ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 08-08-2014

Αριθ. Πρωτ.: Γ/ΕΞ/4941/08-08-2014

Α Π Ο Φ Α Σ Η ΑΡ. 117/2014

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την 06-08-2014, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Π. Χριστόφορος, Πρόεδρος της Αρχής, Λ. Κοτσαλής, Α. - Ι. Μεταξάς, Δ. Μπριόλας, Α. Συμβώνης, ως εισηγητής, Κ. Χριστοδούλου, και Π. Τσαντίλας, τακτικά μέλη. Στη συνεδρίαση, μετά από εντολή του Προέδρου, χωρίς δικαίωμα ψήφου, παρέστησαν η Ζ. Καρδασιάδου, ειδική επιστήμων – νομικός, προϊσταμένη του Τμήματος Ελεγκτών, ο Γ. Ρουσόπουλος, ειδικός επιστήμων – πληροφορικός, ο Ι. Λυκοτραφίτης, ειδικός επιστήμων – πληροφορικός, ως βοηθοί εισηγητές, και η Γ. Παλαιολόγου , υπάλληλος του Τμήματος Διοικητικών και Οικονομικών υποθέσεων, ως γραμματέας,. Ο έτερος βοηθός εισηγητής, Α. Χρυσάνθου ειδικός επιστήμων – πληροφορικός, απουσίαζε λόγω κωλύματος.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Από τη διενέργεια διοικητικών ελέγχων σε εταιρείες που δραστηριοποιούνται στον τομέα της εμπορίας δεδομένων προσωπικού χαρακτήρα διαπιστώθηκε ότι ορισμένες εξ αυτών είχαν στην κατοχή τους μεγάλο όγκο φορολογικών δεδομένων φυσικών προσώπων. Ακολούθως, ο έλεγχος επεκτάθηκε στη Γενική Γραμματεία Πληροφοριακών Συστημάτων (εφεξής Γ.Γ.Π.Σ.). Η Αρχή διαπίστωσε ότι τα ευρεθέντα προσωπικά (φορολογικά) δεδομένα που αφορούν στο σύνολο των φορολογουμένων στην Ελλάδα προέρχονται από τα τηρούμενα στη Γ.Γ.Π.Σ. στοιχεία

και συνοπτικά περιλαμβάνουν: i) στοιχεία του εντύπου Ε1 της φορολογικής δήλωσης για τα οικονομικά έτη από το 2003 έως και το 2009 και εν μέρει για το 2012, ii) στοιχεία του εντύπου Ε2 της φορολογικής δήλωσης για το οικονομικό έτος 2006, iii) στοιχεία του εντύπου Ε9, iv) στοιχεία του ΕΤΑΚ, v) στοιχεία της έκτακτης εισφοράς του ν. 3986/2011 για το οικονομικό έτος 2011, vi) στοιχεία του μητρώου φορολογουμένων, vii) στοιχεία των σημειωμάτων περαίωσης του έτους 2010 και viii) στοιχεία τελών κυκλοφορίας οχημάτων για τα έτη από το 2006 έως και το 2012.

Η Αρχή, με την απόφαση 98/2013, έκρινε ότι η Γ.Γ.Π.Σ., ως υπεύθυνη επεξεργασίας, παραβίασε την υποχρέωση λήψης των κατάλληλων μέτρων ασφάλειας κατά το άρθρο 10 παρ. 3 ν. 2472/1997, γεγονός που οδήγησε από το έτος 2000 έως και το έτος 2012 σε μη εξουσιοδοτημένη πρόσβαση και επεξεργασία από τρίτους ιδιαίτερα μεγάλου όγκου προσωπικών δεδομένων, απλών και ευαίσθητων, τα οποία στην πλειονότητά τους υπόκεινται και στο φορολογικό απόρρητο. Το πλήθος και ο χρόνος αναφοράς των δεδομένων υποδεικνύουν ουσιαστικά σειρά αλλεπάλληλων επιμέρους περιστατικών παραβίασης προσωπικών δεδομένων. Όπως εξάλλου διέλαβε η απόφαση 98/2013 (σκ. 3) η υποχρέωση λήψης των κατάλληλων μέτρων ασφάλειας έχει προληπτικό και κατασταλτικό χαρακτήρα. Προληπτικό ώστε τα εφαρμοστέα μέτρα να αποτρέψουν περιστατικά παραβίασης προσωπικών δεδομένων, κατασταλτικό ώστε τυχόν περιστατικό να μπορεί να ανιχνευθεί και να διερευνηθεί. Λαμβάνοντας υπόψη τη φύση και τον όγκο των δεδομένων που διέρρευσαν και τις ενδεχόμενες και πραγματικές συνέπειες για τα υποκείμενα των δεδομένων η Αρχή επέβαλε στη Γ.Γ.Π.Σ. σύμφωνα με το άρθρο 21 παρ. 1 στοιχ. β ν. 2472/1997 το ανώτερο προβλεπόμενο πρόστιμο, ύψους εκατόν πενήντα χιλιάδων ευρώ (150.000 €). Παράλληλα, κάλεσε τη Γ.Γ.Π.Σ. να εφαρμόζει στο εξής κατάλληλα μέτρα ασφάλειας, τα οποία περιγράφηκαν στη σκέψη 6 της απόφασης 98/2013, και να υποβάλει στην Αρχή, εντός δύο μηνών από την κοινοποίηση της απόφασης, χρονοδιάγραμμα για την εφαρμογή τους, καθώς και να ενημερώνει την Αρχή ανά τρίμηνο για την τήρηση του χρονοδιαγράμματος.

Ειδικότερα, τα μέτρα ασφάλειας αναφέρονται ως εξής: «*Η Γ.Γ.Π.Σ. πρέπει καταρχήν να εφαρμόζει πλήρως, δηλαδή σε όλα τα πληροφοριακά συστήματα που βρίσκονται υπό την ευθύνη της, την εγκεκριμένη πολιτική ασφαλείας ΠΑΠΣ-ΓΓΠΣ. Επίσης, μετά από ολοκληρωμένη μελέτη ανάλυσης επικινδυνότητας και ευπαθειών, πρέπει να προβεί σε αναθεώρηση της υφιστάμενης πολιτικής ασφάλειας, κατάρτιση, εφαρμογή και αξιολόγηση των επιμέρους σχεδίων ασφάλειας.*.

Στο πλαίσιο των ανωτέρω ενεργειών πρέπει να προβλεφθούν και τα ακόλουθα: α) Η σταδιακή διερεύνηση του ενδεχομένου λήψης πιστοποίησης σε θέματα διαδικασιών ασφάλειας. β) Ο έλεγχος από ανεξάρτητο οργανισμό, σε τακτική βάση τουλάχιστον ετησίως, της ασφάλειας των συστημάτων και διαδικασιών, συμπεριλαμβανομένης της αποτίμησης των εφαρμοζόμενων μέτρων ασφάλειας. Τα αποτελέσματά του να κοινοποιούνται στην Αρχή. γ) Ο περιοδικός έλεγχος από τη Γ.Γ.Π.Σ., τουλάχιστον ετησίως, των τυχόν εκτελούντων την επεξεργασία ως προς τη λήψη των κατάλληλων μέτρων ασφάλειας.

Η Γ.Γ.Π.Σ. πρέπει εντός δύο μηνών από την κοινοποίηση της παρούσας, να συντάξει σχετικό χρονοδιάγραμμα, στο οποίο θα προσδιορίζονται οι διαδικασίες για την κατάρτιση, την υλοποίηση, την επίβλεψη και την επικαιροποίηση των ανωτέρω και ο χρόνος εκτέλεσής τους. Πρέπει, επίσης, σύμφωνα με την σκέψη 2 της παρούσας, να γνωστοποιήσει αμελλητί στην Αρχή το χρονοδιάγραμμα, και να την ενημερώνει ανά τρίμηνο για την εφαρμογή του.

Επιπλέον, ως μέτρα για την αποφυγή, ανίχνευση και διερεύνηση περιστατικών παραβίασης προσωπικών δεδομένων θα πρέπει να προβλεφθούν και εφαρμοστούν αμελλητί τα εξής: α) Ελεγχόμενη, μέσω κατάλληλων εξουσιοδοτήσεων, διαδικασία εξαγωγής ή/και λήψης δεδομένων από τα τερματικά που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων ή/και να αποκλειστεί η χρήση αποσπώμενων μέσων και η σύνδεση στο διαδίκτυο από συγκεκριμένα τερματικά. β) Μέτρα για την προστασία της ακεραιότητας των αρχείων καταγραφής, τον έλεγχο της απομακρυσμένης πρόσβασης και την ενεργοποίηση συστηματικής διαδικασίας χρήσης και ελέγχου συνθηματικών σε κάθε σύστημα. γ) Αναθεώρηση της διαδικασίας καταγραφής ενεργειών τύπου ερωτημάτων (SELECT) σε πίνακες της βάσης δεδομένων ή συστήματα που επεξεργάζονται προσωπικά δεδομένα και λήψη μέτρων για τον αυτοματοποιημένο, προληπτικό, έλεγχο των αρχείων καταγραφής.»

Με την υπ’ αριθμ. πρωτ. Γ/ΕΙΣ/6545/16.10.2013 αίτησή της η Γ.Γ.Π.Σ. ζητά:

1. Να μεταρρυθμιστεί η απόφαση ώστε να της χορηγηθεί ο απαραίτητος από τις περιστάσεις χρόνος για την εφαρμογή των συστάσεων της Αρχής, υποστηρίζοντας ότι δεν είναι ανθρωπίνως δυνατή η αμελλητί εφαρμογή των μέτρων που αναφέρονται στην τελευταία παράγραφο της σκέψης 6 της απόφασης 98/2013. Προς επίρρωση ισχυρίζεται συνοπτικώς τα εξής:

α) Σε σχέση με την «*ελεγχόμενη, μέσω κατάλληλων εξουσιοδοτήσεων, διαδικασία εξαγωγής ή/και λήψης δεδομένων από τα τερματικά που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων*» και τον «*αποκλεισμό της χρήσης αποσπώμενων μέσων και τη σύνδεση στο διαδίκτυο από συγκεκριμένα τερματικά*» ότι η εφαρμογή σχετικών μέτρων μπορεί να γίνει με την προμήθεια κατάλληλου λογισμικού μέσω διαδικασίας προμηθειών του Δημοσίου η οποία θα απαιτήσει περίπου ένα έτος μέχρι να υπογραφεί η σχετική σύμβαση. Ο αποκλεισμός της χρήσης αποσπώμενων μέσων και η σύνδεση στο διαδίκτυο από συγκεκριμένα τερματικά μπορεί να αρχίσει άμεσα (μόνο όμως πιλοτικά) στα τερματικά που επεξεργάζονται προσωπικά δεδομένα.

β) Σε σχέση με τα «*μέτρα για την προστασία της ακεραιότητας των αρχείων καταγραφής, τον έλεγχο της απομακρυσμένης πρόσβασης και την ενεργοποίηση συστηματικής διαδικασίας χρήσης και ελέγχου συνθηματικών σε κάθε σύστημα*» ότι βρίσκεται ήδη σε εξέλιξη σχετική διαγωνιστική διαδικασία ενώ η Γ.Γ.Π.Σ. εφαρμόζει όλες τις πρόσφορες τεχνολογίες ελέγχου απομακρυσμένης πρόσβασης και προχωρεί σε αξιολόγηση της δυνατότητας επέκτασης των μέσων ελέγχου φυσικής πρόσβασης ώστε να περιλαμβάνουν συστήματα και εφαρμογές.

γ) Σε σχέση με την «*αναθεώρηση της διαδικασίας καταγραφής ενεργειών τύπου ερωτημάτων (SELECT) σε πίνακες της βάσης δεδομένων ή συστήματα που επεξεργάζονται προσωπικά δεδομένα και λήψη μέτρων για τον αυτοματοποιημένο, προληπτικό, έλεγχο των αρχείων καταγραφής*» ότι θα αξιολογηθεί ειδικό υλικό και λογισμικό ανεξάρτητης δομής για την καταγραφή κινήσεων βάσης δεδομένων ενώ η υπάρχουσα διαδικασία έχει σχεδιαστεί για να υποστηρίζει λειτουργικά τις εφαρμογές και τυχόν επιβάρυνσή της θα οδηγούσε σε εξάλειψη του διαθέσιμου χώρου αποθήκευσης.

2. Να εξαφανιστεί ή να μειωθεί στις 20.000 ευρώ το επιβληθέν πρόστιμο διότι α) ο νόμος προβλέπει τη δυνατότητα επιβολής προστίμου έως 50.000.000 δραχμές (ήτοι με ακριβή μετατροπή 146.735 ευρώ) και η σχετική απόφαση είναι μη νόμιμη κατά το υπερβάλλον και β) η Αρχή οφείλει να τηρεί την αρχή της αναλογικότητας και να αιτιολογεί ειδικά την κρίση της, ιδίως αν το πρόστιμο καθορίζεται πλησίον του ανώτατου νομίμου ορίου και επιπλέον, να λαμβάνει υπ’ όψιν περιστατικά που συντελούν στη μείωση της ποινής (έμπρακτη μετάνοια, προσπάθεια του καθού το

πρόστιμο να εξαλείψει τις αιτίες της παράβασης κ.ο.κ.). Κατά τους ισχυρισμούς της, τα ακόλουθα θα έπρεπε να αποτελέσουν αιτία για μείωση του προστίμου:

α) οι αναμφίβολες διαπιστώσεις ότι πρόκειται για δεδομένα τεράστιου όγκου και ποικιλομορφίας από συστήματα που έχουν τεθεί σε λειτουργία σε διαφορετικές περιόδους και διέθεταν εξαρχής διαφορετικού επιπέδου μηχανισμούς ασφάλειας.

β) γίνεται εργώδης προσπάθεια εκσυγχρονισμού των συστημάτων.

γ) τα μέτρα ασφάλειας ενισχύθηκαν πρόσφατα και καταγράφηκαν σε πολιτική ασφάλειας ενώ από 1-11-2011 λειτουργεί αυτοτελές Γραφείο Ασφαλείας.

δ) μετά την εκδήλωση του περιστατικού διεκόπη η λειτουργία του συστήματος εκτυπώσεων και οι εκτυπώσεις γίνονται μέσω των ΕΛΤΑ

ε) η από 2-11-2011 υπογραφή σύμβασης μεταξύ «Κοινωνία της Πληροφορίας Α.Ε.» και των εταιρειών «Unisystems Σ.Π.Α.Ε.» και «INTRASOFT I.S.A.» με αντικείμενο προμήθεια εξοπλισμού και παροχή υπηρεσιών για λογαριασμό της Γ.Γ.Π.Σ. η οποία αποδεικνύει την επιμέλεια του φορέα για την αναβάθμιση της υποδομής του και την επαύξηση του επιπέδου ασφάλειας.

Τέλος, η Γ.Γ.Π.Σ. ισχυρίζεται ότι δεν ευσταθούν οι εξής διαπιστώσεις της απόφασης:

αα) Ότι δεν έχει πραγματοποιηθεί ολοκληρωμένη αποτίμηση ευπαθειών ως προς τα υφιστάμενα συστήματα, ενώ ως προς τη νέα υποδομή έχει προβλεφθεί αλλά δεν έχει παραληφθεί. Η Γ.Γ.Π.Σ υποστηρίζει ότι έχει πραγματοποιηθεί-υλοποιηθεί ολοκληρωμένη αποτίμηση ευπαθειών στην καινούργια υποδομή, όμως όσον αφορά κάποιες παλιές εφαρμογές, όπως του Ε1, καταδείχθηκε επαρκώς στην Αρχή ότι αυτή σταδιακά μεταλλάσσεται και μεταφέρεται από το ένα τεχνολογικό περιβάλλον στο άλλο, ενώ δεν είναι ανθρωπίνως δυνατό να τροποποιηθεί γρήγορα καθώς βρίσκεται διαρκώς σε παραγωγική λειτουργία.

ββ) Ότι δεν έχει ολοκληρωθεί το κεντρικό σύστημα ελέγχου πρόσβασης, με αποτέλεσμα η πρόσβαση να πραγματοποιείται ανά εφαρμογή, ενώ η απομακρυσμένη πρόσβαση των διαχειριστών δεν ελέγχεται. Η Γ.Γ.Π.Σ. υποστηρίζει ότι στην πραγματικότητα για τα πληροφοριακά συστήματα που έχουν μεταπτωθεί ή έχουν εξαρχής εγκατασταθεί στη νέα υποδομή η πρόσβαση ελέγχεται κεντρικά, ενώ για τα παλαιότερα συστήματα γίνεται προσπάθεια να εφαρμοστεί στο σύνολό τους. Η πρόσβαση γίνεται μέσω κεντρικού καταλόγου στην πλειονότητα των συστημάτων

ενώ η απομακρυσμένη πρόσβαση των διαχειριστών γίνεται με προσωποποιημένους κωδικούς και καταγράφεται από το σύστημα.

γγ) Ότι τα τερματικά από τα οποία πραγματοποιείται η επεξεργασία είναι όλα συνδεδεμένα στο διαδίκτυο, ενώ οι χρήστες μπορούν ανεξέλεγκτα να χρησιμοποιούν αποσπώμενα μέσα. Η Γ.Γ.Π.Σ. υποστηρίζει ότι πρόσβαση στο διαδίκτυο έχει μόνο το προσωπικό της Γ.Γ.Π.Σ. που απασχολείται με τη διαχείριση και την ανάπτυξη των εφαρμογών ενώ οι λοιποί χρήστες, όπως π.χ. αυτοί στις Δ.Ο.Υ. και τα τελωνεία δεν έχουν πρόσβαση.

δδ) Ότι η ενεργοποίηση καταγραφής ενεργειών στη βάση δεδομένων αφορά μόνο στις ενέργειες σύνδεσης και αποσύνδεσης καθώς και στις ενέργειες ανάγνωσης των πινάκων εισοδήματος και της κάρτας αποδείξεων. Η Γ.Γ.Π.Σ. υποστηρίζει ότι κάθε εφαρμογή κάνει τις απαραίτητες καταγραφές όπως αναλυτικά περιγράφεται στο απαντητικό της έγγραφο, οι οποίες αποθηκεύονται στη βάση δεδομένων. Στο παράρτημα του εγγράφου παρατίθεται περιγραφή της καταγραφής ενεργειών ανά εφαρμογή.

Την 22-11-2013 πραγματοποιήθηκε συνάντηση στην έδρα της Αρχής μεταξύ εκπροσώπων της Γ.Γ.Π.Σ., παρουσία του Γενικού Γραμματέα, Χ. Τσαβδάρη, κατόπιν της με αριθμ. πρωτ. Γ/ΕΞ/7298/15-11-2013 έγγραφης πρόσκλησης. Στη συνάντηση αποσαφηνίσθηκαν και έγιναν αποδεκτά τα κατάλληλα μέτρα κατά την τελευταία παράγραφο της σκέψης 6 της απόφασης 98/2013. Τα μέτρα που αναφέρει η Γ.Γ.Π.Σ. στην αίτηση θεραπείας είναι καταρχήν αποδεκτά ως μέτρα που ανταποκρίνονται στις συστάσεις της απόφασης 98/2013 όμως η εφαρμογή τους απαιτεί μακρύτερο διάστημα. Ωστόσο άλλα μέτρα, προσωρινού χαρακτήρα, δύνανται να περιορίσουν σημαντικά την πιθανότητα να συμβεί νέο περιστατικό παραβίασης, μέχρι τη λήψη των ολοκληρωμένων, μόνιμων, μέτρων. Τα μέτρα αυτά συμφωνήθηκαν και αποτυπώθηκαν σε συνοπτικό πρακτικό (αρ. πρωτ. Αρχής Γ/ΕΙΣ/8106/20-12-2013). Ειδικότερα, σε σχέση με όσα αναφέρονται ανωτέρω υπό σημείο 1 α) θα εφαρμοστούν αμελλητί μέτρα, ιδίως η απενεργοποίηση των θυρών USB, ανταλλαγή αρχείων μέσω ελεγχόμενων κοινόχρηστων φακέλων μετά από κατάλληλες εξουσιοδοτήσεις, η εφαρμογή πολιτικής ομάδας (group policy) μέσω τεχνολογίας active directory, η απαγόρευση πρόσβασης σε μια σειρά από τοποθεσίες ιστού που αφορούν υπηρεσίες web email και αποθήκευσης αρχείων. Σε σχέση με όσα αναφέρονται ανωτέρω υπό σημείο 1 β) θα εφαρμοσθούν αμελλητί μέτρα, ιδίως η τήρηση σε ξεχωριστό αρχείο

κατάλληλου κωδικού που θα προκύπτει από συνάρτηση κατακερματισμού (hash) ώστε να ελέγχεται η ακεραιότητα των αρχείων καταγραφής που εξάγονται από τη βάση δεδομένων και η εφαρμογή της ήδη υπάρχουσας δυνατότητας απομακρυσμένης πρόσβασης μέσω σκληρών πιστοποιητικών. Σε σχέση με όσα αναφέρονται ανωτέρω υπό σημείο 1 γ) θα πρέπει με αντικειμενικά στοιχεία (π.χ. μετρήσεις, υπολογισμοί) να εκτιμηθεί η επίπτωση που θα προκαλέσει στην υπάρχουσα υποδομή της Γ.Γ.Π.Σ. η ενεργοποίηση διαδικασιών καταγραφής ερωτημάτων τύπου SELECT σε επιλεγμένους πίνακες, με βάση εγγράφως τεκμηριωμένη εκτίμηση κρισιμότητας των δεδομένων.

Η Αρχή μετά από εξέταση της παραπάνω αίτησης και των λοιπών στοιχείων του φακέλου, αφού άκουσε τον εισηγητή και τους βοηθούς εισηγητές, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Η αιτούσα κατά πρώτον δεν αμφισβητεί τη συνδρομή των πραγματικών γεγονότων τα οποία αποτέλεσαν την πραγματική βάση της παραβάσεως του άρθρου 10 παρ. 3 ν. 2472/1997, δηλαδή τη διαπιστωθείσα από την Αρχή διαρροή των στο ιστορικό της απόφασης 98/2013 αναφερόμενων προσωπικών (φορολογικών) δεδομένων, αλλά το σύνολο των αιτιάσεων κατά της υπ’ αριθμ. 98/2013 απόφασης αναφέρεται σε λόγους που κατά την άποψή της επιβάλλουν τη μείωση του επιβληθέντος προστίμου.

2. Σε σχέση δε προς τα παράπονα της αιτούσας ότι η Αρχή κάλεσε την αιτούσα να προβλέψει και εφαρμόσει «αμελλητί» μέτρα ασφάλειας προς αποτροπή και διερεύνηση περιστατικών παραβίασης προσωπικών δεδομένων στο μέλλον, πρέπει να σημειωθεί ότι η Αρχή, εν γνώσει των νόμιμων διαδικασιών για την προμήθεια νέων ή την αναβάθμιση των παλαιών συστημάτων που οφείλει να τηρεί η Γ.Γ.Π.Σ. ως δημόσια υπηρεσία, επιζήτησε τη λήψη των κατάλληλων μέτρων «αμελλητί», δηλαδή «άνευ υπαιτίου βραδύτητας», και όχι «παραχρήμα».. Εξάλλου, η απόφαση 98/2013 περιγράφει σε γενικές γραμμές τα ληπτέα μέτρα, τα οποία οφείλει να εξειδικεύσει η Γ.Γ.Π.Σ. ως υπεύθυνος επεξεργασίας. Σημειωτέον ότι όπως

αναφέρεται στο ιστορικό της παρούσας, κατά τη συνάντηση της 21.11.2013 διευκρινίσθηκε ότι τα προτεινόμενα από τη Γ.Γ.Π.Σ. οριστικά μέτρα βαίνουν προς την ορθή κατεύθυνση, τα οποία θα ληφθούν στον κατάλληλο τηρουμένων των νόμιμων διαδικασιών χρόνο, και εξειδικεύθηκαν μέτρα προσωρινού χαρακτήρα μέχρι τη λήψη των οριστικών μέτρων.

3. Όσον αφορά στους ισχυρισμούς της Γ.Γ.Π.Σ. ότι ορισμένες διαπιστώσεις της απόφασης 98/2013 δεν ευσταθούν, σημειώνονται τα εξής:

α) Ως προς τη διαπίστωση ότι δεν έχει πραγματοποιηθεί ολοκληρωμένη αποτίμηση ευπαθειών στα υφιστάμενα συστήματα, ενώ ως προς τη νέα υποδομή έχει προβλεφθεί αλλά δεν έχει παραληφθεί, η Αρχή έχει ήδη εξετάσει διεξοδικά το ζήτημα στη σκέψη 6 της απόφασης 98/2013 σε συνδυασμό με τις διαπιστώσεις υπό σημείο δ) στο ιστορικό της ίδιας απόφασης. Εξάλλου, η αιτούσα αποδέχεται ότι δεν υφίστατο ολοκληρωμένη αποτίμηση ευπαθειών που να συμπεριλαμβάνει και τα παλαιότερα συστήματα, ενώ ως προς τη νέα πληροφοριακή υποδομή δεν αμφισβητεί ότι η αποτίμηση ευπαθειών δεν είχε παραληφθεί.

β) Από το υπ' αριθμ. πρωτ. Γ/ΕΞ/8210/21-12-2012 πρακτικό της συνάντησης που πραγματοποιήθηκε στις 3-12-2012 και το υπ' αριθμ. πρωτ. …./…-…-…. υπόμνημα της Γ.Γ.Π.Σ., το οποίο ως στοιχείο του φακέλου της υπόθεσης ελήφθη υπ' όψιν στην απόφαση 98/2013, δεν επιβεβαιώνεται ο ισχυρισμός της αιτούσας ότι δεν ευσταθεί η διαπίστωση της Αρχής ότι δεν έχει ολοκληρωθεί το κεντρικό σύστημα ελέγχου πρόσβασης, με αποτέλεσμα η πρόσβαση να πραγματοποιείται ανά εφαρμογή, ενώ η απομακρυσμένη πρόσβαση των διαχειριστών δεν ελέγχεται. Συγκεκριμένα στο πρακτικό αναφέρεται στην ΕΡ14 «*Δεν υπάρχει κεντρικό σύστημα ελέγχου πρόσβασης. Τώρα εγκαθίσταται active directory (στο πλαίσιο του νέου taxisnet που θα ξεκινήσει να λειτουργεί εντός του Δεκεμβρίου 2012) στο οποίο θα αρχίσουν να προστίθενται σταδιακά ορισμένα συστήματα. Η πρόσβαση γίνεται με χρήση συνθηματικών ανά εφαρμογή*» ενώ στο υπόμνημα της Γ.Γ.Π.Σ. (σελ. 65) αναφέρεται ότι «*αυτή τη στιγμή οι διαχειριστές έχουν τοπικό προσωπικό λογαριασμό στο server διαχείρισης ο οποίος προγραμματίζεται να μεταφερθεί στην κεντρική LDAP υποδομή όπως άλλωστε οι προσωπικοί λογαριασμοί των υπολοίπων χρηστών των servers*».

γ) Ως προς τη διαπίστωση ότι τα τερματικά από τα οποία πραγματοποιείται η επεξεργασία είναι όλα συνδεδεμένα στο διαδίκτυο, ενώ οι χρήστες μπορούν ανεξέλεγκτα να χρησιμοποιούν αποσπώμενα μέσα, είναι σαφές από το γράμμα της

απόφασης 98/2013 ότι αφορά στους χρήστες, υπαλλήλους, της Γ.Γ.Π.Σ και όχι χρήστες άλλων φορέων.

δ) Ως προς τη διαπίστωση ότι η ενεργοποίηση καταγραφής ενεργειών στη βάση δεδομένων αφορά μόνον στις ενέργειες σύνδεσης και αποσύνδεσης καθώς και στις ενέργειες ανάγνωσης των πινάκων εισοδήματος και της κάρτας αποδείξεων, η Αρχή έχει ήδη εξετάσει διεξοδικά το ζήτημα στη σκέψη 5 της απόφασης 98/2013 σε συνδυασμό με τις διαπιστώσεις υπό σημείο δ) στο ιστορικό της ίδιας απόφασης. Εξάλλου, η αιτούσα δεν αμφισβητεί τις ελλείψεις των αρχείων καταγραφής ως προς το ειδικότερο θέμα της δυνατότητας ανίχνευσης περιστατικού παραβίασης προσωπικών δεδομένων.

4. Σε σχέση με την αναλογικότητα του επιβληθέντος προστίμου η Γ.Γ.Π.Σ. υποστηρίζει ότι δεν έχουν ληφθεί υπόψη παράγοντες μείωσης του προστίμου. Στη σκέψη 7 της απόφασης 98/2013 ρητώς αναφέρεται ότι «*για το ύψος της παραπάνω διοικητικής κύρωσης συνεκτιμώνται, ιδίως, η φύση και ο όγκος των δεδομένων, οι ενδεχόμενες και πραγματικές συνέπειες για τα υποκείμενα των δεδομένων από τη μη λήψη των κατάλληλων μέτρων ασφάλειας καθώς και τα τυχόν αντίμετρα (δηλαδή, διορθωτικά μέτρα) που λαμβάνει ο υπεύθυνος επεξεργασίας μετά τη διαπίστωση περιστατικού παραβίασης προσωπικών δεδομένων*» όπως επίσης ότι όπως προκύπτει από το ιστορικό και τις σκέψεις 5 – 6 της απόφασης πρόκειται για διαρροή προσωπικών δεδομένων που υπόκεινται και στο φορολογικό απόρρητο, πρωτοφανούς έκτασης αφού αφορούν στο σύνολο των φορολογουμένων στην Ελλάδα, για ιδιαίτερα μακρύ χρονικό διάστημα, τουλάχιστον από το έτος 2000 έως το 2012, κατ' ουσίαν υποδεικνύοντας σειρά αλλεπάλληλων διαρροών, επιπλέον τα δεδομένα κατέστησαν ήδη αντικείμενο παράνομης επεξεργασίας από τρίτους, ενώ μέχρι και την ημέρα λήψης της απόφασης δεν είχαν ληφθεί κατάλληλα μέτρα ασφάλειας για την αποτροπή, ανίχνευση και διερεύνηση περιστατικών παραβίασης προσωπικών δεδομένων. Συνεπώς, η Αρχή συνεκτιμώντας όλα τα ανωτέρω επέβαλε το ανώτερο προβλεπόμενο πρόστιμο. Σε σχέση με την υπογραφή σύμβασης την 2-11-2011 με αντικείμενο την προμήθεια εξοπλισμού και την παροχή υπηρεσιών για λογαριασμό της Γ.Γ.Π.Σ. (πβλ. σημείο 2 ε' στο ιστορικό της παρούσας) η αιτούσα προ της επιβολής του προστίμου δεν επικαλέσθηκε τη σύμβαση αλλά ούτε και με την αίτηση θεραπείας την προσκόμισε ούτε και απέδειξε καθ΄ οιονδήποτε τρόπο ότι η σύμβαση

έχει ως αντικείμενο τη βελτίωση του επιπέδου ασφάλειας υπό τις ειδικότερες πτυχές που εξετάσθηκαν στην απόφαση 98/2013.

5. Όσον αφορά στον ισχυρισμό της Γ.Γ.Π.Σ. ότι η απόφαση 98/2013 είναι μη νόμιμη κατά το υπερβάλλον ποσό των 146.735 μέχρι το ποσό των 150.000 ευρώ που επιβλήθηκε ως πρόστιμο σημειώνονται τα εξής: Με τις διατάξεις του άρθρου 3 ν. 2943/2001 «Έκτιση ποινών εμπόρων ναρκωτικών και άλλες διατάξεις αρμοδιότητας του Υπουργείου Δικαιοσύνης» ρυθμίσθηκε η μετατροπή και στρογγυλοποίηση των χρηματικών ποσών που προβλέπονται σε νόμους αρμοδιότητας του Υπουργείου Δικαιοσύνης, η οποία πραγματοποιείται σύμφωνα με τις διατάξεις των άρθρων 4 και 5 του Κανονισμού 1103/1997/ΕΚ του Συμβουλίου της Ευρωπαϊκής Κοινότητας και του άρθρου 2 ν. 2842/2000 «Λήψη συμπληρωματικών μέτρων για την εφαρμογή των Κανονισμών 1103/97/974198 και 2866198 του Συμβουλίου, όπως ισχύουν σχετικά με την εισαγωγή του ευρώ», σύμφωνα με τις οποίες ορίσθηκε η τιμή μετατροπής της δραχμής σε ευρώ και η στρογγυλοποίηση προς το πλησιέστερο λεπτό. Περαιτέρω, με τις διατάξεις του άρθρου 4 στοιχ. ε και του άρθρου 5 ν. 2943/2001 τα πρόστιμα των ανεξάρτητων διοικητικών αρχών, τα οποία προβλέπονται σε νόμο αρμοδιότητας του Υπουργείου Δικαιοσύνης αναπροσαρμόσθηκαν. Ειδικότερα, η διάταξη του άρθρου 5 παρ. 7 ν. 2943/2001 ορίζει ότι αν το προκύπτον ποσό σε ευρώ είναι μεγαλύτερο των 100.000 ευρώ και δεν υπερβαίνει το 1.000.000 ευρώ, η αναπροσαρμογή γίνεται στην πλησιέστερη ανώτερη δεκάκις χιλιάδα ευρώ, εφόσον τα τέσσερα τελευταία ακέραια ψηφία του προκύπτοντος ποσού σε ευρώ είναι ίσα ή μεγαλύτερα του αριθμού 5000 ευρώ. Συνεπώς, επειδή ο ν. 2472/1997, στο άρθρο 21 του οποίου ορίζεται η κύρωση του προστίμου και το ύψος αυτού, είναι αρμοδιότητας του Υπουργείου Δικαιοσύνης και το ανώτατο προβλεπόμενο πρόστιμο ανέρχεται σε 50.000.000 δραχμές οι οποίες μετά την μετατροπή στο νόμισμα του ευρώ θα ήταν 146.735 ευρώ, δηλαδή ποσό μεγαλύτερο των 100.000 ευρώ που δεν υπερβαίνει το 1.000.000 ευρώ και τα τέσσερα τελευταία ακέραια ψηφία (6.735) αποτελούν αριθμό μεγαλύτερο του αριθμού 5.000, νομίμως η Αρχή επέβαλε ως πρόστιμο το ποσό των 150.000 ευρώ.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Απορρίπτει την αίτηση θεραπείας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων για τους λόγους που αναφέρονται στο σκεπτικό της παρούσας.

Ο Πρόεδρος	**Η Γραμματέας**
Πέτρος Χριστόφορος	**Γεωργία Παλαιολόγου**