ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 09.08.2013

Αριθ. Πρωτ.: Γ/ΕΞ/5276

Α Π Ο Φ Α Σ Η 98/2013

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε μετά από πρόσκληση του Προέδρου της σε έκτακτη συνεδρίαση στην έδρα της την 30-07-2013, σε συνέχεια της από 17-07-2013 έκτακτης συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Π. Χριστόφορος, Πρόεδρος της Αρχής, Λ. Κοτσαλής, Δ. Μπριόλας, Α. Συμβώνης, ως εισηγητής, Π. Τσαντίλας, και Κ. Χριστοδούλου, τακτικά μέλη και ο Γ. Λαζαράκος, αναπληρωματικό μέλος, ως εισηγητής. Ο Α. - Ι. Μεταξάς δεν παρέστη λόγω κωλύματος αν και εκλήθη νομίμως εγγράφως. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν η Ζ. Καρδασιάδου, ειδική επιστήμων – νομικός, προϊσταμένη του Τμήματος Ελεγκτών, η Α. Μπούρκα, ειδική επιστήμων – πληροφορικός, ο Γ. Ρουσόπουλος, ειδικός επιστήμων – πληροφορικός, η Ε. Χατζηλιάση, ειδική επιστήμων - νομικός, ο Ι. Λυκοτραφίτης, ειδικός επιστήμων – πληροφορικός, ο Α. Χρυσάνθου ειδικός επιστήμων – πληροφορικός, ως βοηθοί εισηγητές, και η Μ. Γιαννάκη, υπάλληλος του Τμήματος Διοικητικών και Οικονομικών υποθέσεων, ως γραμματέας, μετά από εντολή του Προέδρου.

Στην έκτακτη συνεδρίαση της 17-07-2013 και μετά από κλήση της Αρχής (Γ/ΕΞ/…./27-06-2013) παρέστη και εξέφρασε τις απόψεις του ο Γενικός Γραμματέας Πληροφοριακών Συστημάτων, Α, μετά των Β, δικηγόρου - ειδικού συνεργάτη, Γ, δικηγόρου - ειδικού συνεργάτη, Δ, γενικού διευθυντή, Ε, διευθυντή της Δ/νσης Εκμετάλλευσης Συστημάτων Η/Υ, ΣΤ, διευθυντή της Δ/νσης Εφαρμογών Η/Υ, Ζ,

υπαλλήλου στο Γραφείο Ασφαλείας Πληροφοριακών Συστημάτων, Η, προϊσταμένου του Τμήματος Α΄ Τεχνικής Υποστήριξης, Θ, προϊσταμένης του Τμήματος Α΄ Φορολογίας, Εισοδήματος, Κεφαλαίου και Αυτοκινήτων.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Κατά την πραγματοποίηση διοικητικών ελέγχων της Αρχής 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 και νομικών προσώπων. Συγκεκριμένα, κατόπιν εξέτασης των ληφθέντων ψηφιακών πειστηρίων από έλεγχο που πραγματοποιήθηκε στις συστεγαζόμενες εταιρείες «Τ» και «Υ» στις .. και .. Οκτωβρίου 2012, διαπιστώθηκε ότι σε αυτά περιλαμβάνονται αναλυτικά στοιχεία των δηλώσεων φορολογίας εισοδήματος των οικονομικών ετών 2006 και 2009. Ειδικότερα:

α) Για το οικονομικό έτος 2009 βρέθηκε συμπιεσμένο αρχείο κειμένου με 21.283.143 εγγραφές, οι οποίες περιέχουν προσωπικά δεδομένα περίπου 1,5 εκατομμυρίου φορολογούμενων φυσικών προσώπων. Τα δεδομένα, μεταξύ άλλων, περιλαμβάνουν Α.Φ.Μ., ονοματεπώνυμο, διεύθυνση, επάγγελμα, τηλέφωνα, στοιχεία δελτίου αστυνομικής ταυτότητας, στοιχεία συζύγου, καθώς και συγκεκριμένους κωδικούς (με επεξήγηση) του εντύπου Ε1 της δήλωσης φορολογίας εισοδήματος που αντιστοιχούν στο δηλωθέν από το φορολογούμενο εισόδημα και σε άλλα φορολογικά δεδομένα. Επισημαίνεται ότι ορισμένοι εκ των παραπάνω κωδικών συνδέονται με ευαίσθητα, κατά την έννοια του ν. 2472/1997, δεδομένα (για παράδειγμα οι κωδικοί 001 και 002 «ΕΧΕΤΕ ΔΙΚΑΙΩΜΑ ΕΚΠΤΩΣΗΣ ΠΟΣΟΥ 2.400 ΕΥΡΩ ΛΟΓΩ ΑΝΑΠΗΡΙΑΣ 67% ΚΑΙ ΠΑΝΩ ΚΤΛ»).

β) Για το οικονομικό έτος 2006 βρέθηκαν αρχεία βάσεων δεδομένων μορφής MDB και DBF, τα οποία περιέχουν δεδομένα φυσικών και νομικών προσώπων και περιλαμβάνουν μεταξύ άλλων Α.Φ.Μ., στοιχεία Δ.Ο.Υ., ονοματεπώνυμο, διεύθυνση, επάγγελμα, στοιχεία δελτίου αστυνομικής ταυτότητας, ημερομηνία γέννησης, τηλέφωνα, αριθμό κυκλοφορίας οχήματος, μάρκα/τύπο οχήματος, στοιχεία συζύγου και διάφορα πεδία με τίτλο της μορφής (C001…C998). Από αντιπαραβολή με γνωστά στοιχεία προκύπτει ότι τα παραπάνω

δεδομένα αναφέρονται στα στοιχεία του εντύπου Ε1 της δήλωσης φορολογίας εισοδήματος του οικονομικού έτους 2006 και έχουν υποστεί περαιτέρω επεξεργασία με προσθήκη επιπλέον δεδομένων (π.χ. επιπλέον τηλεφωνικοί αριθμοί, μάρκα και μοντέλο οχήματος). Το γεγονός ότι πρόκειται για το συγκεκριμένο οικονομικό έτος προκύπτει και από επιμέρους πεδία (για παράδειγμα η αντιστοίχιση "011";"ΜΙΣΘΩΤΟΣ ΚΑΙ ΠΗΡΑΤΕ ΣΤΕΓΑΣΤΙΚΟ ΕΠΙΔΟΜΑ ΜΕΣΑ ΣΤΟ 2005").

Αξιοποιώντας ψηφιακά ίχνη από την ανάλυση των πειστηρίων των ανωτέρω ελέγχων, η Αρχή πραγματοποίησε στις ..-..-2012 νέους ελέγχους στις εταιρείες «Φ» και «Χ», από τους οποίους, σε συνδυασμό με τα αρχικά ευρήματα, προέκυψαν ενδείξεις ότι φυσικό πρόσωπο, εξωτερικός συνεργάτης των δύο εταιρειών σε θέματα πληροφορικής, είχε, ενδεχομένως παρανόμως, επεξεργαστεί προσωπικά (φορολογικά) δεδομένα. Η Αρχή διαβίβασε τα στοιχεία αυτά, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./19-11-2012 έγγραφό της, στην Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (εφεξής ΔΗΕ). Κατά τον έλεγχο στην οικία του ανωτέρω φυσικού προσώπου, που πραγματοποίησε η ΔΗΕ με τη συνδρομή ελεγκτή της Αρχής, βρέθηκαν νέα ψηφιακά πειστήρια, τα οποία χορηγήθηκαν στην Αρχή σύμφωνα με την υπ' αριθμ. πρωτ. Γ/ΕΞ/…./27-11-2012 έγγραφη εξουσιοδότηση του Πρόεδρου της Αρχής για την παραλαβή των πειστηρίων. Από την εξέταση αυτών των πειστηρίων προέκυψε ότι επρόκειτο για μεγάλο όγκο φορολογικών δεδομένων του οικονομικού έτους 2011. Αναλυτικότερα, βρέθηκαν:

α) Προσωπικά δεδομένα 3.165.546 φυσικών προσώπων που αφορούν σε όλα τα στοιχεία του εκκαθαριστικού σημειώματος της έκτακτης εισφοράς του ν. 3986/2011. Τα δεδομένα περιέχονται σε 130 αρχεία ascii χαρακτήρων, συμπιεσμένα σε 4 αρχεία τύπου rar. Κάθε ένα από τα αρχεία ascii χαρακτήρων έχει όνομα της μορφής "eisfXXY" (και σε δύο περιπτώσεις "eisfXX", όσον αφορά στα τελευταία ημερολογιακά αρχεία), όπου XX διψήφιος αριθμός από 00 έως 12 και Υ πεζό γράμμα του λατινικού αλφαβήτου. Τα αρχεία έχουν αύξουσα ημερομηνία δημιουργίας που ξεκινά από την 03-09-2011 (eisf01a) και καταλήγει την 01-03-2012 (eisf12). Τα αρχεία έχουν 68 διαφορετικά πεδία, η γραμμογράφηση των οποίων περιέχεται σε ξεχωριστό αρχείο με τίτλο rec_eisf.txt.

β) Δεδομένα που αφορούν στην πληρωμή των τελών κυκλοφορίας 6.800.715 οχημάτων φυσικών και νομικών προσώπων για το έτος 2011. Τα δεδομένα αυτά περιέχονται σε 25

αρχεία ascii χαρακτήρων, με ονόματα της μορφής "SHMAXX.Y", όπου το ΧΧ έχει τιμές 13, 24, 57, 68, 90 ή ΜΕ, ενώ το Υ είναι αριθμός από 1 έως το 5. Η ημερομηνία δημιουργίας των αρχείων είναι από την 09-11-2011 έως την 23-11-2011, ενώ δεν ευρέθησαν τα πεδία της γραμμογράφησης.

Λαμβάνοντας υπόψη τον όγκο και τη μορφή των στοιχείων, που ιδίως για το έτος 2011 παρέπεμπε ευθέως στα τηρούμενα από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων (στο εξής Γ.Γ.Π.Σ.) δεδομένα, η Αρχή επεκτείνοντας τον έλεγχο, κάλεσε με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./23-11-2012 έγγραφο τη Γ.Γ.Π.Σ. σε συνάντηση και απέστειλε δείγματα των πειστηρίων και δομημένο ερωτηματολόγιο. Στη συνάντηση που πραγματοποιήθηκε στις 3-12-2012 συμμετείχαν εκ μέρους της Αρχής ο Πρόεδρος και οι βοηθοί εισηγητές και εκ μέρους της Γ.Γ.Π.Σ ο τέως Γενικός Γραμματέας Πληροφοριακών Συστημάτων, Ι, οι σύμβουλοί του και υπηρεσιακοί παράγοντες. Οι απαντήσεις των παραγόντων της Γ.Γ.Π.Σ. επί του δομημένου ερωτηματολογίου αποτυπώθηκαν σε πρακτικό (εφεξής πρακτικό) που της απεστάλη προς σχολιασμό με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./21-12-2012 έγγραφο της Αρχής. Με το ίδιο έγγραφο ζητήθηκαν εντός δεκαπέντε ημερών περαιτέρω διευκρινίσεις σχετικά με: α) την περιγραφή των συστημάτων της Γ.Γ.Π.Σ. και των μέτρων ασφάλειας που έχουν ληφθεί για κάθε ένα από αυτά, β) τα μέτρα που ελήφθησαν από τη Γ.Γ.Π.Σ για την αντιμετώπιση του περιστατικού παραβίασης προσωπικών δεδομένων, γ) τις απαντήσεις που δόθηκαν κατά τη συνάντηση. Παράλληλα, με το ίδιο έγγραφο, απεστάλησαν και κρυπτογραφημένα πλήρη αντίγραφα των διαθέσιμων πειστηρίων ενώ ο κωδικός για την αποκρυπτογράφησή τους απεστάλη με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./27-12-2012 έγγραφο της Αρχής. Παρά τις υπενθυμίσεις εκ μέρους της Αρχής με τα υπ' αριθμ. πρωτ. Γ/ΕΞ/…/06-02-2013 και Γ/ΕΞ/…./01-03-2013 έγγραφα, η Γ.Γ.Π.Σ. απάντησε εγγράφως μόλις στις 10-7-2013 (βλ. παρακάτω), μετά την κλήση της σε ακρόαση ενώπιον της Αρχής.

Αξίζει να σημειωθεί ότι, όπως ενημερώθηκε η Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/…/24-01-2013 έγγραφο της Γ.Γ.Π.Σ., ο Υπουργός Οικονομικών, αφού περιήλθε σε γνώση του το περιστατικό παραβίασης προσωπικών δεδομένων και οι ενέργειες της Αρχής, διέταξε στις 14-1-2013 τη διενέργεια Έρευνας και Προκαταρκτικής Εξέτασης, και εφόσον προκύψουν σαφείς ενδείξεις για τη διάπραξη πειθαρχικών παραπτωμάτων από

συγκεκριμένους υπαλλήλους, τη διενέργεια Ένορκης Διοικητικής Εξέτασης (Ε.Δ.Ε.). Η Αρχή, μάλιστα, παρέσχε τα απαραίτητα στοιχεία στους διενεργούντες την Έρευνα και την Προκαταρκτική Εξέταση. Σύμφωνα με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/…./21-05-2013 έγγραφο της Γ.Γ.Π.Σ., η προθεσμία για τη διενέργεια της Ε.Δ.Ε. παρατάθηκε για ένα επιπλέον μήνα. Αξίζει δε να προστεθεί ότι η εκ των διενεργούντων την έρευνα, οικονομική επιθεωρήτρια Κ απέστειλε υπόμνηση στις υπηρεσίες της Γ.Γ.Π.Σ., ερωτώντας για τις ενέργειες της Γ.Γ.Π.Σ. σε σχέση με τα ερωτήματα που είχε θέσει η Αρχή, ενημερώνοντας σχετικά την Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/…./20-05-2013 έγγραφό της.

Παράλληλα, η Αρχή, αξιοποιώντας τα στοιχεία που προέκυψαν από τους ελέγχους της, διαβίβασε στη ΔΗΕ, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./21-12-2012 έγγραφό της, στοιχεία σχετικά με εμπορία προσωπικών δεδομένων, ενδεχομένως κατά παράβαση του ν. 2472/1997, από την εταιρεία «Ψ». Έρευνα στην εταιρεία αυτή διενεργήθηκε στις ..-.-2013 από τη ΔΗΕ με τη συνδρομή ελεγκτή της Αρχής. Επίσης, η ΔΗΕ ζήτησε, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/../07-01-2013 έγγραφό της, τη συνδρομή της Αρχής σε έρευνά της στην εταιρεία «Ω.». Τα συλλεχθέντα στους ελέγχους αυτούς ψηφιακά πειστήρια ζητήθηκαν από την ΔΗΕ με τα υπ' αριθμ. πρωτ. Γ/ΕΞ/…/11-02-2013 και Γ/ΕΞ/…./08-03-2013 έγγραφα του Προέδρου της Αρχής και χορηγήθηκαν τελικά στην Αρχή με τα υπ' αριθμ. πρωτ. Γ/ΕΙΣ/…./17-04-2013 και Γ/ΕΙΣ/…./22-04-2013 έγγραφα της Διεύθυνσης Εγκ/κων Ερευνών της Ελληνικής Αστυνομίας, κατόπιν έγκρισης των αρμόδιων εισαγγελικών και ανακριτικών αρχών. Κατά την εξέταση των πειστηρίων που αφορούν στην εταιρεία Ψ, δεν κατέστη τεχνικώς δυνατό να ανακτηθούν τα αρχεία που, εκ πρώτης όψεως, περιελάμβαναν φορολογικά δεδομένα. Αντίθετα, τα ψηφιακά πειστήρια που βρέθηκαν κατά τον έλεγχο στην εταιρεία Ω περιλαμβάνουν ιδιαίτερα μεγάλο όγκο φορολογικών δεδομένων φυσικών προσώπων. Συγκεκριμένα, κατά την εκτίμηση της Αρχής, προκύπτει ότι η συγκεκριμένη εταιρεία είχε στην κατοχή της προσωπικά δεδομένα, τα οποία περιλαμβάνουν:

α) Τα δηλωθέντα στοιχεία του εντύπου Ε1 της δήλωσης φορολογίας εισοδήματος για τα οικονομικά έτη από το 2003 έως και το 2009 καθώς και εν μέρει για το 2012. Ενδεικτικά παρατίθεται ο αριθμός ευρεθέντων εγγραφών στο βασικό πίνακα του εντύπου Ε1 για κάθε οικονομικό έτος: 2003 - 9.534.230, 2004 - 9.978.141, 2005 - 10.552.945, 2006 - 11.305.339, 2007 - 11.548.998, 2008 - 11.750.664, 2009 - 12.043.921, 2012 -

5.770.280.

β) Δηλωθέντα στοιχεία του εντύπου Ε2 της δήλωσης φορολογίας εισοδήματος για το οικονομικό έτος 2006.

γ) Στοιχεία ακινήτων του εντύπου Ε9 της δήλωσης φορολογίας εισοδήματος για απροσδιόριστο έτος.

δ) Στοιχεία υπολογισμού του Ενιαίου Τέλους Ακινήτων (ΕΤΑΚ), όπου αναφέρονται τα έτη 2008, 2009 και 2012.

ε) Στοιχεία υπολογισμού της έκτακτης εισφοράς του ν. 3986/2011 για το οικονομικό έτος 2011.

στ) Διάφορους πίνακες με στοιχεία του μητρώου φορολογουμένων καθώς και νεώτερα στοιχεία για την επικαιροποίησή του, χωρίς να μπορεί να διαπιστωθεί με βεβαιότητα το έτος αναφοράς.

ζ) Στοιχεία των σημειωμάτων περαίωσης που εστάλησαν το έτος 2010.

η) Στοιχεία πληρωμής τελών κυκλοφορίας οχημάτων για τα έτη από το 2006 έως και το 2012.

Τα παραπάνω στοιχεία βρέθηκαν καταχωρημένα σε βάση δεδομένων τύπου MySQL, καταλάμβαναν αποθηκευτικό χώρο περί τα 70 Gb, ενώ εκτιμάται ότι κάποια από αυτά είχαν υποστεί από την εταιρεία περαιτέρω επεξεργασία (π.χ. διασταύρωση ως προς την ακρίβειά τους).

Κατόπιν της ανάλυσης και των νεώτερων πειστηρίων, η Αρχή κάλεσε με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./05-06-2013 έγγραφό της τη Γ.Γ.Π.Σ. να παρασταθεί στη συνεδρίαση της ολομέλειας την 27-6-2013, δηλαδή σε διάστημα τριών εβδομάδων από την ημερομηνία της κλήσης, ώστε να είναι σε θέση η κλητευθείσα υπηρεσία να μελετήσει τα πειστήρια, δεδομένου του μεγάλου όγκου αυτών. Ενημέρωσε δε σχετικά τη Γ.Γ.Π.Σ., αναφέροντας ότι θα έπρεπε η ίδια να διαθέσει τα μέσα για την αντιγραφή των πειστηρίων. Ο Γενικός Γραμματέας Πληροφοριακών Συστημάτων, Α, ζήτησε αναβολή με το υπ' αριθμ. πρωτ. ΓρΓΓΠ.....ΕΞ2013ΕΜΠ/25-6-2013 έγγραφό του και κατόπιν αυτού, η Αρχή προχώρησε, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./27-06-2013 έγγραφό της, σε νέα κλήση για τη συνεδρίαση της 17-7-2013. Η Γ.Γ.Π.Σ. παρέλαβε τα νεώτερα πειστήρια, κατόπιν αιτήματός της, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/…./01-07-2013 έγγραφο της Αρχής και κατέθεσε το υπ' αριθμ.

πρωτ. ΓρΓΓΠ…..ΕΞ2013ΕΜΠ/10-7-2013 υπόμνημα (εφεξής πρώτο υπόμνημα), σε απάντηση του υπ' αριθμ. πρωτ. Γ/ΕΞ/…./21-12-2012 εγγράφου της Αρχής. Κατά τη συνεδρίαση της 17-7-2013 έλαβε προθεσμία και κατέθεσε εμπροθέσμως το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/…./24-07-2013 υπόμνημα (εφεξής δεύτερο υπόμνημα).

Διαπιστώσεις

Από την εξέταση του πρακτικού της συνάντησης της 3-12-2012, των υπομνημάτων της Γ.Γ.Π.Σ. και των ψηφιακών πειστηρίων, προκύπτουν τα εξής:

α) Τα ευρεθέντα κατά τον ανωτέρω τρόπο προσωπικά (φορολογικά) δεδομένα προέρχονται πράγματι από τα τηρούμενα στη Γ.Γ.Π.Σ. στοιχεία και συνοπτικά περιλαμβάνουν: i) στοιχεία του εντύπου Ε1 για τα οικονομικά έτη από το 2003 έως και το 2009 και εν μέρει για το 2012, ii) στοιχεία του εντύπου Ε2 για το οικονομικό έτος 2006, iii) στοιχεία του εντύπου Ε9 τα οποία σύμφωνα με τη Γ.Γ.Π.Σ. αφορούν σε παλαιότερα, προ του 2000, έτη, iv) στοιχεία του ΕΤΑΚ, v) στοιχεία της έκτακτης εισφοράς του ν. 3986/2011 για το οικονομικό έτος 2011, vi) στοιχεία του μητρώου φορολογουμένων, χωρίς να μπορεί να διαπιστωθεί με βεβαιότητα το έτος αναφοράς, vii) στοιχεία των σημειωμάτων περαίωσης του έτους 2010, viii) στοιχεία τελών κυκλοφορίας οχημάτων για τα έτη από το 2006 έως και το 2012. Διαπιστώνονται ωστόσο ορισμένες διαφορές με τα στοιχεία που τηρεί η Γ.Γ.Π.Σ., οι οποίες αφορούν στους πίνακες του μητρώου, όπου εμφανίζονται Α.Φ.Μ. και δεδομένα θανόντων, καθώς και ορισμένες διαφορές στην ημερομηνία γέννησης φυσικών προσώπων. Διαφορές εμφανίζονται, επίσης, στο πλήθος των εγγραφών που αφορούν στις δηλώσεις του εντύπου Ε1 για τα προ του 2009 έτη (βλ. σελ. 18 του δεύτερου υπομνήματος της Γ.Γ.Π.Σ.). Οι ανωτέρω διαφορές δεν ανατρέπουν ωστόσο το συμπέρασμα ότι η βασική πηγή προέλευσης των στοιχείων είναι η Γ.Γ.Π.Σ., αλλά απλά καταδεικνύουν ότι τα συγκεκριμένα δεδομένα έχουν υποστεί περαιτέρω επεξεργασία από τις εταιρείες στην κατοχή των οποίων βρέθηκαν.

β) Τα δεδομένα που αφορούν έτη από το 2010 και μετά προέρχονται από το σύστημα που χρησιμοποιείται, μεταξύ άλλων, για την εκτύπωση εκκαθαριστικών σημειωμάτων και λοιπών ειδοποιητηρίων (π.χ. πληρωμής τελών κυκλοφορίας, ΕΤΑΚ, κ.λπ.), με σκοπό την αποστολή τους στους φορολογουμένους, όπως συνομολογεί η Γ.Γ.Π.Σ. (πβλ. σημείο ΕΡ2 του πρακτικού, καθώς και σελ. 60 - 64 του πρώτου υπομνήματος). Δεν κατέστη δυνατό να

διαπιστωθεί από ποια συστήματα προέρχονται τα δεδομένα προηγούμενων ετών. Επιπλέον, ανεξαρτήτως έτους αναφοράς, τα δεδομένα των εντύπων Ε9 και Ε2, καθώς και τα στοιχεία μητρώου, δεν μπορεί να προέρχονται από το σύστημα εκτυπώσεων, καθώς δεν αποστέλλονται σε σχέση με αυτά σχετικά σημειώματα ή ειδοποιητήρια στους φορολογούμενους.

γ) Κατά το έτος 2010 είχε αναφερθεί περιστατικό παραβίασης προσωπικών δεδομένων που αφορούσε στοιχεία εισοδήματος του έτους 2008 και του μητρώου και είχε υποβληθεί σχετική μηνυτήρια αναφορά, χωρίς όμως να πραγματοποιηθεί Ε.Δ.Ε. (πβλ. και σημείο ΕΡ5 του πρακτικού). Αντίγραφο της αναφοράς δεν υπάρχει στα αρχεία της Γ.Γ.Π.Σ., όπως δηλώθηκε κατά τη συνεδρίαση. Με αφορμή το παραπάνω περιστατικό, τα μέτρα ασφάλειας της Γ.Γ.Π.Σ. ενισχύθηκαν, όπως προκύπτει από την πρόβλεψη και έναρξη λειτουργίας από 1-11-2011 του Γραφείου Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων και Υποδομών (άρθ. 89 του ν. 3842/2010, Υ.Α. Δ6Α1159770ΕΞ2011 - ΦΕΚ Β 2841 2011), την ενεργοποίηση της καταγραφής ενεργειών ανάγνωσης (SELECT) των πινάκων στους οποίους τηρούνται τα δεδομένα του εντύπου Ε1 της δήλωσης φορολογίας εισοδήματος και της ηλεκτρονικής κάρτας αποδείξεων (φοροκάρτας), την επικαιροποίηση της Πολιτικής Ασφάλειας Πληροφοριακών Συστημάτων (στο εξής ΠΑΠΣ-ΓΓΠΣ - έκδοση 2.4 - Ιανουάριος 2011) και την κατάρτιση οριζόντιου σχεδίου ασφάλειας των Πληροφοριακών Συστημάτων (Φεβρουάριος 2011).

δ) Δεν έχει πραγματοποιηθεί ολοκληρωμένη αποτίμηση των ευπαθειών ως προς τα υφιστάμενα συστήματα, ενώ ως προς τη νέα πληροφοριακή υποδομή της Γ.Γ.Π.Σ., στην οποία μεταφέρονται σταδιακώς τα υφιστάμενα συστήματα, αυτή έχει προβλεφθεί αλλά δεν έχει ακόμη παραληφθεί (πβλ. σημείο Ε9 του Πρακτικού). Επιπλέον, αν και στην πολιτική και το οριζόντιο σχέδιο ασφάλειας προβλέπονται επαρκή μέτρα, αυτά δεν εφαρμόζονται πλήρως. Ειδικότερα (πβλ. και σημεία ΕΡ7, ΕΡ10, ΕΡ14, ΕΡ15, ΕΡ16, ΕΡ17, ΕΡ18, ΕΡ19, ΕΡ20 του πρακτικού): i) Δεν έχουν καταρτισθεί τα προβλεπόμενα στην ενότητα 1.4 της ΠΑΠΣ-ΓΓΠΣ σχέδια υλοποίησης ασφάλειας των επιμέρους πληροφοριακών συστημάτων (ΣΥΑ-ΠΣ). ii) Δεν ελέγχεται η εφαρμογή των προβλεπόμενων στις υπάρχουσες πολιτικές μέτρων, τα οποία επιπλέον αναφέρονται περισσότερο στις υποδομές και λιγότερο στις διαδικασίες. Για παράδειγμα, η διαδικασία εκτυπώσεων δεν προβλέπεται και κατά

συνέπεια δεν ελέγχεται˙ ο μόνος έλεγχος πραγματοποιήθηκε μετά την ενημέρωση της Γ.Γ.Π.Σ. από την Αρχή για το περιστατικό. iii) Δεν έχει εφαρμοστεί διαδικασία εσωτερικών ή εξωτερικών ελέγχων ασφάλειας. iv) Δεν έχει ολοκληρωθεί το κεντρικό σύστημα ελέγχου πρόσβασης στα πληροφοριακά συστήματα της Γ.Γ.Π.Σ. με αποτέλεσμα η πρόσβαση να πραγματοποιείται ανά εφαρμογή. Η απομακρυσμένη πρόσβαση των διαχειριστών στο πληροφοριακό σύστημα δεν ελέγχεται. v) Τα συνθηματικά που χρησιμοποιούνται για την πρόσβαση δεν είναι πάντα ισχυρά. vi) Δεν εφαρμόζεται πολιτική ελέγχου των αποσπώμενων μέσων ή λήψης αντιγράφων από τους υπολογιστές που χρησιμοποιούνται για την επεξεργασία των προσωπικών δεδομένων. Παρά τη ρητή πρόβλεψη στην πολιτική ασφάλειας για χρήση μόνο καθορισμένου και καταγεγραμμένου λογισμικού, έλεγχο της σύνδεσης του εσωτερικού τοπικού δικτύου με εξωτερικά δίκτυα και χρήση του διαδικτύου μόνο υπό αυστηρές προϋποθέσεις (ενότητες 7.1, 7.7 και 7.9 της ΠΑΠΣ-ΓΓΠΣ), τα τερματικά από τα οποία πραγματοποιείται η επεξεργασία είναι όλα συνδεδεμένα με το διαδίκτυο, ενώ οι χρήστες μπορούν ανεξέλεγκτα να χρησιμοποιούν αποσπώμενα μέσα (π.χ. οπτικούς δίσκους CD-DVD και USB) και να εγκαθιστούν λογισμικό. Η απενεργοποίηση των αποσπώμενων μέσων και η απαγόρευση πρόσβασης στο διαδίκτυο από τους υπολογιστές εφαρμόσθηκαν ως αντίμετρο για την αντιμετώπιση του περιστατικού παραβίασης αλλά και τότε μόνον για το σύστημα εκτυπώσεων (πβλ. σελ 64 του πρώτου υπομνήματος). vii) Η ενεργοποίηση καταγραφής ενεργειών χρηστών στην βάση δεδομένων του πληροφοριακού συστήματος αφορά μόνον στις ενέργειες σύνδεσης και αποσύνδεσης, καθώς επίσης και στις ενέργειες ανάγνωσης των πινάκων εισοδήματος και κάρτας αποδείξεων. Οι διαχειριστές έχουν τη δυνατότητα να απενεργοποιήσουν την καταγραφή και να διαγράψουν τα σχετικά αρχεία καταγραφής, ενώ δεν υπάρχει διαδικασία εξασφάλισης της ακεραιότητας των αρχείων καταγραφής. Ο έλεγχος των αρχείων αυτών δεν πραγματοποιείται με αυτοματοποιημένο τρόπο, συνεπώς είναι εξαιρετικά δυσχερής αν ληφθεί υπόψη το μέγεθός τους. Η Γ.Γ.Π.Σ. ισχυρίζεται ότι η επιλεκτική καταγραφή των ενεργειών σε συγκεκριμένους πίνακες ήταν αποτέλεσμα σωρείας πειραματισμών, όπου συνεκτιμήθηκαν οι επιπτώσεις στην απόδοση των συστημάτων και οι απαιτήσεις χωρητικότητας σε αποθηκευτικά μέσα (πβλ. και σελ 10 του δεύτερου υπομνήματος).

ε) Αναφορικά με την αντιμετώπιση του περιστατικού παραβίασης προσωπικών

δεδομένων, η Γ.Γ.Π.Σ. ανέστειλε (πβλ. σελ 60-64 του πρώτου υπομνήματος) τη λειτουργία του συστήματος εκτυπώσεων (από όπου θεωρεί ότι προέκυψε η διαρροή). Η εκτύπωση των σημειωμάτων, ειδοποιητηρίων, κ.λπ., για τους δύο τελευταίους μήνες του έτους 2012 πραγματοποιήθηκε από την ΕΛΛΗΝΙΚΑ ΤΑΧΥΔΡΟΜΕΙΑ Α.Ε. (ΕΛΤΑ), χωρίς το γεγονός αυτό να μπορεί να θεωρηθεί ως αντίμετρο, καθώς η εν λόγω ανάθεση έλαβε χώρα δυνάμει προϋφιστάμενης του περιστατικού συμφωνίας (συγκεκριμένα δυνάμει του από 21-02-2007 συμφωνητικού μεταξύ της εταιρείας και του ελληνικού Δημοσίου, όπως αυτό τροποποιήθηκε στις 15-11-2012 –πρβλ. δεύτερο υπόμνημα, σελ. 15 - 17) και επιπλέον η συγκεκριμένη σύμβαση περιορίζεται σε εργασίες που πρέπει να πραγματοποιηθούν μέχρι το τέλος του 2012. Επιπλέον, στη σύμβαση της 15-11-2012 και ειδικότερα στο άρθρο 6 αυτής περιέχονται όροι σχετικά με την εμπιστευτικότητα και την ασφαλή επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Παρότι προβλέπεται δικαίωμα επιθεώρησης και ελέγχου των εφαρμοζόμενων από τα ΕΛΤΑ μέτρων ασφαλείας, δεν αναφέρθηκε ότι κάτι τέτοιο έχει λάβει χώρα. Περαιτέρω, για τη διερεύνηση και αντιμετώπιση του περιστατικού, συγκλήθηκε η αρμόδια επιτροπή ασφάλειας πολλές φορές (πβλ. σελ 14-15 του δεύτερου υπομνήματος), αλλά άτυπα και χωρίς πρακτικά, οπότε δεν είναι δυνατόν να εκτιμηθεί πώς και για ποιο λόγο αποφασίστηκαν σταδιακά μέτρα και αντίμετρα. Επισημαίνεται επίσης ότι από την 10-12-2012 έχει ληφθεί ακριβές ηλεκτρονικό αντίγραφο (κλώνος) του υπολογιστή εκτυπώσεων, χωρίς να έχει πραγματοποιηθεί εξέτασή του από την ίδια ή από άλλη αρμόδια υπηρεσία. Αξίζει να σημειωθεί ότι το Γραφείο Ασφάλειας της Γ.Γ.Π.Σ. έχει αρμοδιότητα και για τον έλεγχο και τη διερεύνηση επεισοδίων ασφάλειας, σύμφωνα με το άρθρο 89 στοιχ. δ) του ν. 3842/2010, ενώ στην ΠΑΠΣ-ΓΓΠΣ προβλέπεται, μεταξύ άλλων, ότι, σε περίπτωση σοβαρής παραβίασης της ασφάλειας, το Γραφείο συντάσσει έκθεση περιστατικού μετά από αναφορά του υπευθύνου του εκάστοτε πληροφοριακού συστήματος, όπου περιγράφεται λεπτομερώς η παραβίαση και αναφέρονται τα εμπλεκόμενα μέρη. Τέλος, η Γ.Γ.Π.Σ. ανέφερε κατά την ακρόαση ότι μελετά την πιστοποίησή της σε θέματα διαδικασιών ασφάλειας.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων, αφού άκουσε τους εισηγητές και τους βοηθούς εισηγητές, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν

διεξοδικής συζήτησης

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Κατά τη γενική διάταξη του άρθρου 4 παρ. 2 ν. 2472/1997 οι υποχρεώσεις του νόμου βαρύνουν τον υπεύθυνο επεξεργασίας, προς τον οποίον κατά συνέπεια απευθύνονται συστάσεις κατά το άρθρο 19 παρ. 1 γ) και επιβάλλονται οι κυρώσεις του άρθρου 21. Ο γενικός αυτός κανόνας ακολουθείται και ως προς την υποχρέωση του υπευθύνου επεξεργασίας να λαμβάνει κατά το άρθρο 10 παρ. 3 τα κατάλληλα μέτρα ασφάλειας. Η ύπαρξη εκτελούντος την επεξεργασία κατά την παρ. 4 του ιδίου άρθρου δεν απαλλάσσει τον υπεύθυνο από τη δική του υποχρέωση˙ αντιθέτως η υποχρέωση βαρύνει αναλόγως και τον εκτελούντα έτσι ώστε η ανάθεση της επεξεργασίας να μην οδηγεί στην απομείωση της προστασίας των υποκειμένων των δεδομένων, εν τέλει της αποτελεσματικότητας του νόμου.

Ως υπεύθυνος επεξεργασίας ορίζεται στο νόμο (άρθρο 2 στοιχ. ζ) 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/ΕΚ περιέχει αντίστοιχο ορισμό στο άρθρο 2 στοιχ. δ) με μόνη διευκρινιστική προσθήκη -την οποία δεν αποκλείει το γράμμα και το πνεύμα του ελληνικού νόμου[1]- ότι ο υπεύθυνος επεξεργασίας καθορίζει *από μόνος του ή από κοινού με άλλους* το σκοπό και τον τρόπο της επεξεργασίας, προβλέποντας έτσι ότι η πολυπλοκότητα των εννόμων σχέσεων, των συναλλακτικών και τεχνολογικών αναγκών μπορεί να οδηγεί 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.

Η έννοια του υπευθύνου επεξεργασίας, η οποία αποτελεί αυτόνομη έννοια του ενωσιακού

[1] Πρβλ. ομοίως για τη διατύπωση στο γερμανικό ομοσπονδιακό νόμο προστασίας δεδομένων Dammann σε: Simitis, Bundesdatenschutzgesetz, 7η έκδοση, άρθρο 3, αρ. περ. 226

δικαίου[2], ως προς το υποκειμενικό πεδίο εφαρμογής της αναφέρεται σε σχέση με το δημόσιο τομέα σε αρχή, δημόσια υπηρεσία, νομικό πρόσωπο δημοσίου δικαίου ή άλλο οργανισμό. Στο βαθμό που ο ορισμός του άρθρου 2 στοιχ. δ) της Οδηγίας 95/46/ΕΚ αναφέρει παρατακτικά τις έννοιες δημόσια υπηρεσία, αρχή, οργανισμό κλπ. δεν αποκλείει τη διαφορετική διοικητική οργάνωση των εθνικών εννόμων τάξεων. Βαρύτητα δίδεται στο λειτουργικό κριτήριο, δηλαδή υπεύθυνος επεξεργασίας είναι αυτός που καθορίζει το σκοπό ή/και τα ουσιώδη, τουλάχιστον, στοιχεία του τρόπου της επεξεργασίας. Στη δημόσια διοίκηση το λειτουργικό κριτήριο συνάπτεται κατ' αρχήν με τις αρμοδιότητες που απονέμει ο νόμος σε συγκεκριμένη αρχή, υπηρεσία ή νομικό πρόσωπο δημοσίου δικαίου, οι οποίες θα πρέπει και στην πράξη να ασκούνται από τους φορείς τους.

Η Γενική Γραμματεία Πληροφοριακών Συστημάτων συστάθηκε με το π.δ. 61/1997 και αποτελεί αυτοτελή υπηρεσία κατά τις διατάξεις των άρθρων 26 και 27 ν. 1558/1985 για την Κυβέρνηση και τα Κυβερνητικά όργανα, όπως ισχύουν (βλ. και άρθρα 51 και 52 του κωδικοποιητικού π.δ. 63/2005, όπως ισχύουν). Εκτός της διοικητικής έχει και δημοσιονομική αυτοτέλεια με ιδιαίτερη λογιστική απεικόνιση του προϋπολογισμού της στον κρατικό προϋπολογισμό (Κωδικός Φορέα 150, βλ. ν. 4095/2012 για την Κύρωση του Κρατικού Προϋπολογισμού οικονομικού έτους 2013 σε συνδυασμό με το Παράρτημα, σελ. 104, 108, διαθέσιμο σε: http://www.minfin.gr/portal/el/resource/contentObject/id/05f96a54-21cb-4243-b04c-7cd78adf5bf7). Ως εκ του νόμου αυτοτελής υπηρεσία, κατά μείζονα λόγο αποτελεί ιδιαίτερη οργανωτική ενότητα με δική της γραφειοκρατική οργάνωση που αλληλογραφεί απευθείας με τις δημόσιες υπηρεσίες και τους διοικουμένους και η οποία μάλιστα εκδίδει εκκαθαριστικά σημειώματα προσδιορισμού φορολογικών και δημοσιονομικών υποχρεώσεων απευθυνόμενα στους υπόχρεους[3]. Στο βαθμό που η έννοια του υπευθύνου επεξεργασίας στη δημόσια διοίκηση προϋποθέτει κάποια αυτοτελή οργανωτική δομή, η Γ.Γ.Π.Σ. πληροί, οπωσδήποτε, το κριτήριο αυτό[4] και εξετάζεται στη συνέχεια η συνδρομή

[2] Πρβλ. για την έννοια του υπευθύνου και εκτελούντος την επεξεργασία τη Γνώμη 1/2010 της Ο.Ε. του Άρθρου 29, διαθέσιμη σε: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_el.pdf

[3] Πβλ. για τις αυτοτελείς υπηρεσίες και την έννοια της δημόσιας αρχής Ε. Σπηλιωτόπουλος, Εγχειρίδιο Διοικητικού Δικαίου, 2001, σελ. 255 – 257, 130 υποσημ. 2, αντιστοίχως, και Μ. Στασινόπουλος, Μαθήματα Διοικητικού Δικαίου, 1957, σελ. 275 επ.).

[4] Εξάλλου, σύμφωνα με τη διάταξη του άρθρου πρώτου παρ. Ε.2-7, υποπαράγραφος Ε.2, περ. 3 του ν.

του λειτουργικού κριτηρίου.

Ως προς το λειτουργικό κριτήριο: Σύμφωνα με το άρθρο 1 παρ. 3 και 4 του π.δ. 61/1997 σε συνδυασμό με το άρθρο 1 παρ. 1 του π.δ. 43/1997 για τη σύσταση Γενικής Διεύθυνσης Κέντρου Πληροφορικής Υπουργείου Οικονομικών (ΚΕ.Π.Υ.Ο.) και τα άρθρα 32 – 34 του π.δ. 284/1988 για τον Οργανισμό του Υπουργείου Οικονομικών στη Γ.Γ.Π.Σ. ανήκουν οι αρμοδιότητες των Διευθύνσεων 30 – 32 του Υπουργείου Οικονομικών, όπως ενδεικτικώς: α) δημιουργία μηχανογραφικών εφαρμογών σε θέματα i) εκκαθάρισης, βεβαίωσης και είσπραξης φόρων εισοδήματος φυσικών και νομικών προσώπων, ii) φορολογίας κεφαλαίου (μεταβιβάσεις ακινήτων, κληρονομιές, δωρεές, ακίνητη περιουσία, γονικές παροχές) και αντικειμενικού προσδιορισμού αξίας ακινήτων, iii) βεβαίωσης και είσπραξης τελών κυκλοφορίας αυτοκινήτων, iv) εκκαθάρισης, βεβαίωσης και είσπραξης Φ.Π.Α. και άλλων ειδικών και έμμεσων φόρων, v) τελωνείων και ειδικότερα για τον υπολογισμό δασμών και φόρων, β) διασταύρωση στοιχείων των ανωτέρω εφαρμογών, γ) καθορισμός και σύνταξη προτύπων ανάπτυξης και συντήρησης των εφαρμογών, δ) παρακολούθηση της αποδοτικής λειτουργίας των συστημάτων Η/Υ, ε) συντήρηση (προληπτικής και κατασταλτικής) του υλικού και λογισμικού στ) επεξεργασία των χρονοδιαγραμμάτων ροής των εφαρμογών και συντονισμό των εργασιών, ζ) τήρηση των διαδικασιών για την αποκατάσταση της λειτουργίας του συστήματος, μετά από οποιαδήποτε διακοπή ή βλάβη, η) μέριμνα για την ασφάλεια των αρχείων, θ) καθορισμός και σύνταξη προτύπων για την ασφάλεια και την ακεραιότητα των πληροφοριών, ι) καθορισμός των διαδικασιών για την αποκατάσταση της λειτουργίας των συστημάτων μετά από διακοπή ή βλάβη, ια) μελέτη των στοιχείων για την αποτελεσματικότητα των εγκατεστημένων εφαρμογών εισαγωγής πληροφοριών και η εισήγηση για οργανωτικές βελτιώσεις. Ορισμένες δε από τις προηγούμενες αρμοδιότητες καθώς και άλλες ανατέθηκαν με το άρθρο 89 ν. 3842/2010 σε αυτοτελές Γραφείο Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων και Υποδομών, το οποίο υπάγεται απευθείας στο Γενικό Γραμματέα Πληροφοριακών Συστημάτων, όπως: α) η μέριμνα για την ασφάλεια των πληροφοριακών συστημάτων με την καθιέρωση και

4093/2012 για το Μεσοπρόθεσμο 2013-2016, όπως αυτή προστέθηκε με την περ. 1 υποπαρ.Β.!. της παρ.Β του άρθρου πρώτου του ν. 4152/2013 η Γ.Γ.Π.Σ. συνάπτει μνημόνιο συνεργασίας με τη Γενική Γραμματεία Δημοσίων Εσόδων, στο οποίο καθορίζονται οι υπηρεσίες που παρέχονται από τη Γ.Γ.Π.Σ. στη Γενική Γραμματεία Δημοσίων Εσόδων.

εφαρμογή αρχών, διαδικασιών, τεχνικών και μέτρων προστασίας των δεδομένων και του πληροφοριακού συστήματος από κάθε τυχαία ή σκόπιμη απειλή, β) η σύνταξη προτύπων σχεδιασμού, ανάπτυξης και λειτουργίας πληροφοριακού συστήματος, ασφάλειας και ποιοτικού ελέγχου, γ) η ανάπτυξη του σχεδίου και η παρακολούθηση της υλοποίησης των αναγκαίων μέτρων προστασίας, καθώς και η αποτίμηση του βαθμού αποτελεσματικότητας των μέτρων προστασίας, δ) ο έλεγχος και η διερεύνηση των επεισοδίων ασφάλειας, ε) ο προσδιορισμός των απαιτούμενων ανθρώπινων, οικονομικών, γνωστικών και λοιπών πόρων για την ασφάλεια των πληροφοριακών συστημάτων, στ) η ανάπτυξη σχεδίου ανάκαμψης σε περίπτωση καταστροφής τους. Συμπληρωματικώς, η Απόφαση Δ6Α 1083438ΕΞ2010/22.6.2010 (ΦΕΚ Β 920) του Υπουργού Οικονομικών για τη μεταβίβαση αρμοδιοτήτων και εξουσιοδότηση υπογραφής με εντολή υπουργού στο Γενικό Γραμματέα Πληροφοριακών Συστημάτων, όπως ισχύει, ορίζει ότι ο Γενικός Γραμματέας α) έχει την ευθύνη λειτουργίας της ΓΓΠΣ ως κέντρο δεδομένων του Υπουργείου Οικονομικών και την αρμοδιότητα να εγκαθιστά στους χώρους της ΓΓΠΣ, να λειτουργεί και να υποστηρίζει τεχνικά το σύνολο των κεντρικών υπολογιστών των πληροφοριακών συστημάτων των υπηρεσιών του Υπουργείου και β) καθορίζει την τεχνολογική στρατηγική του Υπουργείου Οικονομικών. Επίσης, η Γ.Γ.Π.Σ. σύμφωνα με τη διάταξη του άρθρου 28 παρ. 4 ν. 3528/2007 (Κώδικας Δημοσίων Υπαλλήλων), μεριμνά για τη μηχανογραφική επεξεργασία των δηλώσεων περιουσιακής κατάστασης και την κατοχύρωση του απόρρητου χαρακτήρα των στοιχείων που περιέχονται σε αυτές.

Από τις εκ του νόμου αρμοδιότητες της Γ.Γ.Π.Σ. συνάγεται ότι η δημόσια αυτή υπηρεσία καθορίζει πρωτοτύπως ουσιώδη στοιχεία του τρόπου της επεξεργασίας που συνάπτονται με την ασφάλεια της επεξεργασίας, δηλαδή θέτει τους στόχους της ασφάλειας των δεδομένων, σχεδιάζει, υλοποιεί και ελέγχει τα τεχνικά και οργανωτικά μέτρα ασφάλειας, προσδιορίζει τους απαιτούμενους οικονομικούς, ανθρώπινους κλπ. πόρους, χωρίς επιπλέον να προβλέπεται ως προς τούτα ο έλεγχος της από άλλη υπηρεσία[5].

Συνεπώς, η Γ.Γ.Π.Σ. είναι κατά τα προεκτεθέντα υπεύθυνος επεξεργασίας κατά την έννοια

[5] Αντιθέτως ο εκτελών την επεξεργασία ελέγχεται από τον υπεύθυνο επεξεργασίας σύμφωνα με τη διάταξη του άρθρου 10 παρ. 4 ν. 2472/1997 σε συνδυασμό με την αντίστοιχη διάταξη του άρθρου 17 παρ. 3 της Οδηγίας 95/46/ΕΚ. Για παράδειγμα, στο προαναφερθέν συμφωνητικό του ελληνικού Δημοσίου με την ΕΛ.ΤΑ. Α.Ε προβλέπονται ειδικά μέτρα εποπτείας εκ μέρους του πρώτου συμβαλλομένου .

του άρθρου 2 στοιχ. ζ) ν. 2472/1997, ανεξαρτήτως αν τα προσωπικά δεδομένα τυγχάνουν επεξεργασίας και από άλλες δημόσιες υπηρεσίες, που καθίστανται υπεύθυνοι επεξεργασίας. Τούτο δεν ανατρέπεται από τη διάταξη του άρθρου μόνον περ. Α. της Απόφασης Δ6Α 1000443ΕΞ2012 (ΦΕΚ Β 33/19-1-2012) του Υπουργού Οικονομικών, η οποία σημειωτέον αντικατέστησε αντιθέτου περιεχομένου διάταξη τριών προηγούμενων υπουργικών αποφάσεων[6], και προβλέπει ότι ο Γενικός Γραμματέας της Γ.Γ.Π.Σ. ορίζεται ως εκτελών την επεξεργασία, εφόσον, όπως αναλυτικώς προεξετέθη, οι αρμοδιότητες μιας υπηρεσίας σχετικά με τον καθορισμό του σκοπού ή/και των ουσιωδών στοιχείων του τρόπου της επεξεργασίας είναι το κρίσιμο στοιχείο για το νομικό χαρακτηρισμό της ως υπευθύνου της επεξεργασίας.

2. Κατά το άρθρο 19 παρ. 1 στοιχ. η) του ν. 2472/1997 «*Η Αρχή έχει τις εξής ιδίως αρμοδιότητες :… η) Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους στο πλαίσιο των οποίων ελέγχονται η τεχνολογική υποδομή και άλλα, αυτοματοποιημένα ή μη, μέσα που υποστηρίζουν την επεξεργασία των δεδομένων. Έχει προς τούτο δικαίωμα προσβάσεως στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο…*». Στην ανωτέρω έννοια των διοικητικών ελέγχων δεν περιλαμβάνονται μόνον οι επιτόπιοι έλεγχοι αλλά και οι έλεγχοι που διεξάγονται μέσω συλλογής στοιχείων με άλλους τρόπους, όπως για παράδειγμα μέσω αλληλογραφίας ή μέσω συναντήσεων με τους ελεγχόμενους φορείς, όπως εν προκειμένω. Επιπλέον, λαμβάνοντας υπόψη στην υπό κρίση περίπτωση την πληθώρα των Πληροφοριακών Συστημάτων που διαχειρίζεται η Γ.Γ.Π.Σ, τον όγκο των δεδομένων που επεξεργάζεται καθώς και την κρισιμότητα αυτών καθίσταται σαφές ότι ο έλεγχος της Αρχής δύναται να είναι συνεχής ώστε η τελευταία να ενημερώνεται ανά τακτά χρονικά διαστήματα για την πρόοδο της Γ.Γ.Π.Σ. ως προς τη λήψη των κατά τα κατωτέρω κατάλληλων μέτρων ασφάλειας.

3. Κατά το άρθρο 10 παρ. 3 του ν. 2472/1997 «*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,*

[6] Άρθρο 2 παρ. 1 της Απόφασης Δ6Α 1083438ΕΞ2010/22.6.2010 (ΦΕΚ Β 920/24-6-2010) του Υπουργού Οικονομικών, όπως τροποποιήθηκε με την Δ6Α 1128876ΕΞ2010 (ΦΕΚ Β 1554/21-9-2010) και την Δ6Α

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...». Ο φορέας της υποχρέωσης, δηλαδή ο υπεύθυνος επεξεργασίας, οφείλει ο ίδιος, όπως προαναφέρθηκε στη σκέψη 1 της παρούσας, να προσδιορίζει την καταλληλότητα των μέτρων με κριτήρια α) τη φύση των δεδομένων, όπως καταρχήν απλά ή ευαίσθητα, χωρίς να αποκλείονται υποπεριπτώσεις αυτών, για παράδειγμα τα προστατευόμενα από ειδικά απόρρητα δεδομένα, και β) την επικινδυνότητα της επεξεργασίας, δηλαδή ιδίως τις επιπτώσεις που ενδέχεται να επιφέρουν στα φυσικά πρόσωπα περιστατικά παραβίασης των δεδομένων.

Καταρχάς η ασφάλεια εξειδικεύεται σε τρεις βασικούς στόχους, ήτοι την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, ενώ συμπληρωματικοί στόχοι, ιδίως από τη σκοπιά της προστασίας των προσωπικών δεδομένων, αποτελούν ιδίως η μη αποποίηση της ευθύνης (ή λογοδοσία) καθώς και ο διαχωρισμός των δεδομένων ανάλογα με το σκοπό της επεξεργασίας. Κατά τα διεθνώς αποδεκτά πρότυπα ασφάλειας πληροφοριακών συστημάτων (π.χ. βλ. σειρά ISO/IEC 27000) τα κατάλληλα μέτρα κατά το άρθρο 10 παρ. 3 ν. 2472/1997 εντάσσονται σε ένα Σύστημα Ασφάλειας Πληροφοριακών Συστημάτων (ISMS). Το εν λόγω Σύστημα προϋποθέτει την εκπόνηση μελέτης επικινδυνότητας με βάση τους κινδύνους και τη φύση των δεδομένων, και μεταξύ άλλων περιλαμβάνει την κατάρτιση πολιτικής και σχεδίων ασφάλειας, όπου προσδιορίζονται συγκεκριμένα τεχνικά και οργανωτικά μέτρα. Τα μέτρα αυτά, εκτός του ότι πρέπει να εφαρμόζονται, επιπλέον παρακολουθούνται και αξιολογούνται με σκοπό τη διαρκή προσαρμογή τους στις επιχειρησιακές ανάγκες του υπευθύνου επεξεργασίας και στις τεχνολογικές εξελίξεις, τις οποίες οφείλει να λαμβάνει υπ΄ όψιν ο υπεύθυνος επεξεργασίας (βλ. άρθρο 17 παρ. 1 Οδηγία 95/46/ΕΚ).

Από το γράμμα και το σκοπό της διάταξης είναι σαφές ότι η υποχρέωση αυτή του υπευθύνου επεξεργασίας 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. Όπως

1073973 ΕΞ2011 (ΦΕΚ Β 1296/16-6-2011).

ήδη έκρινε το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου σχετικά με τα μέτρα της ελεγχόμενης πρόσβασης και καταγραφής των ενεργειών σε ένα πληροφοριακό σύστημα, η έλλειψη τους στοιχειοθετεί παραβίαση της εκπορευόμενης από το άρθρο 8 της ΕΣΔΑ θετικής υποχρέωσης του κράτους να διασφαλίσει το σεβασμό της ιδιωτικής ζωής μέσω της λήψης κατάλληλων μέτρων ασφαλείας, καθώς η ανωτέρω έλλειψη καθιστά αδύνατο τον κατασταλτικό έλεγχο και ως εκ τούτου την ικανοποίηση των δικαιωμάτων του υποκειμένου των δεδομένων, όπως αυτά προβλέπονται κάθε φορά στο εθνικό δίκαιο (βλ. I v. Finland, απόφαση της 17ης Ιουλίου 2008).

4. Η Γ.Γ.Π.Σ. επεξεργάζεται εν γένει δεδομένα προσωπικού χαρακτήρα τόσο απλά όσο και ευαίσθητα κατά την έννοια του άρθρου 2 στοιχ. α) και β) του ν. 2472/1997, για παράδειγμα στο βαθμό που οι δηλώσεις φορολογίας εισοδήματος περιέχουν πεδία για τη φορολόγηση με ειδικό τρόπο (π.χ. ΑΜΕΑ). Ένα σημαντικό μέρος αυτών υπόκειται παράλληλα και στο φορολογικό απόρρητο κατά τη διάταξη του άρθρου 85 παρ. 2 του ν. 2238/1994 (Κώδικας Φορολογίας Εισοδήματος), όπως και η ίδια η Γενική Γραμματεία συνομολογεί (πβλ. σελ. 7, 10, 11, 12, 21 , 22, 23, 25 του πρώτου υπομνήματος). Για παράδειγμα, στο μέτρο που οι δηλώσεις περιουσιακής κατάστασης των δημοσίων υπαλλήλων περιέχουν στοιχεία των φορολογικών δηλώσεων, τα δεδομένα αυτά υπόκεινται επίσης στο φορολογικό απόρρητο. Άλλες κατηγορίες δεδομένων αφορούν τη μισθοδοσία διάφορων υπουργείων, την Ενιαία Αρχή Πληρωμών, το επίδομα πετρελαίου θέρμανσης κ.α. (πβλ. σελ. 26 – 50 του πρώτου υπομνήματος). Από το σύνολο των δεδομένων που τηρεί η Γ.Γ.Π.Σ. είναι δυνατό να εξαχθεί το οικονομικό και περιουσιακό προφίλ κάθε φορολογουμένου στην Ελλάδα. Η χρήση των στοιχείων αυτών από μη εξουσιοδοτημένα πρόσωπα, όπως οι εταιρείες στις οποίες διενεργήθηκαν οι διοικητικοί έλεγχοι καθώς και όσοι τρίτοι προμηθεύθηκαν από τις εταιρείες τα δεδομένα, συνιστά ιδιαίτερα έντονη προσβολή του δικαιώματος στην προστασία των προσωπικών δεδομένων. Συνεπώς, η Γ.Γ.Π.Σ. οφείλει, κατ' εφαρμογή των οριζομένων στο άρθρο 10 παρ. 3 του ν. 2472/1997 να εξασφαλίζει ιδιαίτερα υψηλό επίπεδο ασφάλειας, χωρίς να αποκλείονται διαβαθμίσεις ανάλογα με κάθε κατηγορία δεδομένων, εφόσον αυτά διαχωρίζονται, όπως άλλωστε οφείλει ο υπεύθυνος επεξεργασίας σύμφωνα με τους προεκτεθέντες στόχους της ασφάλειας των δεδομένων (βλ. σκ. 3 της παρούσας). Επιπλέον, στο μέτρο που σε ένα σύστημα

τηρούνται προσωπικά καθώς και άλλα δεδομένα, τα οποία δεν μπορούν να τύχουν ή δεν τυγχάνουν ξεχωριστής επεξεργασίας, τα μέτρα ασφάλειας πρέπει να διαμορφωθούν με γνώμονα τους κανόνες προστασίας των προσωπικών δεδομένων (βλ. Γνώμη 4/2007 της ομάδας εργασίας του άρθρου 29 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», σελ. 29).

5. Ειδικότερα τα δεδομένα, τα οποία κατέστησαν αντικείμενο μη εξουσιοδοτημένης πρόσβασης και περαιτέρω επεξεργασίας συνιστούν προσωπικά δεδομένα, τόσο απλά όσο και ευαίσθητα, και επιπλέον υπόκεινται στο σύνολό τους στο φορολογικό απόρρητο. Το πλήθος και ο χρόνος αναφοράς των δεδομένων υποδεικνύουν ουσιαστικά σειρά αλλεπάλληλων επιμέρους περιστατικών παραβίασης προσωπικών δεδομένων, τουλάχιστον από το 2000 (στοιχεία Ε9) έως και το 2012, τα οποία και μεμονωμένα έχουν ιδιαίτερη έκταση και σοβαρότητα. Τα υφιστάμενα μέτρα ασφάλειας δεν κατέστησαν δυνατή την ανίχνευση και εξιχνίασή τους. Και τούτο, όπως αποδεικνύουν τα πιο πρόσφατα περιστατικά, παρά το γεγονός ότι, μετά το προηγούμενο περιστατικό παραβίασης προσωπικών δεδομένων του έτους 2010, τα μέτρα ασφάλειας, είχαν ενισχυθεί και ειδικώς καταγραφεί σε εγκεκριμένη πολιτική ασφαλείας (ΠΑΠΣ-ΓΓΠΣ), ενώ παράλληλα είχε θεσμοθετηθεί από την 01-11-2011 η λειτουργία αυτοτελούς Γραφείου Ασφάλειας με συναφείς αρμοδιότητες για τον προσδιορισμό των κατάλληλων μέτρων και την εξιχνίαση περιστατικών παραβίασης δεδομένων. Επιπλέον, όπως αναλυτικώς αναφέρεται στο ιστορικό της παρούσας, διαπιστώθηκε ότι μέχρι και σήμερα η πολιτική ασφάλειας δεν εφαρμόζεται πλήρως (βλ. σημείο δ) των διαπιστώσεων στο ιστορικό της παρούσας), και σε αρκετές περιπτώσεις τα εφαρμοζόμενα μέτρα είναι ιδιαιτέρως ελλιπή, συμπεριλαμβανομένων των αντίμετρων ασφάλειας που λήφθηκαν κατόπιν του περιστατικού αφού αυτά αφορούν μόνον στο σύστημα εκτυπώσεων και δεν αποτρέπουν τον κίνδυνο νέου περιστατικού από τα λοιπά συστήματα.

6. Λαμβάνοντας υπόψη τα παραπάνω, 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.

7. Η μη λήψη των κατάλληλων μέτρων ασφάλειας κατά το άρθρο 10 παρ. 3 του ν. 2472/1997, που ήδη οδήγησε σε ιδιαιτέρως εκτεταμένο σε πλήθος και διάρκεια

περιστατικό παραβίασης προσωπικών δεδομένων δικαιολογεί την επιβολή στη Γενική Γραμματεία Πληροφοριακών Συστημάτων, ως υπευθύνου επεξεργασίας, προστίμου, σύμφωνα με τα οριζόμενα στο άρθρο 21 του νόμου αυτού. 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. Εν προκειμένω, όπως αναλυτικώς αναφέρεται στις σκέψεις 5 και 6 της παρούσας πλήθος προσωπικών δεδομένων φορολογικού χαρακτήρα που αφορούν στο σύνολο των φορολογουμένων στην Ελλάδα για τα έτη τουλάχιστον από το 2000 έως και το 2012 κατέστησαν ήδη αντικείμενο παράνομης επεξεργασίας από τρίτους, γεγονός που οφείλεται στην μη ύπαρξη μέχρι και σήμερα κατάλληλων μέτρων ασφάλειας για την αποτροπή, ανίχνευση και διερεύνηση περιστατικών παραβίασης προσωπικών δεδομένων. Δικαιολογείται, συνεπώς, η επιβολή του ανώτερου προβλεπόμενου προστίμου των εκατόν πενήντα χιλιάδων (150.000) Ευρώ.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή :

Επιβάλλει στη Γενική Γραμματεία Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών, ως υπευθύνου επεξεργασίας, πρόστιμο εκατόν πενήντα χιλιάδων (150.000) Ευρώ για την ως άνω διαπιστωθείσα παραβίαση της διάταξης του άρθρου 10 παρ. 3 του ν. 2472/1997.

Καλεί τη Γενική Γραμματεία Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών να εφαρμόζει κατάλληλα μέτρα ασφάλειας, όπως αυτά περιγράφονται στο σημείο 6 του σκεπτικού της παρούσας, και να ενημερώνει την Αρχή κατά τα προβλεπόμενα στο ίδιο σημείο χρονικά διαστήματα.

Ο Πρόεδρος	Η Γραμματέας
Πέτρος Χριστόφορος	Μελπομένη Γιαννάκη