, όπως επισημαίνει η ΓΓΠΣ, ρητά στην σχετική Υ.Α. (ΠΟΛ. 1150 15/05/2014 ΦΕΚ 1357/Β'/2014 - Τροποποίηση της ΠΟΛ 1163). Επίσης η ΓΓΠΣ αναφέρει - όπως και η ΑΑΔΕ - ότι σε περίπτωση απόδοσης χωριστών διαπιστευτηρίων θα εμφανίζονταν προβλήματα διαχείρισης και ασφάλειας στα πληροφοριακά συστήματα και τους τελικούς χρήστες. Τέλος, η ΓΓΠΣ αναφέρει ότι η διαδικασία δέσμευσης των ηλεκτρονικών παραβόλων είναι ανεξάρτητη από άλλες διαδικασίες οικονομικής φύσης (όπως συναλλαγές με τράπεζες, έκδοση επιταγών κ.α.), αποτελεί «οριζόντια» διαδικασία και μπορεί να διεκπεραιωθεί από οποιονδήποτε υπάλληλο, ανεξαρτήτως θέσης, καθώς και ότι η εφαρμογή του ηλεκτρονικού παραβόλου δεν είναι πλέον σε πιλοτική αλλά σε παραγωγική λειτουργία.

Το ΥΔΔΑΔ απάντησε με το υπ' αριθμ. πρωτ. 36812/08-06-2017 έγγραφό του (αρ. πρωτ. Αρχής Γ/ΕΙΣ/4685/16-06-2017). Στο έγγραφο αυτό αναφέρει ότι η διαδικασία δέσμευσης ηλεκτρονικών παραβόλων γίνεται με βάση την προαναφερθείσα Υ.Α. και ότι ο εξουσιοδοτημένος χρήστης προβαίνει μόνο σε έλεγχο εγκυρότητας του παραβόλου και σε εκτυπώσεις ελέγχου. Μετά τον έλεγχο, το παράβολο δεσμεύεται ώστε να αποκλειστεί η εκ νέου χρήση του. Με βάση την υπάρχουσα νομοθεσία, οι δικαστικές αρχές οφείλουν να εξασφαλίζουν στον αιτούντα τη δυνατότητα καταβολής του παραβόλου, το οποίο προβλέπεται επί ποινή απαραδέκτου. Το Υπουργείο επισημαίνει, κατά λόγο αρμοδιότητας, ότι το ενδεχόμενο αποστολής χωριστών διαπιστευτηρίων ανά φυσικό πρόσωπο και εφαρμογή φαίνεται εκ πρώτης όψεως εφικτό, αλλά κρίνει ότι είναι δυσανάλογο ως προς το διαχειριστικό όγκο και τους πόρους που θα απαιτηθούν για τις χιλιάδες των χρηστών ανά τη χώρα, καθώς επίσης και αμφιβόλου προσδοκώμενου αποτελέσματος.

Ο Σύλλογος Δικαστικών Υπαλλήλων Διοικητικών Δικαστηρίων Αθήνας, η Γενική Γραμματεία Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών, το Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και η Ανεξάρτητη Αρχή Δημοσίων Εσόδων κλήθηκαν νομίμως, με τα υπ' αριθμ. πρωτ. Γ/ΕΞ/823-2/10-07-2017, Γ/ΕΞ/823-3/10-07-2017, Γ/ΕΞ/823-4/10-07-2017 και Γ/ΕΞ/823-5/10-07-2017 έγγραφα της Αρχής

αντίστοιχα, σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 17-07-2017 της Ολομέλειας της Αρχής, για να δώσουν περαιτέρω διευκρινίσεις και να εκθέσουν τις απόψεις τους επί των ανωτέρω. Στη συνεδρίαση, παρέστησαν νομίμως, ως εκπρόσωποι του Συλλόγου Δικαστικών Υπαλλήλων Διοικητικών Δικαστηρίων Αθήνας οι Α, πρόεδρος του συλλόγου και Β, μέλος, ως εκπρόσωποι της ΓΓΠΣ οι Γ, σύμβουλος του Γενικού Γραμματέα της ΓΓΠΣ, Δ, Προϊστάμενος της Διεύθυνσης Σχεδιασμού και Ανάπτυξης Εφαρμογών – Τμήμα Β΄ και Ε, υπάλληλος, ως εκπρόσωποι του ΥΔΔΑΔ οι ΣΤ΄, Προϊσταμένη Διεύθυνσης και Πρόεδρος στην Ομάδα Εργασίας του ΥΔΔΑΔ με αντικείμενο την υιοθέτηση του ηλεκτρονικού παραβόλου και Ζ, Προϊστάμενος Τμήματος και μέλος της ως άνω Ομάδας Εργασίας και ως εκπρόσωποι της ΑΑΔΕ οι Η, Προϊσταμένη της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης, Θ, Προϊστάμενος του Τμήματος Ε΄, Ι της Διεύθυνσης Εισπράξεων - Τμήμα Δ΄, ΙΑ, υπάλληλος του Τμήματος ΙΓ΄ και ΙΒ, υπάλληλος Γραφείου Ασφαλείας. Κατά την ακρόαση, οι ως άνω εκπρόσωποι εξέθεσαν προφορικά τις απόψεις τους και εξήτησαν και έλαβαν προθεσμία υποβολής υπομνήματος. Συναφώς δε, η ΓΓΠΣ και η ΑΑΔΕ κατέθεσαν εμπροθέσμως σχετικά υπομνήματα με αριθμ. πρωτ. ΓρΓΓΠ0049ΕΞ2017ΕΜΠ από 1-8-2017 ΔΗΔ/9415 (αριθμ. πρωτ. Αρχής: Γ/ΕΙΣ/5832/01-08-2017), και ΔΗΛΕΔ ΙΓ 1115214 ΕΞ 2017 από 28-7-2017 (αρ. πρωτ. Αρχής: Γ/ΕΙΣ/5776/31-07-2017), αντιστοίχως. Στα εν λόγω υπομνήματα σημειώνονται μεταξύ άλλων, τα ακόλουθα:

Η ΑΑΔΕ στο υπόμνημά της αναφέρει ότι με τη διάταξη του άρθρου 29 του ν. 3943/2011 προβλέφθηκε η δυνατότητα αντικατάστασης του έντυπου παραβόλου με το ηλεκτρονικό που δημιουργείται με τη χορήγηση μοναδικού ψηφιακού αριθμού, ο οποίος πιστοποιείται και ελέγχεται από το κεντρικό Πληροφοριακό Σύστημα του Υπουργείου Οικονομικών. Οι όροι και οι διαδικασίες είσπραξης – επιστροφής του ηλεκτρονικού παραβόλου προβλέπονται με την Απόφαση ΠΟΛ 1163/2013 (Β΄ 1675) του Υπουργείου Οικονομικών, όπως τροποποιήθηκε και ισχύει. Ειδικότερα, στο άρθρο 4 της ως άνω ΠΟΛ, όπως αντικαταστάθηκε με την παρ. 1 της ΠΟΛ 1150/2014 (Β΄ 1357), περιγράφεται η διαδικασία, την οποία πρέπει να ακολουθεί μία δημόσια υπηρεσία προκειμένου να αποδεχτεί και να ελέγξει την εγκυρότητα του ηλεκτρονικού παραβόλου. Στη διαδικασία αυτή περιγράφεται¹ μεταξύ άλλων ότι για την ταυτοποίηση των υπαλλήλων που αποδέχονται/δεσμεύουν ηλεκτρονικά παράβολα για λογαριασμό του Δημόσιου Φορέα χρησιμοποιούνται τα προσωπικά διαπιστευτήρια –ήτοι όνομα χρήστη («username») και συνθηματικό («password»)– τα οποία διαθέτει ο υπάλληλος για το σύστημα TAXISNET.

¹ Το ακριβές περιεχόμενο της εν λόγω διάταξης παρατίθεται στη συνέχεια, στο Σκεπτικό της παρούσας

Κατ' εφαρμογή των ανωτέρω, η Δ/ση Σχεδιασμού και Ανάπτυξης Εφαρμογών της ΓΓΠΣ και η Δ/ση Ηλεκτρονικής Διακυβέρνησης της ΑΑΔΕ ανέπτυξαν και έθεσαν σε λειτουργία την εφαρμογή του ηλεκτρονικού παραβόλου («e-παράβολο»). Προς τούτο ακολουθήθηκε η διεθνής πρακτική, σύμφωνα με την οποία σε κάθε χρήστη αποδίδονται μοναδικά διαπιστευτήρια (όνομα χρήστη και συνθηματικό) και, ακολούθως, του αποδίδονται ρόλοι βάσει των οποίων παρέχεται πρόσβαση σε ορισμένα ή σε όλα τα τμήματα του Πληροφοριακού Συστήματος – ενδεχομένως με διαφορετικά δικαιώματα. Κατά την ίδια λογική, το ολοκληρωμένο Πληροφοριακό Σύστημα TAXISNET του Υπουργείου Οικονομικών, το οποίο διαχειρίζεται η ΑΑΔΕ, έχει σχεδιαστεί κατά τρόπο τέτοιο ώστε οι χρήστες του να αποκτούν μοναδικά διαπιστευτήρια τα οποία χρησιμοποιούν είτε για ιδιωτικές υποθέσεις είτε για υπηρεσιακές, επιλέγοντας κάθε φορά τον αντίστοιχο ρόλο. Για να είναι δυνατή η χρήση των διαπιστευτηρίων για υπηρεσιακούς σκοπούς, θα πρέπει η Υπηρεσία του υπαλλήλου-χρήστη να του αποδώσει αυτή τη δυνατότητα, η δε χρήση για υπηρεσιακούς σκοπούς είναι διακριτή, με σχετική καταγραφή.

Στην προκειμένη περίπτωση, κατόπιν σχετικού αιτήματος, η Δ/ση Σχεδιασμού και Ανάπτυξης Εφαρμογών της ΓΓΠΣ και η Δ/ση Ηλεκτρονικής Διακυβέρνησης της ΑΑΔΕ έχουν αποδώσει στο ΥΔΑΔΔ πρόσθετο ρόλο και δικαιώματα χρήσης της εφαρμογής e-παράβολο. Το ΥΔΑΔΔ έχει ακολουθήσει την προβλεπόμενη κατά τα ανωτέρω διαδικασία και εξουσιοδότησε υπαλλήλους του, οι οποίοι είναι πιστοποιημένοι χρήστες του TAXISNET, ως εκπροσώπους του, προκειμένου να κάνουν χρήση της πλατφόρμας του συστήματος «e-παράβολο» για λογαριασμό του, για την εξυπηρέτηση των συναλλασσομένων. Ο υπάλληλος-χρήστης, μετά την είσοδό του στην εφαρμογή, επιλέγει από σχετικού μενού αν θα ενεργήσει για τον εαυτό του ή ως εκπρόσωπος Δημόσιου Φορέα. Η ταυτοποίηση των χρηστών σε επίπεδο ατόμου είναι αναγκαία ώστε να είναι δυνατή η καταγραφή κινήσεων και η ανάκτησή τους μελλοντικά, σε περίπτωση ερευνών περιστατικών ασφαλείας ή άλλης παραβατικής συμπεριφοράς. Κατά τη χρήση της εφαρμογής «e-παράβολο» δεν υφίσταται επεξεργασία ούτε των διαπιστευτηρίων του TAXISNET ούτε των προσωπικών δεδομένων του υπαλλήλου-χρήστη που είναι καταχωρημένα στο TAXISNET.

Περαιτέρω, η ΑΑΔΕ εκθέτει στο εν λόγω υπόμνημά της ότι ο υπάλληλος-χρήστης της εφαρμογής οφείλει να μεριμνά για την ορθή και ασφαλή χρήση των διαπιστευτηρίων του στο TAXISNET, όπως θα έπραττε και για οποιαδήποτε άλλα διαπιστευτήρια τυχόν είχε για την πρόσβαση στην ίδια ή σε άλλη εφαρμογή. Επιπλέον, η ΑΑΔΕ εξετάζει την υλοποίηση νέων μηχανισμών αυθεντικοποίησης του χρήστη στο πλαίσιο ενίσχυσης της ασφάλειας, όπως η αυθεντικοποίηση δύο επιπέδων (two-factor authentication). Ωστόσο, η χρήση ενός τέτοιου

μηχανισμού αφενός δεν καλύπτει τις ανησυχίες των χρηστών σχετικά με τον πιθανολογούμενο κίνδυνο ως προς τα προσωπικά τους δεδομένα και αφετέρου επιβαρύνει τη διαδικασία. Η εναλλακτική της απόδοσης πολλαπλών διαπιστευτηρίων ανά εφαρμογή (λαμβάνοντας υπόψη ότι στο μέλλον θα λειτουργήσουν και άλλες εφαρμογές, πέραν της «e-παράβολο») θα οδηγήσει σε αύξηση διαχειριστικού κόστους, σε δυσκολία στην παρακολούθηση και έλεγχο ορθής χρήσης των εφαρμογών, ενώ θα δυσχεράνει και τους ίδιους τους χρήστες (ανάγκη διατήρησης πολλαπλών διαπιστευτηρίων, πολλαπλή προσωπική παρουσία για την απόκτηση κωδικών κτλ.). Επιπλέον, η υλοποίηση ενός παράλληλου μητρώου υπηρεσιακών χρηστών απαιτεί σημαντικές αλλαγές στην κεντρική δομή του TAXISNET αλλά και σε επιμέρους εφαρμογές.

Τέλος, η ΑΑΔΕ αναφέρει ότι εξετάζει επιπροσθέτως την αλλαγή του τρόπου εισόδου των χρηστών σε κάποιες ηλεκτρονικές της υπηρεσίες, του ονομαζόμενου «single sign-on», που συνίσταται στη δυνατότητα διακριτής εισόδου σε μία (ή σε κάθε μία) από τις προσφερόμενες υπηρεσίες μιας διαδικτυακής πύλης. Ειδικότερα, με το νέο τρόπο («non single sign-on»), ο χρήστης θα εισέρχεται στην υπηρεσία που επιθυμεί (εν προκειμένω, στην εφαρμογή «e-παράβολο») με χρήση των διαπιστευτηρίων του στο TAXISNET, χωρίς δυνατότητα μεταφοράς του σε άλλη ηλεκτρονική υπηρεσία (όπως, π.χ., υποβολής ηλεκτρονικών δηλώσεων) παρά μόνο με την επαναχρησιμοποίηση των διαπιστευτηρίων. Οι εργασίες για τη μετατροπή των «single sign-on» υπηρεσιών σε υπηρεσίες τύπου «non single sign-on» θα απαιτήσουν, κατά τους ισχυρισμούς της ΑΑΔΕ, συνέργειες και, ενδεχομένως, αρκετό χρόνο.

Η ΓΓΠΣ, στο ως άνω υπόμνημά της, αναφέρει ότι για την εφαρμογή «e-παράβολο» υπάρχουν δύο τρόποι αυθεντικοποίησης των χρηστών και, συγκεκριμένα, είτε με τη λειτουργία των διαπιστευτηρίων του TAXISNET είτε με τη λειτουργία διαδικτυακών υπηρεσιών (web services) για την εκπλήρωση των επιχειρησιακών τους στόχων. Στην πρώτη περίπτωση, δεν απαιτείται η ανάπτυξη και συντήρηση από τους φορείς οποιουδήποτε Πληροφοριακού Συστήματος, ενώ στη δεύτερη περίπτωση απαιτούνται πρόσθετοι οικονομικοί πόροι και τεχνογνωσία. Η ΓΓΠΣ περιγράφει στο υπόμνημά της τις δύο διαδικασίες: ως προς την περίπτωση των διαπιστευτηρίων του TAXISNET περιγράφεται η ίδια διαδικασία με αυτή που εκτέθηκε και στο υπόμνημα της ΑΑΔΕ, ενώ ως προς τη χρήση των διαδικτυακών υπηρεσιών αναφέρει ότι χρησιμοποιείται το Πληροφοριακό Σύστημα του φορέα για τη διαχείριση ηλεκτρονικών παραβόλων, μέσω του οποίου ο κάθε φορέας αποδίδει διαφορετικούς κωδικούς στους υπαλλήλους του, τους οποίους και διαχειρίζεται. Ενδεικτικά, με διαδικτυακές υπηρεσίες λειτουργούν η Ελληνική Αστυνομία, το Υπουργείο Εσωτερικών και το Υπουργείο Αγροτικής Ανάπτυξης. Ως προς την ασφάλεια του Πληροφοριακού

Συστήματος «e-παράβολο» πραγματοποιείται λεπτομερής καταγραφή των ενεργειών (αναζήτηση, δέσμευση και επιστροφή των παραβόλων) του υπαλλήλου, ενώ επιπλέον υπάρχει διαδικασία ελέγχου από τους φορείς για τα παράβολα, τα οποία δεσμεύουν ή επιστρέφουν οι εξουσιοδοτημένοι χρήστες/υπάλληλοί τους. Η ΓΓΠΣ αναφέρει επίσης ότι η ορθή χρήση των κωδικών και η προστασία τους είναι σε κάθε περίπτωση ευθύνη του κάθε πολίτη ή/και υπαλλήλου, και ότι η λειτουργία της εν λόγω εφαρμογής πραγματοποιείται ήδη επί τρία (3) χρόνια, χωρίς να έχουν καταγραφεί φαινόμενα κακής χρήσης. Τέλος, η ΓΓΠΣ αναφέρει ότι προσανατολίζεται σε υιοθέτηση αυθεντικοποίησης δύο επιπέδων που δεν θα επηρεάσουν την επιχειρησιακή λειτουργία των φορέων και δεν θα επιφέρουν πρόσθετα κόστη.

Η Αρχή, μετά από εξέταση όλων των στοιχείων του φακέλου και των απόψεων που αναπτύχθηκαν στην από 17-07-2017 συνεδρίαση, αφού άκουσε τους εισηγητές και τις διευκρινίσεις των βοηθών εισηγητών, οι οποίοι στην συνέχεια αποχώρησαν πριν από τη διάσκεψη και τη λήψη απόφασης, και κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

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

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

2. Ως υπεύθυνος επεξεργασίας ορίζεται, στο άρθρο 2 στοιχ. ζ του ίδιου ν. 2472/1997,

όποιος «...καθορίζει το σκοπό και τον τρόπο της επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και τρόπος καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο». Η Οδηγία 95/46/EK περιέχει αντίστοιχο ορισμό στη διάταξη του άρθρου 2 στοιχ. δ', στην οποία διευκρινίζεται περαιτέρω ότι ο υπεύθυνος επεξεργασίας καθορίζει από μόνος του ή από κοινού με άλλους το σκοπό και τον τρόπο της επεξεργασίας, προκειμένου να καλυφθεί η πολυπλοκότητα των εννόμων σχέσεων, των συναλλακτικών και τεχνολογικών αναγκών, η οποία μπορεί να οδηγήσει σε περισσότερους υπευθύνους επεξεργασίας για την ίδια ή διαφορετική επιμέρους εργασία στο ευρύτερο πλαίσιο της επεξεργασίας των προσωπικών δεδομένων κατά την έννοια του άρθρου 2 στοιχ. δ' ν. 2472/1997. Συγκεκριμένα στην ανωτέρω διάταξη της Οδηγίας ορίζεται ως υπεύθυνος επεξεργασίας «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα». Παρά το ότι στην αντίστοιχη διάταξη του εθνικού νόμου παραλείπεται η αναφορά σε από κοινού καθορισμό των στόχων και του τρόπου επεξεργασίας, δεν αποκλείεται, κατά την έννοια της διάταξης αυτής, η αναγνώριση περισσότερων υπευθύνων για την ίδια επεξεργασία, ούτε άλλωστε θα ήταν νομικώς επιτρεπτό να αποκλειστεί κατά παρέκκλιση από τον ορισμό της Οδηγίας.

Εξάλλου, το υποκειμενικό πεδίο εφαρμογής σε σχέση με το δημόσιο τομέα της έννοιας του υπευθύνου επεξεργασίας, η οποία αποτελεί αυτόνομη έννοια του ενωσιακού δικαίου, και, ειδικότερα, σε σχέση με το περιεχόμενο των όρων δημόσια αρχή, και δημόσια υπηρεσία, συναρτάται με τη διοικητική οργάνωση των εθνικών εννόμων τάξεων. Στη έννοια δε της δημόσιας αρχής, κατά τη διάταξη του άρθρου 2 στοιχ. δ' της Οδηγίας 95/46/EK και της αντίστοιχης διάταξης άρθρου 2 στοιχ. ζ ν. 2472/1997, εμπίπτουν και οι υπηρεσίες, οι οποίες χαρακτηρίζονται από τη νομοθεσία ως ανεξάρτητες αρχές, όπως η ΑΑΔΕ. Βασικό είναι το λειτουργικό κριτήριο, δηλαδή υπεύθυνος επεξεργασίας είναι αυτός που καθορίζει το σκοπό ή/και τα ουσιώδη, τουλάχιστον, στοιχεία του τρόπου της επεξεργασίας (πρβλ. για την έννοια του υπευθύνου και εκτελούντος την επεξεργασία τη Γνώμη 1/2010 της Ο.Ε. του Άρθρου 29, στην οποία και αναφέρεται μεταξύ άλλων ότι ο καθορισμός των στόχων και του τρόπου ισοδυναμεί με τον καθορισμό, αντίστοιχα, του «γιατί» και του «πώς» ορισμένων δραστηριοτήτων επεξεργασίας). Στη Δημόσια Διοίκηση το λειτουργικό κριτήριο συνάπτεται κατ' αρχήν με τις αρμοδιότητες συγκεκριμένης αρχής, υπηρεσίας ή νομικού προσώπου δημοσίου δικαίου, οι οποίες, επιπλέον, θα πρέπει στην πράξη να ασκούνται από τους φορείς

τους. Συνεπώς, η επεξεργασία προσωπικών δεδομένων από δημόσια υπηρεσία ή Ανεξάρτητη Αρχή πρέπει να λειτουργεί και αναπτύσσει τις συνέπειές της στο πλαίσιο του κράτους δικαίου και της αρχής της νομιμότητας. Όπως παγίως γίνεται δεκτό, σύμφωνα με την αρχή της νομιμότητας, που λειτουργεί ως περιοριστικό όριο της διοικητικής δράσης, η διοικητική ενέργεια πρέπει να είναι σύμφωνη προς τον κανόνα δικαίου που διέπει τη δράση της Διοίκησης.

Περαιτέρω,, ως εκτελών την επεξεργασία ορίζεται στο νόμο (άρθρο 2 στοιχ. η) ν. 2472/1997) «οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός».

3. Στη συγκεκριμένη περίπτωση, η διαδικασία για το ηλεκτρονικό παράβολο περιγράφεται στην ΠΟΛ 1150/2014. Συγκεκριμένα, με το αρ. 1 αυτής αντικαθίσταται το άρθρο 4 της ΠΟΛ. 1163/03-07-2013 (ΦΕΚ 1675 Β΄) ως εξής:

«Η κατάθεση του e-Παραβόλου από τον ενδιαφερόμενο προς την αρμόδια Υπηρεσία πραγματοποιείται όπως κατά περίπτωση ορίζεται από αυτήν την Υπηρεσία. Προκειμένου η Υπηρεσία να αποδεχθεί και να ελέγξει την εγκυρότητα του e-Παραβόλου ακολουθείται η παρακάτω διαδικασία:

Ο Δημόσιος Φορέας, αφού πρωτίστως έχει καθορίσει τα είδη των παραβόλων που αποδέχεται, λαμβάνει από το Υπουργείο Οικονομικών, κατόπιν σχετικού του αιτήματος προς τη «Διεύθυνση Σχεδιασμού & Ανάπτυξης Εφαρμογών της Γ.Γ.Π.Σ.» και την «Διεύθυνση Ηλεκτρονικής Διακυβέρνησης (e-εφαρμογές)» της Γενικής Γραμματείας Δημοσίων Εσόδων, κωδικό πρόσβασης στις ηλεκτρονικές υπηρεσίες Taxisnet (σύμφωνα με τα οριζόμενα στην Α.Υ.Ο. ΠΟΛ 1178/07-12-2010, ΑΔΑ:41ΦΜΗ-ΤΛ (ΦΕΚ 1916/Β΄/09-12-10) και δικαίωμα χρήσης της εφαρμογής «e-Παράβολο».

Ακολούθως, ο Δημόσιος Φορέας ορίζει τουλάχιστον δύο υπαλλήλους ως υπεύθυνους Διαχείρισης της εφαρμογής. Ο υπεύθυνος Διαχείρισης της εφαρμογής έχει την αρμοδιότητα να εξουσιοδοτήσει τους υπαλλήλους που αποδέχονται/δεσμεύουν τα e-Παράβολα για λογαριασμό του Δημόσιου Φορέα. Για την ταυτοποίηση των υπαλλήλων που αποδέχονται/δεσμεύουν e-Παράβολα θα χρησιμοποιηθούν οι κωδικοί πρόσβασης (Username και password) που χρησιμοποιεί ο υπάλληλος στο Taxisnet και συνεπώς δεν απαιτείται νέα πιστοποίηση για τους ήδη πιστοποιημένους χρήστες σε οποιαδήποτε ηλεκτρονική υπηρεσία του Taxisnet. Ο υπάλληλος της Υπηρεσίας που κατατίθεται το e-Παράβολο για να το αποδεχθεί/δεσμεύσει συνδέεται με την εφαρμογή κάνοντας την επιλογή του ρόλου ως εκπρόσωπος φορέα, αναζητά το e-Παράβολο και ελέγχει την εγκυρότητά του. Για τον έλεγχο εγκυρότητας, η εφαρμογή του e-

*Παραβόλου διαθέτει οθόνη αναζήτησης, προβολής και διαχείρισης των e-Παραβόλων καθώς και εκτυπώσεις ελέγχου. Μετά τον σχετικό έλεγχο η Υπηρεσία αποδέχεται το e-Παράβολο και αυτό δεσμεύεται ώστε να αποκλειστεί η εκ νέου χρήση του. **Εναλλακτικά, η σύνδεση της Υπηρεσίας μπορεί να γίνει με την ανάπτυξη διαδικτυακής εφαρμογής από το Δημόσιο Φορέα η οποία θα επικοινωνεί με την ηλεκτρονική εφαρμογή του e-Παραβόλου.»***

Η εν λόγω Υ.Α. έχει εκδοθεί με βάση το άρθρο 29 παρ. 3 του ν. 3943/2011 που αναφέρει «Όπου, κατά τις ισχύουσες διατάξεις, απαιτείται κατάθεση παραβόλου σε έντυπη μορφή, δύναται να αντικατασταθεί η έντυπη μορφή με ηλεκτρονικό παράβολο. Το ηλεκτρονικό παράβολο δημιουργείται με τη χορήγηση μοναδικού ψηφιακού κωδικού, ο οποίος πιστοποιείται και ελέγχεται από κεντρικό πληροφοριακό σύστημα. Η διάθεση των ηλεκτρονικών παραβόλων δύναται να πραγματοποιείται με χρήση οποιουδήποτε καθιερωμένου στις συναλλαγές τρόπου πληρωμής. **Με απόφαση του Υπουργού Οικονομικών καθορίζονται οι αρμοδιότητες, οι διαδικασίες, οι λεπτομέρειες και ό, τι άλλο απαιτείται για την εφαρμογή του ηλεκτρονικού παραβόλου.»**

4. Σύμφωνα με το άρθρο 10 παρ. 1 του ν. 2472/1997, η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Στην παράγραφο 2 του ίδιου άρθρου ορίζεται ότι για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Περαιτέρω, στην παρ. 3 του ίδιου άρθρου ορίζεται ότι ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.

5. Ως προς τη συγκεκριμένη επεξεργασία, η οποία αφορά δεδομένα δικαστικών υπαλλήλων, που από διοικητική άποψη υπάγονται στο Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, το οποίο επέλεξε, κατ' εφαρμογή της ανωτέρω ΠΟΛ 1150/2014, να αξιοποιήσει τον μηχανισμό αυθεντικοποίησης του TAXISNET και όχι την ανάπτυξη διαδικτυακής εφαρμογής η οποία θα επικοινωνεί με την ηλεκτρονική εφαρμογή του e-Παραβόλου, το Υπουργείο αυτό είναι υπεύθυνος επεξεργασίας. Ωστόσο, δεδομένου ότι για τον εν λόγω μηχανισμό αυθεντικοποίησης, ο οποίος πρωτίστως αναπτύχθηκε για φορολογικούς και λοιπούς σκοπούς του Υπουργείου Οικονομικών, αρμόδιος φορέας είναι η

ΑΑΔΕ, η οποία και καθορίζει πλήρως τον τρόπο και τα μέσα με τα οποία θα επιτυγχάνεται ο επιδιωκόμενος σκοπός της αυθεντικοποίησης των χρηστών, πρέπει να θεωρηθεί ότι η ΑΑΔΕ αποτελεί από κοινού υπεύθυνο για την εν λόγω επεξεργασία. Τέλος, η ΓΠΠΣ, η οποία αποτελεί το φορέα υλοποίησης και υποστήριξης του εν λόγω μηχανισμού αυθεντικοποίησης αποτελεί τον εκτελούντα την επεξεργασία.

6. Στην προκειμένη περίπτωση, τίθεται προεχόντως το ζήτημα αν είναι νόμιμη η υποχρεωτική χρήση του συγκεκριμένου μηχανισμού αυθεντικοποίησης των χρηστών που έχουν και την ιδιότητα του υπαλλήλου (ή λειτουργού) του Δημοσίου – ειδικότερα, του μηχανισμού αυθεντικοποίησης του συστήματος TAXISNET – για σκοπούς που εντάσσονται στο πλαίσιο της δραστηριότητάς τους ως εργαζομένων, με δεδομένο ότι ο εν λόγω μηχανισμός αναπτύχθηκε και χρησιμοποιείται, επίσης υποχρεωτικά, για τους προσωπικούς τους σκοπούς (ιδιωτικούς) σκοπούς, που αφορούν το πλαίσιο των δραστηριοτήτων τους ως πολιτών (διοικουμένων).

Ως προς τη χρήση του εν λόγω μηχανισμού αυθεντικοποίησης, πρέπει να αναγνωριστούν γενικότερα δύο διακριτές περιπτώσεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Η πρώτη αφορά τη σχέση του φυσικού προσώπου (πολίτη), ως διοικουμένου, έναντι του Κράτους. Στην περίπτωση αυτή, αποδίδονται διαπιστευτήρια (όνομα χρήστη και συνθηματικό) στους διοικουμένους (εδώ φυσικά πρόσωπα), μέσω των οποίων συνδέονται στο πληροφοριακό σύστημα TAXISNET, κυρίως για τη διεκπεραίωση των υποχρεώσεών τους έναντι των Δημοσίων Οικονομικών Υπηρεσιών. Τα διαπιστευτήρια αυτά αποδίδονται με συγκεκριμένη διαδικασία, στο πλαίσιο της οποίας απαιτείται, για την παραλαβή τους, φυσική παρουσία του κάθε προσώπου στην αρμόδια Οικονομική Υπηρεσία. Δεδομένου, μάλιστα, ότι η εν λόγω διαδικασία είναι η πλέον ευρέως διαδομένη για τη χορήγηση ατομικών διαπιστευτηρίων, έχει χρησιμοποιηθεί και για άλλους σκοπούς ταυτοποίησης ενός φυσικού προσώπου έναντι δημόσιας αρχής (π.χ. ΕΚΔΔΑ, ΟΓΑ, αναζήτηση ενημερότητας κλπ.) και παρέχεται από τη ΓΠΠΣ σε διάφορους φορείς ως διαδικτυακή υπηρεσία (web service). Και ως προς αυτές τις υπηρεσίες ωστόσο, υφίσταται η σχέση πολίτη (διοικουμένου) με το Κράτος και, συνεπώς, κάθε τέτοιος νέος σκοπός επεξεργασίας (αυτός της Υπηρεσίας που χρησιμοποιεί το web service) δύναται να χαρακτηριστεί κατ' αρχήν ως συναφής με τον αρχικό σκοπό επεξεργασίας.

Η δεύτερη περίπτωση –στην οποία εμπίπτει η υπό εξέταση υπόθεση– αφορά τη σχέση του φυσικού προσώπου με το Κράτος ως υπαλλήλου (ή λειτουργού) του Δημοσίου φορέα. Ουσιαστικά, στην περίπτωση αυτή το Κράτος υποχρεώνει το φυσικό πρόσωπο που έχει την ιδιότητα του πολίτη –ενώ ταυτόχρονα είναι και υπάλληλος Φορέα του– να χρησιμοποιεί τα

διαπιστευτήρια που του έχουν χορηγηθεί για ιδιωτικό/προσωπικό σκοπό, ως διοικουμένου, προκειμένου να διεκπεραιώνει διαδικασίες που αφορούν αμιγώς τα υπηρεσιακά του καθήκοντα². Κατά συνέπεια, τα φυσικά πρόσωπα (υπάλληλοι) υποχρεώνονται - χωρίς να έχουν άλλη επιλογή - να χρησιμοποιήσουν (εισάγουν) τα ατομικά τους διαπιστευτήρια μέσω της υποδομής του φορέα απασχόλησής τους (όχι μόνο της ΓΓΠΣ/ΑΑΔΕ, αλλά στην προκειμένη περίπτωση του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων). Με τον τρόπο αυτό, η ασφαλής χρήση των διαπιστευτηρίων τους κατά τη σύνδεσή τους στα συστήματα δεν εξαρτάται αποκλειστικά από αυτούς, αλλά και από τα μέτρα ασφάλειας τα οποία λαμβάνει ο φορέας τους. Περαιτέρω, για τη χρήση αυτή των διαπιστευτηρίων του TAXISnet εντός των εγκαταστάσεων του φορέα από υπάλληλο αυτού, για υπηρεσιακούς σκοπούς, δεν παρέχεται βεβαιότητα ότι εξασφαλίζονται συνθήκες ώστε ο χρήστης (υπάλληλος) να έχει τη δυνατότητα να διασφαλίσει απόλυτα τη μυστικότητα των διαπιστευτηρίων, αφού είναι πιθανό στο χώρο εργασίας του να υπάρχουν και άλλα πρόσωπα, σε αντίθεση με την περίπτωση της χρήσης των εν λόγω κωδικών από τον προσωπικό του χώρο.

7. Βάσει των ανωτέρω, ανακύπτει το ζήτημα αν με την εν λόγω επεξεργασία θίγεται το συνταγματικό δικαίωμα του πληροφοριακού αυτοκαθορισμού (άρθρο 9Α του Συντάγματος). Η απαίτηση από το Κράτος να χρησιμοποιούνται οι συγκεκριμένοι κωδικοί/διαπιστευτήρια, οι οποίοι έχουν δοθεί στους πολίτες/διοικουμένους προκειμένου να συνδέονται στο πληροφοριακό σύστημα TAXISNET, κυρίως για τη διεκπεραίωση των υποχρεώσεών τους έναντι των Δημοσίων Οικονομικών Υπηρεσιών, για έτερο σκοπό, ο οποίος αντιστοιχεί σε διαφορετικό και εμφανώς διακριτό ρόλο και ιδιότητα των πολιτών, δηλαδή αυτή του υπαλλήλου, η οποία σαφώς διαχωρίζεται από την ατομική-ιδιωτική ζωή, δίχως αυτό να αποτελεί απόφαση ή και επιλογή του πολίτη, συνιστά περιορισμό του προαναφερόμενου δικαιώματος, θεμελιώδες στοιχείο του οποίου αποτελεί και η επεξεργασία των προσωπικών δεδομένων για προκαθορισμένο και συγκεκριμένο σκοπό.

Κατά συνέπεια, η Αρχή κρίνει ομόφωνα ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα την οποία συνεπάγεται η υποχρεωτική χρήση των διαπιστευτηρίων για δύο κατηγορίες σκοπών που δεν είναι συμβατές, πλήττει το δικαίωμα του πληροφοριακού

² Πρέπει να σημειωθεί ότι και σε άλλες περιπτώσεις ο μηχανισμός αυθεντικοποίησης του TAXISNET έχει χρησιμοποιηθεί για άλλον, πέραν του αρχικού, σκοπό - και, μάλιστα, για υπηρεσιακό σκοπό, όπως στην περίπτωση της απογραφής Δημοσίων Υπαλλήλων βάσει του ν. ν. 3845/2010 ή στις περιπτώσεις που σημειώνονται στο σκεπτικό της παρούσας. Καίτοι υπάρχει συνάφεια των διαφόρων αυτών περιπτώσεων, κάθε μία εξ αυτών φέρει τα δικά της χαρακτηριστικά -όπως, π.χ., κάθε φορά άλλος υπηρεσιακός σκοπός- και, συνεπώς, κάθε μία εξ αυτών πρέπει, κατ' αρχήν, να εξετάζεται με βάση τα συγκεκριμένα πραγματικά και νομικά δεδομένα.

αυτοκαθορισμού και, ως εκ τούτου, έρχεται σε αντίθεση με τις ουσιαστικές προϋποθέσεις επεξεργασίας προσωπικών δεδομένων κατά τον εφαρμοστέο στην παρούσα υπόθεση ν. 2472/1997 (αρχή του σκοπού – άρθρο 4 παρ. 1 στοιχ. α΄).

8. Επισημαίνεται ότι στο παρελθόν η Αρχή είχε εξετάσει εν μέρει παρόμοιο ζήτημα, σε περιπτώσεις κατά τις οποίες γίνεται χρήση από υπαλλήλους δημόσιου φορέα των συγκεκριμένων ατομικών τους στοιχείων αυθεντικοποίησης (κωδικοί TAXISNET) για υπηρεσιακούς σκοπούς, τόσο με τη γνωμοδότηση 5/2013 (υπ' αριθ. πρωτ. Γ/ΕΞ/5668-2/20-09-2013) όσο και με τη απόφαση χορήγησης αδείας στον Οργανισμό Γεωργικών Ασφαλίσεων (υπ' αριθμ. πρωτ. ΓΝ/ΕΞ/303-1/31-03-2014). Και στις δύο περιπτώσεις αυτές η Αρχή –καίτοι είχε εξετάσει το ζήτημα της υποχρεωτικής αξιοποίησης των κωδικών TAXISnet για υπηρεσιακούς σκοπούς μόνο από τη σκοπιά της ασφάλειας της επεξεργασίας– είχε εκφράσει επιφυλάξεις και, συγκεκριμένα, έχει κρίνει ότι η αυθεντικοποίηση ενός υπαλλήλου μόνο με τα προσωπικά του στοιχεία (όνομα χρήστη και κωδικό) για το TAXISNET δεν είναι επαρκής, με τις εξής σκέψεις:

«Ο περιγραφόμενος μηχανισμός αυθεντικοποίησης των χρηστών του συστήματος βασίζεται στη χρήση των κωδικών πρόσβασης που οι ίδιοι χρησιμοποιούν για τις υπηρεσίες του Υπουργείου Οικονομικών (κωδικοί TAXISnet), χωρίς να περιγράφεται συμπληρωματικός μηχανισμός αυθεντικοποίησής τους, όπως για παράδειγμα βάσει διαδικτυακής (IP) διεύθυνσης ή βάσει ψηφιακού πιστοποιητικού. Ως εκ τούτου, ο ανωτέρω μηχανισμός, όπως περιγράφεται, είναι προβληματικός, διότι η επιλογή συνθηματικού είναι ιδιαίτερα κρίσιμη για την ασφάλεια του συστήματος και, ως εκ τούτου, η χρήση κωδικού πρόσβασης που ήδη χρησιμοποιείται από τους ίδιους χρήστες στο Διαδίκτυο για άλλους σκοπούς, και μάλιστα και από σταθμούς εργασίας εκτός των χώρων εργασίας τους, πρέπει να αποφεύγεται.»

«Κατά την σύνδεση των αρμόδιων υπαλλήλων του υπευθύνου επεξεργασίας στο σχετικό πληροφοριακό σύστημα, θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί αυθεντικοποίησής τους: εφόσον η αυθεντικοποίηση βασίζεται αποκλειστικά σε χρήση συνθηματικού, αυτό θα πρέπει να είναι μοναδικό για κάθε χρήστη και να μην χρησιμοποιείται το ίδιο συνθηματικό από τον ίδιο χρήστη σε άλλες εφαρμογές. Ως εκ τούτου, δεν θα πρέπει να επιλεγεί ως μοναδικός μηχανισμός αυθεντικοποίησης η χρήση κωδικών πρόσβασης που οι ίδιοι χρησιμοποιούν για τις υπηρεσίες του Υπουργείου Οικονομικών (κωδικοί TAXISnet).»

Εξάλλου, πέραν αυτού, ακόμα και αν γίνει δεκτό ότι το Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων λαμβάνει –ως οφείλει άλλωστε, βάσει του άρθρου 10 του ν. 2472/1997– τα απολύτως απαραίτητα μέτρα (οργανωτικά, τεχνικά και μέτρα φυσικής ασφάλειας) για την ασφάλεια της επεξεργασίας και ότι, συνεπώς, η χρήση

των συγκεκριμένων διαπιστευτηρίων εντός του φορέα δεν συνεπάγεται κινδύνους από τη σκοπιά των πληροφοριακών συστημάτων, για τη συνολική αποτίμηση της ασφάλειας της εν λόγω επεξεργασίας, πρέπει να ληφθεί υπόψη ο ιδιαίτερος χαρακτήρας που εκ της φύσεώς τους προσλαμβάνουν τα εν λόγω διαπιστευτήρια. Συγκεκριμένα, μολονότι κάθε φυσικό πρόσωπο, ως φορολογούμενος, ενημερώνεται σαφώς ότι υπέχει υποχρέωση ασφαλούς φύλαξης και χρήσης των διαπιστευτηρίων του και μη διαβίβασής τους σε τρίτους, και τούτο στο πλαίσιο του αρχικού (φορολογικού) σκοπού για τον οποίο του έχουν αποδοθεί, δεν πρέπει να θεωρείται ως δεδομένο ότι είναι αποκλειστικά ο μόνος ο οποίος τα γνωρίζει. Για παράδειγμα, δεν μπορεί να αποκλειστεί το γεγονός ότι μέλη της οικογένειας ενός υπαλλήλου ή τρίτοι συνεργάτες του (π.χ. λογιστές) γνωρίζουν και οι ίδιοι τα εν λόγω διαπιστευτήρια, με πρωτοβουλία και ενέργειες του προσώπου στο οποίο ανήκουν, προς υποβοήθησή του στην άσκηση των υποχρεώσεών του ως φορολογούμενου. Η πρακτική αυτή –ακόμα και αν οι οδηγίες των ΑΑΔΕ/ΓΓΠΣ ρητά την αποθαρρύνουν/απαγορεύουν και παρά το ότι δεν μπορεί να εκτιμηθεί αν και σε ποιο βαθμό υιοθετείται από μικρό ή μεγάλο πλήθος φορολογουμένων– δεν μπορεί να αγνοηθεί κατά την αποτίμηση της ασφάλειας της επεξεργασίας στην υπό κρίση περίπτωση.

Συνεπώς, είναι υπαρκτός ο κίνδυνος από τη χρήση των προσωπικών κωδικών, αν και μπορεί να περιοριστεί με τεχνικά μέτρα. Η υλοποίηση μηχανισμού αυθεντικοποίησης δύο παραγόντων, η οποία προτείνεται από την ΑΑΔΕ και τη ΓΓΠΣ αποτελεί ένα κατ' αρχήν πρόσφορο μέτρο μετριασμού αυτού του κινδύνου, το οποίο μάλιστα αποτελεί πλέον συνήθη πρακτική.

Η λήψη, όμως μέτρων ασφαλείας δεν αίρει την παραβίαση την οποία συνιστά, κατά τα εκτιθέμενα στη σκέψη 7, η υποχρεωτική χρήση των διαπιστευτηρίων για δύο μη συμβατές κατηγορίες σκοπών.

9. Ενόψει των ανωτέρω, και λαμβάνοντας επίσης υπόψη αφενός ότι η διαδικασία απόδοσης διαπιστευτηρίων σε φυσικά πρόσωπα η οποία έχει υλοποιηθεί στο πλαίσιο του μηχανισμού TAXISNET είναι ασφαλής, δεδομένου και ότι για να αποκτήσει κάποιο φυσικό πρόσωπο τα διαπιστευτήριά του απαιτείται φυσική παρουσία του σε αρμόδια Οικονομική Υπηρεσία με έγγραφα που αποδεικνύουν την ταυτότητά του³ και, αφετέρου, ότι απαιτείται εύλογο χρονικό διάστημα, λόγω των εγγενών τεχνικών δυσκολιών, της κρισιμότητας των εφαρμογών που πρέπει να τροποποιηθούν και του κόστους των αναγκαίων τροποποιήσεων,

³ Η διαδικασία αυτή είναι σύμφωνη και με τα όσα σχετικώς προβλέπονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (ΥΑΠ Φ.40.4/1/989, ΦΕΚ 1301/Β/2012) και, ειδικότερα, στο Παράρτημα ΙΙΙ αυτού, ως προς τους κανόνες και πρότυπα αναφορικά με την εγγραφή, ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών σε ηλεκτρονικές υπηρεσίες του δημόσιου τομέα

προκειμένου να μεταβληθεί ο υφιστάμενος μηχανισμός αυθεντικοποίησης των αρμόδιων δικαστικών υπαλλήλων Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, η Αρχή κρίνει ότι πρέπει να επιβληθεί στην ΑΑΔΕ και στο Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, ως υπευθύνους επεξεργασίας στην περίπτωση, την οποία αφορά το εξεταζόμενο ερώτημα, η προβλεπόμενη στο εφαρμοστέο στην παρούσα υπόθεση άρθρο 21 παρ. 1 στοιχ. α΄ του ν. 2472/1997, προειδοποίηση η οποία περιγράφεται στο διατακτικό της παρούσας. Τα παραπάνω δε, ισχύουν για όλες τις περιπτώσεις δικαστικών υπαλλήλων. Περαιτέρω, επισημαίνεται ότι η ΑΑΔΕ οφείλει να επανεξετάσει το σχεδιασμό της διαδικασίας αυθεντικοποίησης για την έκδοση ηλεκτρονικού παραβόλου από υπαλλήλους όλων των φορέων του δημοσίου.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα απευθύνει, με βάση το άρθρο 21 παρ. 1 στοιχ. α΄ του ν. 2472/1997, προειδοποίηση στην ΑΑΔΕ και στο Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων να αναπροσαρμόσουν, μέχρι το τέλος του έτους 2019, τους μηχανισμούς αυθεντικοποίησης των δικαστικών υπαλλήλων, οι οποίοι είναι αρμόδιοι για τη δέσμευση και τον εν γένει χειρισμό των ηλεκτρονικών παραβόλων, κατά τρόπο τέτοιο ώστε να μην απαιτείται να εισάγουν, για την αυθεντικοποίησή τους, τα διαπιστευτήρια του TAXISNET, καθώς επίσης και να ενημερώσουν σχετικώς την Αρχή.

Ο Πρόεδρος

Η γραμματέας

Κωνσταντίνος Μενουδάκος

Ειρήνη Παπαγεωργοπούλου