ΟΡΘΗ ΕΠΑΝΑΛΗΨΗ
(Ως προς τον αριθμό της Γνωμοδότησης)

Αθήνα, 20-09-2013

Αριθ. Πρωτ.: Γ/ΕΞ/5668-2/20-09-2013

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Γ Ν Ω Μ Ο Δ Ο Τ Η Σ Η 5/2013

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε μετά από πρόσκληση του Προέδρου της σε έκτακτη συνεδρίαση την 19η Σεπτεμβρίου 2013 στο κατάστημά της, σε συνέχεια της από 18.9.2013 τακτικής συνεδρίασής της, αποτελούμενη από τους Π. Χριστόφορο, Πρόεδρο, Λ. Κοτσαλή, Α.Ι. Μεταξά, Δ. Μπριόλα Α. Συμβώνη, ως εισηγητή, Κ. Χριστοδούλου και Π. Τσαντίλα τακτικά μέλη. Μετά από εντολή του Προέδρου συμμετείχε επίσης το αναπληρωματικό μέλος της Αρχής Σ. Βλαχόπουλος, ως εισηγητής, με δικαίωμα ψήφου. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν η Ζ. Καρδασιάδου, ειδική επιστήμων-νομικός, προϊσταμένη του τμήματος ελεγκτών, Κ. Λωσταράκου, ειδική επιστήμων-νομικός, Ε. Χατζηλιάση, ειδική επιστήμων-νομικός και Κ. Λιμνιώτης, ειδικός επιστήμων-πληροφορικός, ως βοηθοί εισηγητές και η Μ. Γιαννάκη, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας, μετά από εντολή του Προέδρου.

Η Αρχή συνεδρίασε προκειμένου να γνωμοδοτήσει, σύμφωνα με το άρθρο 19 παρ. 1 στοιχ. θ΄ του ν. 2472/1997, επί ερωτήματος του Γενικού Γραμματέα Δημοσίων Εσόδων κατά τα αμέσως κατωτέρω αναφερόμενα. Στη συνεδρίαση και μετά από πρόσκληση της Αρχής (Γ/ΕΞ/5668-1/16-09-2013) παρέστησαν και εξέφρασαν τις απόψεις τους ο Α, σύμβουλος του Γενικού Γραμματέα Δημόσιων Εσόδων, και ο Β, υπάλληλος του Γραφείου Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων και Υποδομών της Γενικής Γραμματείας Πληροφοριακών Συστημάτων.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Ο Γενικός Γραμματέας Δημοσίων Εσόδων με το με αριθμ. πρωτ. Γ.Γ.Δ.Ε 0006891 ΕΞ 2013/4.9.2013 (αριθμ. πρωτ. Αρχής Γ/ΕΙΣ/5668/4.9.2013) έγγραφό του ζήτησε τη γνωμοδότηση της Αρχής επί του σχεδίου υπουργικής απόφασης για την ενεργοποίηση και λειτουργία του Συστήματος Μητρώων Τραπεζικών Λογαριασμών και Λογαριασμών Πληρωμών (στο εξής και Σ.Μ.Τ.Λ. και Λ.Π.). Ακολούθως, στις 13.9.2013 (αριθμ. πρωτ. Αρχής Γ/ΕΙΣ/5846/13.9.2013) και 19.9.2013 (αριθμ. πρωτ. της Αρχής Γ/ΕΙΣ/5951/19.9.2013) διαβιβάσθηκαν στην Αρχή το σχέδιο Κανονισμού Διαχείρισης και Λειτουργίας καθώς και κείμενο τεχνικών προδιαγραφών του ίδιου συστήματος αντίστοιχα.

Το Σύστημα Μητρώων Τραπεζικών Λογαριασμών και Λογαριασμών Πληρωμών συνιστάται με το άρθρο 62 του ν. 4170/2013· σε αυτό δε εντάσσονται δημόσιες αρχές και υπηρεσίες που ασκούν ελεγκτικό και διωκτικό έργο στις οποίες μέσω του συστήματος παρέχεται η δυνατότητα αυτοματοποιημένης πρόσβασης σε στοιχεία τραπεζικών λογαριασμών και λογαριασμών πληρωμών που τηρούν τα πιστωτικά ιδρύματα και τα ιδρύματα πληρωμών για φυσικά και νομικά πρόσωπα.

Με την παράγραφο 6 της ανωτέρω διάταξης παρέχεται εξουσιοδότηση στον Υπουργό Οικονομικών να ρυθμίσει με απόφασή του «*το χρόνο έναρξης λειτουργίας του Συστήματος Μητρώων Τραπεζικών Λογαριασμών και Λογαριασμών Πληρωμών, τη λεπτομερή διαδικασία ένταξης των φορέων και πρόσβασης τους στο Σύστημα, τα διαβιβαζόμενα και τηρούμενα στοιχεία από τα πιστωτικά ιδρύματα και τα ιδρύματα πληρωμών, τις προθεσμίες και τα θέματα παροχής πληροφοριών από τα υπόχρεα πρόσωπα προς τις αρχές, τις υπηρεσίες και τους φορείς του Δημοσίου στις περιπτώσεις που η παροχή αυτών των πληροφοριών διενεργείται εκτός Σ.Μ.Τ.Λ. και Λ.Π., καθώς και κάθε σχετικό θέμα για την εφαρμογή των διατάξεων του παρόντος*». Παράλληλα σύμφωνα με την παράγραφο 2 του ίδιου άρθρου «*με απόφαση του Υπουργού Οικονομικών μετά από εισήγηση της Γενικής Γραμματείας Πληροφοριακών Συστημάτων ορίζεται υπεύθυνος διαχείρισης του Σ.Μ.Τ.Λ. και Λ.Π. και χωρίς προηγούμενη άδεια από την Αρχή Προστασίας Προσωπικών Δεδομένων εκδίδεται Κανονισμός Διαχείρισης της Λειτουργίας του εντός αποκλειστικής προθεσμίας δύο (2) μηνών στον οποίο ειδικότερα ορίζεται η διαδικασία διασύνδεσης και επικοινωνίας των αρχών, υπηρεσιών και φορέων του Δημοσίου με τα υπόχρεα πρόσωπα, ο τρόπος καταγραφής των πληροφοριών και στοιχείων που επιτρέπει την προσήκουσα αποτύπωση και διαβίβαση τους, οι μορφότυποι παροχής των πληροφοριών και στοιχείων και κάθε άλλο σχετικό θέμα με τη*

διαχείριση της λειτουργίας του Σ.Μ.Τ.Λ. και Λ.Π.».

Το Σ.Μ.Τ.Λ. και Λ.Π, όπως ορίζεται στο άρθρο 62 του ν. 4170/2013, αποσκοπεί στη διευκόλυνση της διαβίβασης αιτημάτων άρσης του τραπεζικού απορρήτου από τις αρμόδιες δημόσιες αρχές και υπηρεσίες (συγκεκριμένα από τη Γενική Γραμματεία Δημοσίων Εσόδων του Υπουργείου Οικονομικών, το Σώμα Δίωξης Οικονομικού Εγκλήματος, την Οικονομική Αστυνομία, τον Οικονομικό Εισαγγελέα, τον Εισαγγελέα Εγκλημάτων Διαφθοράς και την Αρχή Καταπολέμησης της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες) προς τα πιστωτικά ιδρύματα και τα ιδρύματα πληρωμών και στην άμεση λήψη των σχετικών απαντήσεων χωρίς πρόθεση να θιγεί η κείμενη νομοθεσία περί άρσης του τραπεζικού και επαγγελματικού απορρήτου. Από το σύνολο των διαβιβασθεισών ρυθμίσεων (δηλαδή το σχέδιο απόφασης του Υπουργού Οικονομικών και τον Κανονισμό Διαχείρισης και Λειτουργίας του συστήματος) και το κείμενο τεχνικών προδιαγραφών του συστήματος προκύπτουν, όμως, τα παρακάτω: α) η πρόσβαση των δημόσιων αρχών και υπηρεσιών στο Σ.Μ.Τ.Λ. και Λ.Π πραγματοποιείται μέσω της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (στο εξής και Γ.Γ.Π.Σ.) του Υπουργείου Οικονομικών, β) η Γ.Γ.Π.Σ. δεν λειτουργεί απλώς ως μοναδικός κόμβος διασύνδεσης και επικοινωνίας μεταξύ των αρχών αυτών και των πιστωτικών ιδρυμάτων αλλά και ως αποθετήριο των αιτημάτων και των απαντήσεων, από τις οποίες ένα μήνα μετά διαγράφονται οι επονομαζόμενες «*ευαίσθητες πληροφορίες*», δηλαδή το περιεχόμενο των απαντήσεων, γ) προβλέπεται η πρόσβαση των δημοσίων αρχών και υπηρεσιών όχι μόνο στα βασικά στοιχεία των τραπεζικών λογαριασμών αλλά και σε επιπλέον στοιχεία, όπως για παράδειγμα στο πρόσημο του λογαριασμού, στο υπόλοιπο και στην ημερομηνία τελευταίας κίνησης του λογαριασμού (βλ. Παράρτημα Γ΄ του σχεδίου της υπουργικής απόφασης), δ) ο έλεγχος νομιμότητας των αιτημάτων παροχής πληροφοριών – άρσης του τραπεζικού απορρήτου ανατίθεται εξ' ολοκλήρου στις δημόσιες αρχές και υπηρεσίες που έχουν πρόσβαση στο Σ.Μ.Τ.Λ. και Λ.Π (άρ. 62 παρ. 1 εδ. γ΄ του ν. 4170/2013), οι οποίες αναλαμβάνουν και την ευθύνη σε περίπτωση παραβίασης του (άρ. 63 παρ. 1 εδ. β΄ του ν. 4170/2013), ε) ο χρόνος τήρησης των στοιχείων των τραπεζικών λογαριασμών στο συγκροτούμενο Σ.Μ.Τ.Λ. και Λ.Π δεν προβλέπεται σε διάταξη νόμου (τυπικού ή ουσιαστικού) αλλά μόνο στο κείμενο τεχνικών προδιαγραφών του συστήματος (10 έτη από τη στιγμή που ο λογαριασμός έπαψε να είναι ενεργός), στ) προβλέπεται η τήρηση αρχείων καταγραφής από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων, τη διατραπεζική εταιρεία «Τειρεσίας Α.Ε.» και

τα πιστωτικά ιδρύματα χωρίς εντούτοις να ορίζεται και ο χρόνος τήρησης αυτών (Παράρτημα 6 του Κανονισμού Διαχείρισης και Λειτουργίας του συστήματος). Στο σημείο αυτό πρέπει να σημειωθεί ότι τόσο το σχέδιο υπουργικής απόφασης όσο και το σχέδιο Κανονισμού Διαχείρισης και Λειτουργίας του συστήματος περιέχουν ουσιώδεις ρυθμίσεις στα παραρτήματά τους, τέσσερα (σε σύνολο εννέα) από τα οποία είναι κενά.

Η Αρχή, αφού άκουσε τους εισηγητές και τους βοηθούς εισηγητές, οι οποίοι μετά τη διατύπωση των απόψεών τους αποχώρησαν, και κατόπιν διεξοδικής συζήτησης, εκδίδει την ακόλουθη

ΓΝΩΜΟΔΟΤΗΣΗ

1. Η Αρχή έχει αρμοδιότητα να γνωμοδοτήσει επί του σχεδιασμού και της υλοποίησης του προτεινόμενου συστήματος βάσει του άρθρου 19 παρ. 1 στοιχ. θ΄ του ν. 2472/1997, το οποίο ορίζει ότι «*1. Η Αρχή έχει τις εξής ιδίως αρμοδιότητες : ... θ) Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα …*». Από τη διάταξη αυτή, ερμηνευομένη υπό το πρίσμα του άρθρου 28 της Οδηγίας 95/46/ΕΚ, προκύπτει ότι η γνωμοδοτική αρμοδιότητα της Αρχής πρέπει να ασκείται εγκαίρως κατά το στάδιο καταρτίσεως νομοθετικών ή κανονιστικών ρυθμίσεων, διοικητικών μέτρων καθώς και κατά το σχεδιασμό επιμέρους επεξεργασιών (βλ. και Γνμ Αρχής 2/2010, σκ. 1).

2. Η επεξεργασία προσωπικών δεδομένων φυσικών προσώπων από δημόσιες αρχές λειτουργεί και αναπτύσσει τις συνέπειές της στο πλαίσιο του κράτους δικαίου και της αρχής της νομιμότητας. Επιπλέον, στο βαθμό που η προβλεπόμενη επεξεργασία συνιστά περιορισμό του ατομικού δικαιώματος του πληροφοριακού αυτοκαθορισμού, θα πρέπει να ορίζεται γενικώς και αντικειμενικώς με τυπικό νόμο ή κατόπιν ειδικής νομοθετικής εξουσιοδότησης με διάταγμα, να δικαιολογείται από αποχρώντες λόγους δημοσίου συμφέροντος, να τελεί σε πρόδηλη λογική συνάφεια με τον επιδιωκόμενο σκοπό, να είναι πρόσφορη, κατάλληλη και αναγκαία για την επίτευξη του σκοπού αυτού, να μην θίγει τον πυρήνα του δικαιώματος και να μην απονέμει στη Διοίκηση ευρεία διακριτική ευχέρεια. Κατά συνέπεια είναι απαραίτητο η σκοπούμενη επεξεργασία να προβλέπεται σε νομοθετική διάταξη, η οποία θα αναφέρει τα βασικά χαρακτηριστικά της επεξεργασίας, δηλαδή τον υπεύθυνο επεξεργασίας, το σκοπό αυτής, τα δεδομένα τα οποία θα τύχουν επεξεργασίας και το χρόνο τήρησης αυτών καθώς και τους αποδέκτες των δεδομένων. Με ειδικότερη νομοθετική εξουσιοδότηση επιτρέπεται να ανατεθεί στον

κανονιστικό νομοθέτη η ρύθμιση ειδικότερων, τεχνικών ή λεπτομερειακών θεμάτων, όπως ο σχεδιασμός του συγκεκριμένου συστήματος, δηλαδή οι τεχνικές προδιαγραφές των απαιτούμενων για τη λειτουργία του Σ.Μ.Τ.Λ. και Λ.Π. εφαρμογών, τα εν γένει οργανωτικά και τεχνικά μέτρα για την ασφάλεια της επεξεργασίας των δεδομένων, καθώς και κάθε άλλη αναγκαία λεπτομέρεια.

3. Το άρθρο 62 παρ. 2 του ν. 4170/2013 ορίζει ότι «*Η πρόσβαση των αρχών και υπηρεσιών του πρώτου εδαφίου της παραγράφου 1 του παρόντος στο Σ.Μ.Τ.Λ. και Λ.Π. πραγματοποιείται ηλεκτρονικά μέσω της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (Γ.Γ.Π.Σ.) του Υπουργείου Οικονομικών, η οποία λειτουργεί ως μοναδικός κόμβος διασύνδεσης και επικοινωνίας μεταξύ αυτών των αρχών και υπηρεσιών με τα υπόχρεα πρόσωπα.* ***Αντίστοιχα****, ως κόμβος ηλεκτρονικής διασύνδεσης και επικοινωνίας των υπόχρεων προσώπων με τη Γ.Γ.Π.Σ. για τις ανάγκες του παρόντος, ορίζεται η διατραπεζική εταιρεία "Τραπεζικά Συστήματα Πληροφοριών – Τειρεσίας Α.Ε."*». Από την ανωτέρω διάταξη προκύπτει ότι η Γ.Γ.Π.Σ οφείλει να λειτουργεί ως απλός κόμβος διασύνδεσης και επικοινωνίας μεταξύ των δημοσίων αρχών και υπηρεσιών και των πιστωτικών ιδρυμάτων και κατά συνέπεια ο χρόνος τήρησης της «*ευαίσθητης πληροφορίας*» (των απαντήσεων δηλαδή των πιστωτικών ιδρυμάτων) από την ίδια θα πρέπει να περιοριστεί στον απολύτως αναγκαίο για τη λειτουργία του συστήματος. Ως εκ τούτου η διάταξη του άρ. 4.3. του σχεδίου Κανονισμού Διαχείρισης και Λειτουργίας του συστήματος στο μέτρο που προβλέπει τη λειτουργία της Γ.Γ.Π.Σ. και ως αποθετηρίου «*ευαίσθητων πληροφοριών*» που περιέχουν προσωπικά δεδομένα για χρονικό διάστημα ενός μηνός δεν συνάδει με την προαναφερθείσα διάταξη του άρ. 62 παρ. 2 του ν. 4170/2013 και για το λόγο αυτό οι «*ευαίσθητες πληροφορίες*» θα πρέπει να διαγράφονται από το σύστημα αμέσως μόλις διαπιστώνεται η λήψη της απάντησης από τις αρμόδιες δημόσιες αρχές και υπηρεσίες. Προς τούτο επιπλέον τεχνικά μέτρα θα πρέπει να εφαρμοσθούν για την ασφαλή διαπίστωση ότι η απάντηση ελήφθη από τον αιτούντα χρήστη.

Τα «*διαβιβαζόμενα και τηρούμενα στοιχεία από τα πιστωτικά ιδρύματα και τα ιδρύματα πληρωμών*» (κατά τις προβλέψεις της παραγράφου 6 του άρ. 62 του ν. 4170/2013) συνιστούν ουσιώδη στοιχεία της επεξεργασίας και ως εκ τούτου ο προσδιορισμός τους θα πρέπει λάβει χώρα με τυπικό νόμο. Κατά συνέπεια, η πρόβλεψη των μεν πρώτων στο παράρτημα Γ΄ του σχεδίου της υπουργικής απόφασης των δε δεύτερων στο παράρτημα Δ΄ του κειμένου τεχνικών προδιαγραφών, δεν είναι ισχυρή.

Η παραπάνω παρατήρηση ισχύει και για τον προσδιορισμό του χρόνου τήρησης των στοιχείων του μητρώου, διότι η χρονική διάρκεια της επεξεργασίας αποτελεί βασική αρχή του δικαίου της προστασίας των προσωπικών δεδομένων (βλ. άρθρα 4 του ν. 2472/1997 και 6 της Οδηγίας 95/46/ΕΚ). Ως εκ τούτου η πρόβλεψη στο κείμενο τεχνικών προδιαγραφών του συστήματος του χρόνου τήρησης των στοιχείων των τραπεζικών λογαριασμών στο συγκροτούμενο Σ.Μ.Τ.Λ. και Λ.Π (10 έτη από τη στιγμή που ο λογαριασμός έπαψε να είναι ενεργός) δεν είναι ισχυρή.

4. Όπως και παραπάνω (υπό σημείο 2) αναφέρθηκε, η ρύθμιση ειδικότερων, τεχνικών ή λεπτομερειακών θεμάτων, όπως τα εν γένει οργανωτικά και τεχνικά μέτρα για την ασφάλεια της επεξεργασίας των δεδομένων επιτρέπεται να ανατεθεί με νομοθετική εξουσιοδότηση στον κανονιστικό νομοθέτη, υπό την έννοια ότι στην κανονιστική απόφαση θα τίθενται οι στόχοι της ασφάλειας της επεξεργασίας, οι οποίοι δύναται να εξειδικεύονται με την υιοθέτηση πολιτικής και σχεδίου ασφαλείας, τα οποία με τη σειρά τους επιβάλλεται να επικαιροποιούνται.

4.1. Η ασφάλεια των δεδομένων εξειδικεύεται με μέτρα που ικανοποιούν τρεις βασικούς στόχους, ήτοι την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, ενώ συμπληρωματικοί στόχοι, ιδίως από τη σκοπιά της προστασίας των προσωπικών δεδομένων, αποτελούν η μη αποποίηση της ευθύνης καθώς και ο διαχωρισμός των δεδομένων ανάλογα με το σκοπό της επεξεργασίας. Ως εκ τούτου, για το συγκεκριμένο σύστημα, θα πρέπει στην κανονιστική πράξη να υπάρχει ρητή αναφορά στην υποχρέωση λήψης μέτρων ώστε:

α) να απαγορεύεται η καθ' οιονδήποτε τρόπο ανάγνωση, αντιγραφή, τροποποίηση ή διαγραφή δεδομένων από μη δικαιούμενα και εξουσιοδοτημένα πρόσωπα,

β) να διασφαλίζεται η δυνατότητα ελέγχου και εξακρίβωσης: i) των δεδομένων που έχουν τύχει επεξεργασίας στο πλαίσιο λειτουργίας του συστήματος, ii) της επιμέρους ενέργειας, iii) του χρόνου της ενέργειας, iv) του προσώπου που προέβη στην ενέργεια (όχι μόνο σε επίπεδο φορέα, αλλά και σε επίπεδο φυσικού προσώπου που προέβη στη σχετική ενέργεια),

γ) να εξασφαλίζεται ότι τα εξουσιοδοτημένα πρόσωπα έχουν πρόσβαση μόνο στα δεδομένα που εμπίπτουν στον τομέα της αρμοδιότητάς τους βάσει των ειδικών διατάξεων,

δ) να διασφαλίζεται η ασφαλής μετάδοση (εμπιστευτικότητα και ακεραιότητα) των δεδομένων, τόσο από τα υπόχρεα πρόσωπα προς τη ΓΓΠΣ, όσο και από τη ΓΓΠΣ προς

τους αρμόδιους φορείς.

4.2. Από το περιεχόμενο των αρχείων καταγραφής (Παράρτημα 6 του σχεδίου Κανονισμού Διαχείρισης και Λειτουργίας του συστήματος) προκύπτει ότι δεν καθίσταται πλήρως εφικτός ο εκ των υστέρων έλεγχος της ορθής χρήσης του συστήματος – και τούτο διότι στα αρχεία καταγραφής (όπου και αποτυπώνονται οι αναζητήσεις που έλαβαν χώρα μέσω του συστήματος) δεν τηρείται η κρίσιμη πληροφορία αναφορικά με το πρόσωπο στο οποίο αφορά η κάθε αναζήτηση καθώς και το περιεχόμενο της απάντησης του πιστωτικού ιδρύματος. Η εδώ περιγραφόμενη διαδικαστική εγγύηση εξυπηρετεί την προστασία των προσωπικών δεδομένων και την παροχή αποτελεσματικής έννομης προστασίας, αφού καθιστά δυνατό τον έλεγχο από τις αρμόδιες δικαστικές αρχές και την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ενώ παράλληλα επιβεβαιώνει ότι δεν διαφοροποιείται η μέχρι σήμερα πρακτική άρσης του απορρήτου, κατά την οποία τα πιστωτικά ιδρύματα προβαίνουν σε έλεγχο της αρμοδιότητας της αιτούσας δημόσιας αρχής, έλεγχος ο οποίος με το προτεινόμενο σύστημα μπορεί να λάβει χώρα μόνον εκ των υστέρων. Προς αυτήν την κατεύθυνση, επισημαίνουμε ότι ως πλέον πρόσφορη λύση παρουσιάζεται η επιβολή υποχρέωσης τήρησης αυτής της πληροφορίας στα πιστωτικά ιδρύματα και όχι στη Γ.Γ.Π.Σ., η οποία λειτουργεί ως κόμβος διασύνδεσης και επικοινωνίας. Επίσης, κατά την αρχή του χρονικού περιορισμού θα πρέπει να προβλεφθεί ο χρόνος τήρησης των αρχείων καταγραφής από τα εμπλεκόμενα μέρη, ο οποίος θα πρέπει να προσδιορίζεται ευλόγως ώστε να συνάδει με τη συνταγματικώς κατοχυρωμένη αρχή της αποτελεσματικής έννομης προστασίας.

4.3. 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.

5. Η παράγραφος 2 του άρθρου 62 του ν. 4170/2013 προβλέπει ότι με απόφαση του

Υπουργού Οικονομικών και «*χωρίς προηγούμενη άδεια από την Αρχή Προστασίας Προσωπικών Δεδομένων*» εκδίδεται Κανονισμός Διαχείρισης της Λειτουργίας του Σ.Μ.Τ.Λ. και Λ.Π, στον οποίο ορίζεται η διαδικασία διασύνδεσης και επικοινωνίας των αρχών, υπηρεσιών και φορέων του Δημοσίου με τα υπόχρεα πρόσωπα, ο τρόπος καταγραφής των πληροφοριών και στοιχείων που επιτρέπει την προσήκουσα αποτύπωση και διαβίβασή τους, οι μορφότυποι παροχής των πληροφοριών και στοιχείων και κάθε άλλο σχετικό θέμα με τη διαχείριση της λειτουργίας του Σ.Μ.Τ.Λ. και Λ.Π. Στο σημείο αυτό πρέπει να διευκρινισθεί ότι, υπό το καθεστώς του ν. 2472/1997, η προηγούμενη άδεια της Αρχής δεν συνιστά προαπαιτούμενο όρο για την έκδοση (με κανονιστική πράξη) του κανονισμού λειτουργίας ενός συστήματος επεξεργασίας προσωπικών δεδομένων. Άδεια απαιτείται μόνο για τη λειτουργία ενός συστήματος, στην περίπτωση που το εν λόγω σύστημα επεξεργάζεται ευαίσθητα προσωπικά δεδομένα, κατά την έννοια του άρθρου 2 στοιχ. β΄ του ν. 2472/1997, γεγονός που δεν συντρέχει εν προκειμένω. Σε κάθε περίπτωση παραμένει η γενική γνωμοδοτική αρμοδιότητα της Αρχής, όπως αυτή προβλέπεται στο άρθρο 19 παρ. 1 στοιχ. θ΄ του ν. 2472/1997, αλλά και η εκ του άρθρου 6 του ίδιου νόμου υποχρέωση του υπεύθυνου επεξεργασίας να γνωστοποιήσει στην Αρχή την πραγματοποιούμενη επεξεργασία και μάλιστα πριν από την έναρξη αυτής.

6. Η απαλλαγή, βάσει της παραγράφου 5 του άρθρου 62 του ν. 4170/2013, από την ευθύνη σε περίπτωση διαβίβασης δεδομένων, τα οποία δεν περιλαμβάνονται στο αίτημα των δημοσίων αρχών και υπηρεσιών, πρέπει, κατ' ορθή ερμηνεία της σχετικής διάταξης, να διευκρινισθεί ότι για λόγους ισότητας αφορά και στις τράπεζες και είναι για τις τράπεζες εντελώς περιορισμένη. Περιλαμβάνει μόνο την περίπτωση κατά την οποία η διαβίβαση διαφορετικών από τα αιτηθέντα δεδομένων οφείλεται στον ίδιο τον αλγόριθμο που προβλέπεται στο παράρτημα Α΄ του σχεδίου της υπουργικής απόφασης, εφόσον αυτός ορίζεται σε κανονιστική πράξη και οι τράπεζες οφείλουν να τον εφαρμόσουν. Σε καμία περίπτωση, όσον αφορά την προστασία των προσωπικών δεδομένων, η προαναφερθείσα διάταξη δεν μπορεί να θεωρηθεί ότι προβλέπει την απαλλαγή των τραπεζών από την ευθύνη τους για τη μη λήψη των κατάλληλων μέτρων αποτροπής απαγορευμένης πρόσβασης ή απαγορευμένης διαβίβασης δεδομένων κατά τη λειτουργία του Μητρώου Τραπεζικών Λογαριασμών και Λογαριασμών Πληρωμών,

καθώς κάτι τέτοιο θα ήταν αντίθετο με το ενωσιακό δίκαιο περί προστασίας των

προσωπικών δεδομένων και ειδικότερα με τα άρθρα 6 και 17 της Οδηγίας 95/46/ΕΚ.

Ο Πρόεδρος	Η Γραμματέας
Π. Χριστόφορος	Μ. Γιαννάκη