ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 03-08-2016

Αριθ. Πρωτ.: Γ/ΕΞ/4912/03-08-2016

Α Π Ο Φ Α Σ Η ΑΡ. 69/2016

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος στην έδρα της την 30-3-2016 και ώρα 10:00 μετά από πρόσκληση του Προέδρου της σε συνέχεια των από 9-12-2015, 20-1-2016, 10-2-2016, 17-2-2016 και 9-3-2016 συνεδριάσεων, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Πέτρος Χριστόφορος, Πρόεδρος, και τα αναπληρωματικά μέλη Σπυρίδων Βλαχόπουλος, ως εισηγητής, Γρηγόριος Λαζαράκος και Χαράλαμπος Ανθόπουλος, σε αντικατάσταση των τακτικών μελών Λεωνίδα Κοτσαλή, Αναστάσιου–Ιωάννη Μεταξά και Δημητρίου Μπριόλα, αντίστοιχα, οι οποίοι, αν και εκλήθησαν νομίμως εγγράφως δεν παρέστησαν λόγω κωλύματος. Παρόντες χωρίς δικαίωμα ψήφου ήταν οι Φίλιππος Μίτλεττον, νομικός, προϊστάμενος Τμήματος Ελεγκτών και Λεωνίδας Ρούσσος, πληροφορικός ελεγκτής, ως βοηθοί εισηγητές και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Η Α υπέβαλε στην Αρχή την υπ’ αρ. πρωτ. Γ/ΕΙΣ/3958/31-05-2012 καταγγελία κατά του Ταμείου Παρακαταθηκών και Δανείων (εφεξής Ταμείο) η οποία αφορά σε παρακολούθηση εργαζομένου χωρίς προηγούμενη ενημέρωση και κοινοποίηση προσωπικών δεδομένων του στον Σύλλογο Υπαλλήλων του ως άνω Ταμείου.

Με τις με αρ. πρωτ. Γ/ΕΞ/403/25-1-2016, Γ/ΕΞ/407/25-1-2016, Γ/ΕΞ/409/25-1-2016 Γ/ΕΞ/411/25-1-2016 και Γ/ΕΞ/424/25-1-2016 Κλήσεις είχαν κληθεί και παρέστησαν κατά

τη συνεδρίαση της 10-2-2016 η Ανδριανή Κατσαρού, δικαστική πληρεξούσια του Ταμείου Παρακαταθηκών και Δανείων, η καταγγέλλουσα Α, ο Β, Τμηματάρχης του Τμήματος … και ο Γ, Σύμβουλος …του Ταμείου.

Η Αρχή, αφού άκουσε τους εκπροσώπους του καταγγελλόμενου, την καταγγέλλουσα, τους λοιπούς κληθέντες και τους εισηγητές της υπόθεσης, οι οποίοι στη συνέχεια αποχώρησαν, και έλαβε υπόψη όλα τα στοιχεία του φακέλου, μετά και από διεξοδική συζήτηση,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Το άρθρο 4 παρ. 1 εδ. α' του ν. 2472/1997 ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών, ενώ πρέπει να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.

2. Το άρθρο 10 παρ. 3 του ν. 2472/1997 ορίζει 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.

3. Το άρθρο 11 του ν. 2472/97 ορίζει ότι ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία:

α. την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του

β. τον σκοπό της επεξεργασίας.

γ. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων.

δ. την ύπαρξη του δικαιώματος πρόσβασης

4.. Ως περιστατικό παραβίασης προσωπικών δεδομένων θεωρείται κάθε περίπτωση παραβίασης της ασφάλειας των δεδομένων στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια,

αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

5. Από την εξέταση των κληθέντων προσώπων και το σύνολο των εγγράφων του φακέλου της υπόθεσης προέκυψαν τα εξής:

Η Α, υπάλληλος της Διεύθυνσης … του Ταμείου Παρακαταθηκών και Δανείων με την υπ' αρ. πρωτ. Γ/ΕΙΣ/3958/31-05-2012 καταγγελία κατήγγειλε ότι στην υπηρεσία της καταγράφονται και παρακολουθούνται τα επερωτήματα επιλογής (Select queries) που εκτελεί στην Βάση Δεδομένων (ΒΔ) εφαρμογής του Ταμείου από τις 8-12-2011, χωρίς να έχει ενημερωθεί για αυτό, αλλά και ότι η καταγραφή αυτή κοινοποιήθηκε στις αρχές Ιανουαρίου 2012 στα μέλη του Συλλόγου Υπαλλήλων από τον Γ, Σύμβουλο … του Ταμείου, ο οποίος ήταν και μέλος του ΔΣ του Συλλόγου. Η καταγγέλλουσα αναφέρει ότι παρά τις αιτήσεις της για ενημέρωσή της αναφορικά με τον σκοπό της καταγραφής κάτι τέτοιο δεν έχει γίνει, ενώ αναφέρει ότι δεν υπάρχει γραπτή ανάθεση καθηκόντων στην υπηρεσία της. Η καταγγέλλουσα καταγγέλλει ότι αρχικά και συγκεκριμένα από την 8-12-2011, η καταγραφή αφορούσε την αλληλεπίδραση του χρήστη 'hrm' της ΒΔ, που χρησιμοποιείται κατά την προσπέλαση της ΒΔ από τους περίπου 100 χρήστες των εφαρμογών του τμήματός της, με τον χρήστη 'timertpd' που έχει δημιουργηθεί για την εφαρμογή υπολογισμού του ωραρίου, ενώ μετά την 2-1-2012 η καταγραφή αφορούσε ακόμα τον χρήστη 'prs' που έχει δημιουργηθεί για τις εφαρμογές προσωπικού και μισθοδοσίας, καθώς και όλες τις αλληλεπιδράσεις των δύο παραπάνω χρηστών με οποιοδήποτε στοιχείο της ΒΔ. Τέλος, κατήγγειλε την ύπαρξη λογισμικού παρακολούθησης (TightVNC) στον σταθμό εργασίας της.

Η καταγγέλλουσα διαβίβασε στην Αρχή απόσπασμα των πρακτικών με αρ. … της συνέλευσης του ΔΣ του Συλλόγου Υπαλλήλων της 10-1-2012 όπου κλήθηκε για να απαντήσει για τον λόγο παρέμβασής της στην εφαρμογή παρακολούθησης παρουσιών και αδειών του προσωπικού, στα πλαίσια των υπηρεσιακών της καθηκόντων και αν χρησιμοποιεί την συγκεκριμένη εφαρμογή κατόπιν εντολής της Διοίκησης. Όπως προκύπτει από το ως άνω προσκομισθέν Πρακτικό, ο Αντιπρόεδρος του Συλλόγου ανέφερε τα εξής: *«Ο Πρόεδρος του Ταμείου έχει λίστα […] συναδέλφων που δεν τηρούν το ωράριο και αυτή τη λίστα δεν την έχει ζητήσει από τη Διεύθυνση Προσωπικού. Δεν απευθύνθηκε στο Διοικητικό θεσμικά όπως ενδεχομένως θα έπρεπε, αλλά την έχει πάρει από αλλού. Υπάρχει συνάδελφος που έχει πρόσβαση στα στοιχεία του ωραρίου των συναδέλφων και μπαίνει πολλές φορές τη μέρα χωρίς να του έχει ζητηθεί από το Διοικητικό. Θα αφήσω τη Διοίκηση απέξω. Θα κατονομάσω τη συνάδελφο και προτείνω να την καλέσουμε εδώ να μας δώσει*

εξηγήσεις γιατί το κάνει αυτό. Είναι η συνάδελφος Α από τη …». Σε ερώτηση ενός μέλους του ΔΣ του Συλλόγου, ο Ταμίας του Συλλόγου Γ απάντησε ότι *«έχω στοιχεία που αποδεικνύουν ότι ο χρήστης, δηλαδή η Α, μπαίνει καθημερινά, πολλές φορές τη μέρα στο συγκεκριμένο πρόγραμμα με τους δύο κωδικούς που έχει. Δεν δικαιολογείται αυτό. Δεν ξέρω αν κάποιος της το έχει ζητήσει. Συμφωνώ να την καλέσουμε».*. Μετά την εξέταση της καταγγέλλουσας, ο Πρόεδρος του Συλλόγου πρότεινε να κλείσει το θέμα και εφόσον υπάρχουν αποδείξεις, να απευθυνθεί ο Σύλλογος στον Διευθυντή του Ταμείου και τον Προϊστάμενό της ώστε να εξετάσουν εκείνοι ως αρμόδιοι το θέμα.

Στη συνέχεια η καταγγέλλουσα ενημέρωσε την 12-1-2012 σχετικά τον προϊστάμενό της Β με ηλεκτρονικό μήνυμα, όπου του ανέφερε τα εξής: *«Θα ήθελα να σας ενημερώσω ότι στις 10-1-2012 κλήθηκα προφορικά από το ΔΣ του Συλλόγου των εργαζομένων. Μου ζητήθηκε να απαντήσω για ποιο λόγο αλληλεπιδρώ με συγκεκριμένη εφαρμογή που έχω αναπτύξει, στα πλαίσια των υπηρεσιακών καθηκόντων που μου ανατίθενται από το τμήμα μου, και η οποία αφορά το σύστημα παρακολούθησης παρουσιών και αδειών του προσωπικού. Επίσης ερωτήθηκα αν χρησιμοποιώ τη συγκεκριμένη εφαρμογή κατόπιν εντολής της Διοίκησης (!) . Ισχυρίστηκαν ότι γνωρίζουν πόσες φορές τη μέρα μπαίνω σε συγκεκριμένα αρχεία της βάσης δεδομένων και ότι επιβαρύνω τη λειτουργία της βάσης δεδομένων. Θέτω τα ανωτέρω σε γνώση σας και παρακαλώ για τις ενέργειες σας ως άμεσα προϊσταμένου μου. Επιφυλάσσομαι για κάθε δικαίωμα που θίγει την τιμή και την αξιοπρέπεια μου.»*

Ο Β ανέφερε το ζήτημα σε σχετική συνάντηση με τον Διευθυντή … Δ την 13-1-2012, ενώ στην συνέχεια τον πληροφόρησε αναφορικά με τις ανάγκες πρόσβασης στην εφαρμογή παρακολούθησης παρουσιών και αδειών του προσωπικού και ζήτησε να πληροφορηθεί για τους λόγους παρακολούθησης των χρηστών του τμήματός του, αν αυτοί δημιουργούν πρόβλημα για να παρέμβει, ενώ δήλωσε ότι απαγόρεψε κάθε πρόσβαση στους πίνακες του χρήστη timertpd, αναλαμβάνοντας προσωπικά την συντήρηση της εφαρμογής, παρά την εμπιστοσύνη που εξακολουθούσε να διατηρεί προς τους υπαλλήλους του τμήματός του.

Κατόπιν των ανωτέρω, την 23-1-2012, ο Δ απέστειλε το ακόλουθο μήνυμα ηλεκτρονικού ταχυδρομείου προς τους Τμηματάρχες της Διεύθυνσης:

«Θα ήθελα να σας ενημερώσω και να σας παρακαλέσω για τα παρακάτω :

1) Η ανάπτυξη εφαρμογών και τα αντίστοιχα τεστ θα γίνονται στο περιβάλλον ανάπτυξης. Τα όποια αντικείμενα της βάσης (πίνακες ,κ.λ.π) από το περιβάλλον παραγωγής σας είναι αναγκαία θα σας μεταφέρονται από τους αρμόδιους υπαλλήλους του τμήματος

υποστήριξης. Οι ίδιοι άνθρωποι θα σας μεταφέρουν τα αντικείμενα(πίνακες, κ.λ.π) από το περιβάλλον ανάπτυξης στο περιβάλλον παραγωγής. Για πληροφορίες: Ε, Γ, support@tpd.gr.»

Στη συνέχεια η καταγγέλλουσα υπέβαλε τα με αρ. πρωτ. Γ/ΕΙΣ/3959/31-05-2012, Γ/ΕΙΣ/3960/31-05-2012, Γ/ΕΙΣ/4010/01-06-2012, Γ/ΕΙΣ/4011/01-06-2012, Γ/ΕΙΣ/4030/05-06-2012, Γ/ΕΙΣ/4084/06-06-2012, Γ/ΕΙΣ/4155/08-06-2012, Γ/ΕΙΣ/4156/08-06-2012, Γ/ΕΙΣ/4459/21-06-2012, Γ/ΕΙΣ/4647/02-07-2012, Γ/ΕΙΣ/4710/04-07-2012, Γ/ΕΙΣ/5102/24-07-2012, Γ/ΕΙΣ/6601/16-10-2012, Γ/ΕΙΣ/6602/16-10-2012, Γ/ΕΙΣ/7723/30-11-2012, Γ/ΕΙΣ/8291/28-12-2012, Γ/ΕΙΣ/188/14-01-2013, Γ/ΕΙΣ/218/15-01-2013 και Γ/ΕΙΣ/350/18-01-2013 συμπληρωματικά έγγραφα και ηλεκτρονικά πειστήρια, τα οποία περιέχουν ηλεκτρονική αλληλογραφία, στιγμιότυπα οθόνης από τους πίνακες καταγραφής της ΒΔ και φύλλα επεξεργασίας δεδομένων (spreadsheets) με τις καταγεγραμμένες εγγραφές ανά τακτά χρονικά διαστήματα, με τα οποία στοιχειοθετεί τα ισχυριζόμενα στην καταγγελία της. Όπως προκύπτει από τα εν λόγω αρχεία συστήματος, είναι ενεργοποιημένη η καταγραφή των επερωτημάτων επιλογής και ενημέρωσης δεδομένων που εκτελούν οι χρήστες ‘hrm’ και ‘prs’, καθώς και εισαγωγής και διαγραφής του τελευταίου. Επίσης, υπάρχουν καταγεγραμμένα τέτοιου είδους επερωτήματα για τους εν λόγω χρήστες.

Η Αρχή απεύθυνε το με αρ. πρωτ. Γ/ΕΞ/559/28-01-2013 ερώτημα για διευκρινήσεις στο καταγγελλόμενο Ταμείο, το οποίο απάντησε με το με αρ. πρωτ. Γ/ΕΙΣ/1152/18-02-2013 έγγραφό του, μέσω του Διευθυντή …. Σε αυτό αναφέρει ότι οι υπάλληλοι της Διεύθυνσης που ασχολούνται με την ανάπτυξη εφαρμογών και τον προγραμματισμό έχουν απευθείας πρόσβαση στη ΒΔ, εξαιτίας της έλλειψης διαχειριστών της ΒΔ και της ανάπτυξης εφαρμογών σε ειδική γλώσσα προγραμματισμού (Cobol). Ωστόσο, διευκρινίζει ότι οι υπάλληλοι με δικαίωμα πρόσβασης στη ΒΔ θα πρέπει να κάνουν χρήση του δικαιώματος μόνο για συγκεκριμένους λόγους, ενώ απαγορεύεται ρητά η οποιαδήποτε επεξεργασία αντικειμένων της ίδιας της ΒΔ. Επίσης, σημειώνει ότι εκτός των άλλων καταγράφονται οι δικτυακοί τόποι που επισκέπτονται οι υπάλληλοι με ειδικό λογισμικό (Threat Management Gateway της εταιρίας Microsoft). Ως αιτιολόγηση, αναφέρει ότι υπήρξαν περιπτώσεις που συνέβη μη διαθεσιμότητα του εσωτερικού δικτύου και διακοπή συναλλαγής, εξαιτίας υπερβολικής χρήσης του διαθέσιμου εύρους ζώνης κατά το «κατέβασμα» μεγάλων αρχείων από χρήστη, ενώ ισχυρίζεται ότι δεν θα ήταν δυνατό να επιλυθεί το πρόβλημα χωρίς εικόνα των χρηστών που ήταν συνδεδεμένοι στο διαδίκτυο. Στο ανωτέρω έγγραφο το καταγγελλόμενο ισχυρίζεται ότι δεν πραγματοποιείται καταγραφή προσωπικών δεδομένων, παρά μόνον καταγραφή των εντολών που εκτελούν

οι χρήστες στη ΒΔ, χωρίς τα αποτελέσματά τους, ώστε εάν η εντολή δημιουργεί επεξεργαστικό πρόβλημα (απαιτεί μεγάλη υπολογιστική ισχύ ή μνήμη) να εξετασθεί η αιτία του προβλήματος (λανθασμένος συντακτικός τύπος ενέργειας, μη σωστά δομημένος πίνακας, κλπ.). Ως παράδειγμα περιστατικού, αναφέρει ότι δύο υπάλληλοι είχαν εκτελέσει μη σωστά δομημένη εντολή στη ΒΔ με αποτέλεσμα το συγκεκριμένο υποσύστημα του Ταμείου να τεθεί προσωρινά εκτός λειτουργίας. Στο εν λόγω περιστατικό, μέσω της καταγραφής, έγινε αυστηρή υπενθύμιση προς τους υπαλλήλους να μην εκτελούν μη δοκιμασμένες εντολές σε ώρα συναλλαγής, και στην συνέχεια έγιναν οι απαραίτητες ενέργειες και επιλύθηκε το πρόβλημα. Αναφορικά με τα κριτήρια επιλογής των χρηστών οι εντολές των οποίων καταγράφονται, ο υπεύθυνος επεξεργασίας δηλώνει ότι σχετίζονται με την παλαιότητα των εφαρμογών που οι τελευταίοι αναπτύσσουν, καθώς οι παλαιότερες είναι δοκιμασμένες, το είδος της εφαρμογής (Web, client, κτλ.) και το πόσο συχνά παρουσιάζουν προβλήματα.

Επίσης το Ταμείο επικαλείται ότι η καταγγέλλουσα, ως υπάλληλος Πληροφορικής γνωρίζει ότι είναι δυνατός ο έλεγχος των ενεργειών της σε κάθε στιγμή που κρίνεται αναγκαίος για την ασφαλή λειτουργία του Πληροφοριακού Συστήματος. Το Ταμείο αναφέρει, ακόμη, ότι η νομιμότητα της καταγραφής προκύπτει από την εγκύκλιο με αριθμό ΓρΓΓΠ0000110 ΕΞ 2012/20-01-2012 της Γενικής Γραμματείας Πληροφοριακών Συστημάτων, σύμφωνα με την οποία «*Κάθε χρήστης των Πληροφοριακών Συστημάτων (Π.Σ.) του Υπ. Οικονομικών θα πρέπει να [...] γνωρίζει ότι οποιαδήποτε ενέργεια (δηλ. καταχώρηση, μεταβολή, διαγραφή, εμφάνιση ή εκτύπωση στοιχείων) που πραγματοποιείται στα Π.Σ. δύναται να καταγράφεται και μπορεί να αποδοθεί στον υπάλληλο που την πραγματοποίησε*». Η εγκύκλιος αυτή διαβιβάστηκε, εκτός των άλλων, σε όλους τους Προϊσταμένους ων Δ/σεων της Κεντρικής Υπηρεσίας του Ταμείου με το υπ' αρ. πρωτ. 25979/23-2-2012 διαβιβαστικό έγγραφο, με εντολή να λάβουν ενυπόγραφη ενημέρωση από όλους τους υπαλλήλους.

Μετά τις διευκρινίσεις του Ταμείου, η καταγγέλλουσα απέστειλε τα με αρ. πρωτ. Γ/ΕΙΣ/667/31-01-2013, Γ/ΕΙΣ/868/07-02-2013, Γ/ΕΙΣ/1614/05-03-2013, Γ/ΕΙΣ/2008/19-03-2013 και Γ/ΕΙΣ/3062/30-04-2013 έγγραφα, με τα οποία κατήγγειλε την συνέχιση των καταγραφών, την διαγραφή καταγεγραμμένων ενεργειών και την επιλεκτική συνέχιση της καταγραφής για δύο χρήστες της ΒΔ.

Στη συνέχεια η Αρχή απέστειλε το με αρ. πρωτ. Γ/ΕΞ/3162/08-05-2013 έγγραφο στον υπεύθυνο επεξεργασίας, ζητώντας του επιπλέον διευκρινήσεις σχετικά με την ενημέρωση των χρηστών για την καταγραφή των ενεργειών τους στα πληροφοριακά συστήματα του

Ταμείου, τους χρήστες που έχουν δικαίωμα πρόσβασης ή τροποποίησης/διαγραφής στους διαχειριστικούς πίνακες της ΒΔ, τη διαγραφή καταγεγραμμένων ενεργειών άλλων χρηστών, εκτός της συγκεκριμένης υπαλλήλου, την παρακολούθηση των σταθμών εργασίας των χρηστών με ειδικό λογισμικό (π.χ. TightVNC, κτλ) και την ενημέρωση των χρηστών για την καταγραφή των ιστοσελίδων όπου πλοηγούνται στο διαδίκτυο.

Το Ταμείο, μέσω του Διευθυντή Μηχανογράφησης, απάντησε με το με αρ. πρωτ. Γ/ΕΙΣ/3720/30-05-2013 έγγραφο με το οποίο ανέφερε τα εξής:

«1. Δεν γίνεται καταγραφή, αλλά έλεγχος των χρηστών. Οι χρήστες γνωρίζουν ότι υπάρχει η δυνατότητα ελέγχου από τους χειριστές της κεντρικής κονσόλας του συστήματος, αφού σε καθημερινή σχεδόν βάση ζητούν βοήθεια για προβλήματα όπως αδυναμία εισόδου στο σύστημα, ακύρωση εκτύπωσης , «πάγωμα» της οθόνης του χρήστη. και στη συνέχεια ο υπεύθυνος χειριστής της κονσόλας του προσπαθεί με τα εργαλεία του λειτουργικού συστήματος – εν προκειμένω του Unix να δώσει λύση στο πρόβλημα. (η πρώτη ενέργεια των υπευθύνων του τμήματος υποστήριξης στα πλαίσια του λειτουργικού συστήματος Unix είναι να εκτελέσουν την εντολή who για να διαπιστωθεί η ύπαρξη της εισόδου συγκεκριμένου χρήστη στο σύστημα).

Δυνατότητα αναλυτικής καταγραφής των ενεργειών των χρηστών – ημερολόγιο χρηστών θα ήταν χρήσιμη, αλλά δεν υφίσταται λόγω του τρόπου ανάπτυξης των εφαρμογών και λόγω έλλειψης αποθηκευτικού χώρου.

2. Δικαίωμα πρόσβασης η τροποποίησης / διαγραφής στου διαχειριστικούς πίνακες της Βάσης Δεδομένων έχουν ο Σύμβουλος Πληροφορικής ο οποίος εκτελεί χρέη Διαχειριστή της Βάσης Δεδομένων(DBA). Κατά διαστήματα όμως, λόγω και του μεγέθους των αρχείων, το περιεχόμενο των ελέγχων των χρηστών διαγράφονται για να «ελαφρύνει» η Βάση Δεδομένων και να εξοικονομηθεί αποθηκευτικός χώρος. Κάτι τέτοιο έχει γίνει και πρόσφατα μετά από υπόδειξη της εταιρίας που υποστηρίζει την ΒΔ, λόγω έλλειψης αποθηκευτικού χώρου, κατά την διαδικασία λήψης εφεδρικών αντιγράφων.

3. Εκτός από την ενημέρωση που έγινε στους χρήστες κατά την διαδικασία ένταξης τους στο Active Directory για τους υφιστάμενους ελέγχους, τον μήνα Μάρτιο του περασμένου έτους και για σχεδόν τέσσερες μήνες έγινε εκπαίδευση – ενημέρωση των χρηστών της Κεντρικής Υπηρεσίας. Οι εκπαιδευόμενοι ενημερώθηκαν συστηματικά και ολοκληρωμένα για όλα τα θέματα που σχετίζονται με την πληροφορική: Σωστή χρήση των υλικών πληροφορικής(υπολογιστές , εκτυπωτές, κ.λ.π), κανόνες ασφαλείας και ελέγχου, υποχρεώσεις και περιορισμοί, κ.λ.π.

4. Η εγκατάσταση του λογισμικού TighVNC πραγματοποιήθηκε για την ένταξη των χρηστών των δύο κυρίως απομακρυσμένων Καταστημάτων(Θεσσαλονίκη, Πάτρα) στο AD, όπου θεωρήθηκε αναγκαία η ταυτόχρονη απομακρυσμένη συνεργασία χρηστών και υπαλλήλων της Πληροφορικής. Η ύπαρξή του είναι γνωστή σε όλους τους εμπλεκόμενους. Έκτοτε σπάνια χρησιμοποιείται, κυρίως όταν πρόκειται για ανάγκη άμεσης ενημέρωσης των χρηστών για τον τρόπο λειτουργίας κάποιου λογισμικού (όπως συνέβη πριν από οκτώ μήνες όταν οι χρήστες των Καταστημάτων άρχισαν να χρησιμοποιούν το λογισμικό που αφορούσε την εφαρμογή των διαδικασιών για την πρόληψη νομιμοποίησης εσόδων από παράνομες ενέργειες).

5. Όταν δίδεται δικαίωμα πρόσβασης στο διαδίκτυο ενημερώνονται οι χρήστες ότι η χρήση του διαδικτύου πρέπει να αποσκοπεί στην εξυπηρέτηση των υπηρεσιακών αναγκών, ότι οι κινήσεις τους ελέγχονται εγγενώς από το σύστημα, και ότι η επίσκεψη σε πάρα πολλές ιστοσελίδες δεν είναι δυνατή λόγω των κανόνων εξαίρεσης που έχουν τεθεί.»

Το Ταμείο, με το γ' συνημμένο στο παραπάνω έγγραφο, διαβίβασε στην Αρχή σχετικά τις υπογραφές των υπαλλήλων που είχαν λάβει γνώση της εγκυκλίου της ΓΓΠΣ. Οι ημερομηνίες των υπογραφών κυμαίνονταν από τις 8 έως τις 18 Φεβρουαρίου 2013.

Επίσης, το Ταμείο, με το β' συνημμένο στο παραπάνω έγγραφο διαβίβασε στην Αρχή υπηρεσιακό σημείωμα με αρ. πρωτ. 19945/7-2-2013 με το οποίο ενημέρωνε τους υπαλλήλους ότι η χρήση του διαδικτύου επιτρέπεται μόνο για υπηρεσιακούς λόγους.

Στη συνέχεια, η καταγγέλλουσα απέστειλε τα με αρ. πρωτ. Γ/ΕΙΣ/3875/06-06-2013, Γ/ΕΙΣ/4259/21-06-2013 και Γ/ΕΙΣ/5824/12-09-2013 έγγραφα, με τα οποία αναφέρει ότι η επιλεκτική καταγραφή συνεχίζεται

Η Αρχή, στο πλαίσιο της εξέτασης της καταγγελίας, επικοινώνησε την 16-10-2013 τηλεφωνικά με την καταγγέλλουσα, ζητώντας της διευκρινήσεις, αναφορικά με τα καταγγελλόμενα. Η καταγγέλλουσα απάντησε με τις με αρ. πρωτ. Γ/ΕΙΣ/6544/16-10-2013 διευκρινήσεις της, με τις οποίες δήλωσε ότι η ενεργοποίηση της καταγραφής ξεκίνησε από την κατηγορία ενός μέλους του συλλόγου εργαζομένων ότι παραδίδει στοιχεία των εργαζομένων που δεν τηρούν το ωράριο στον Πρόεδρο, προσθέτοντας ότι χρονικά αυτό μπορεί να διαπιστωθεί από τα αντίγραφα ασφαλείας (back up) που παίρνονται καθημερινά στη βάση δεδομένων. Επίσης, ανέφερε ότι δεν ανακοινώθηκε ότι υπήρχε πρόβλημα στην απόδοση της βάσης δεδομένων στους συγκεκριμένους χρήστες και δεν υπάρχει σχετική απόδειξη, ενώ η καταγραφή συνεχίζεται. Η καταγγέλλουσα αναφέρει ότι ο χρήστης lo (λογαριασμός όψεως) του τμήματος έχει πρόσβαση σε χιλιάδες εγγραφές και θα υπήρχε μεγαλύτερη πιθανότητα να δημιουργεί επιβάρυνση ωστόσο δεν καταγράφηκε, ενώ ο

χρήστης prs έχει πρόσβαση σε εκατοντάδες εγγραφές αλλά αφορά σε εφαρμογές προσωπικού. Η καταγγέλλουσα ανέφερε ότι για επαλήθευση της καταγγελλόμενης διαγραφής των υπολοίπων καταγραφών εκτός εκείνων που αφορούν στην παρακολούθησή της, μπορεί να ζητηθεί η μαρτυρία του προϊσταμένου της Β, καθώς και να αποδειχτεί από τα αντίγραφα ασφαλείας.

Τέλος, η καταγγέλλουσα απέστειλε με το με αρ. πρωτ. Γ/ΕΙΣ/7239/14-11-2013 έγγραφο, το καταστατικό του Συλλόγου των Υπαλλήλων του Ταμείου, καθώς και τα με αρ. πρωτ. Γ/ΕΙΣ/7342/18-11-2013, Γ/ΕΙΣ/8036/18-12-2013, Γ/ΕΙΣ/5/02-01-2014 και Γ/ΕΙΣ/2127/02-04-2014 συμπληρωματικά, έγγραφα που τεκμηριώνουν τις αλλαγές στο είδος και την διάρκεια των καταγραφών. Στο πρώτο εξ αυτών, ο προϊστάμενος της καταγγέλλουσας δίνει εντολή για καταγραφή τεχνικών χαρακτηριστικών των σταθμών εργασίας της Διοίκησης, όπως το όνομα χρήστη, η χωρητικότητα της μνήμης και το όνομα του σταθμού, όπως δηλώνεται καθαρά για λόγους διαπίστωσης της δυνατότητας των σταθμών. Με τα επόμενα δύο ανωτέρω συμπληρωματικά, τεκμηριώνεται ότι μετά την μετάπτωση της υποδομής της εφαρμογής από IBM/AIX σε Oracle/Linux, δεν καταγράφονται τα ερωτήματα και συγκεκριμένοι χρήστες. Στο τελευταίο εξ αυτών, υπάλληλος (τμηματάρχης) της διεύθυνσης διαπιστώνει την ύπαρξη λογισμικού παρακολούθησης στον σταθμό εργασίας του και ενημερώνει την Διοίκηση. Κατόπιν αυτού, η διοίκηση ενημερώνει τους χρήστες για την Πολιτική ορθής χρήσης των πληροφοριακών συστημάτων του υπουργείου οικονομικών.

6. Από τα ανωτέρω και ειδικότερα από το από 10-1-2012 Πρακτικό του ΔΣ του Συλλόγου Υπαλλήλων του Ταμείου, προκύπτει ότι ο Γ δεν προσκόμισε κάποιο γραπτό στοιχείο για τα όσα ανέφερε στο ΔΣ για την καταγγέλλουσα ούτε ο Σύλλογος είχε στην κατοχή του κάποιο γραπτό στοιχείο από αυτά που είχε επεξεργασθεί ο Γ υπό την ιδιότητά του ως Σύμβουλου … του Ταμείου. Παρά ταύτα πρέπει να γίνει δεκτό ότι και μόνη η αναφορά από τον Γ προς το ΔΣ του Συλλόγου των ενεργειών της καταγγέλλουσας συνιστά επεξεργασία προσωπικών δεδομένων αυτής, δεδομένων τα οποία μάλιστα εγνώριζε όχι από την ιδιότητά του ως Ταμία του Συλλόγου, αλλά ως Σύμβουλου … του Ταμείου. Όπως δε παγίως γίνεται δεκτό τόσο από τη θεωρία όσο και από τη νομολογία, για τις ενέργειες υπαλλήλου ή προσώπου που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο ανάθεσης έργου από τον υπεύθυνο επεξεργασίας η ευθύνη βαρύνει τον υπεύθυνο επεξεργασίας ο οποίος έχει την υποχρέωση του άρθρου 10 του ν. 2472/12997 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. Ως εκ τούτου πρέπει να γίνει δεκτό ότι έλαβε χώρα διάδοση προσωπικών δεδομένων εργασιακής συμπεριφοράς εργαζομένου από τον Υπεύθυνο Ασφάλειας του Ταμείου στον Σύλλογο Υπαλλήλων του Ταμείου ο οποίος αποτελεί τρίτο νομικό πρόσωπο, ανεξαρτήτως αν τα μέλη του Συλλόγου τυγχάνει να είναι και υπάλληλοι του υπεύθυνου επεξεργασίας. Η οποιαδήποτε διευκρίνιση αναφορικά με τις προσβάσεις και ενέργειες υπαλλήλων που υποπίπτουν στο πεδίο αντίληψης του Υπεύθυνου Ασφάλειας ως ελεγχόμενες, θα έπρεπε να γίνεται υπηρεσιακά και όχι μέσω του Συλλόγου Υπαλλήλων, ανεξαρτήτως αν ο Υπεύθυνος Ασφαλείας τυγχάνει στη συγκεκριμένη περίπτωση και Ταμίας του Συλλόγου.

Σύμφωνα όμως με τη γνώμη ενός μέλους της Αρχής, ακριβώς επειδή η ανακοίνωση των δεδομένων έλαβε χώρα στο πλαίσιο της συνεδρίασης του διοικητικού συμβουλίου του Συλλόγου Υπαλλήλων του Ταμείου, τα μέλη του οποίου συμπίπτουν με τους εργαζόμενους στο Ταμείο, η ανακοίνωση αυτή έλαβε χώρα στον ίδιο στενό κύκλο προσώπων τα οποία αποτελούν ταυτόχρονα τόσο μέλη του Σωματείου όσο και υπαλλήλους του Ταμείου και περαιτέρω, μετά τις εξηγήσεις της καταγγέλλουσας, μέλους επίσης του Συλλόγου, δεν εδόθη περαιτέρω συνέχεια, αλλά το γεγονός παρέμεινε εντός του πλαισίου των παρόντων υπαλλήλων μελών του Συλλόγου κατά τη συγκεκριμένη συνεδρίαση, το οποίο μπορεί να θεωρηθεί ότι παρέμεινε ως εσωτερικό ζήτημα του Συλλόγου στα πλαίσια καλής λειτουργίας του πληροφοριακού του συστήματος του Ταμείου. Δηλαδή, κατ' αυτόν τον τρόπο δεν μπορεί να θεωρηθεί ότι από ουσιαστική άποψη έλαβε χώρα διάδοση δεδομένων προς τρίτους.

7. Περαιτέρω, οι ενέργειες του υπεύθυνου ασφαλείας με τις οποίες καταγραφόταν η δραστηριότητα της καταγγέλλουσας έγιναν στο πλαίσιο των ορισμένων σε αυτόν αρμοδιοτήτων και δεν συνιστούν παρακολούθηση εργαζομένου. Ωστόσο, προκύπτει ότι ο υπεύθυνος επεξεργασίας δεν είχε ενημερώσει με τρόπο πρόσφορο και σαφή τα υποκείμενα των όποιων η εργασιακή συμπεριφορά καταγραφόταν για τον σκοπό της καταγραφής, τους αποδέκτες των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης. Στα υποκείμενα των δεδομένων περιλαμβάνονται οι υπάλληλοι του Ταμείου που χρησιμοποιούν τους λογαριασμούς χρηστών της ΒΔ, των οποίων οι κινήσεις καταγράφονταν. Ειδική αναφορά ώφειλε να γίνει προς τους υπάλληλους του Τμήματος Μηχανογράφησης που χρησιμοποιούσαν τους εν λόγω χρήστες και των όποιων τα επερωτήματα που εκτελούσαν στις εφαρμογές του Ταμείου καταγράφονταν.

8. Τέλος, όσον αφορά την επεξεργασία προσωπικών δεδομένων από το Ταμείο, προκύπτουν τα εξής:

α) Ενώ το Ταμείο επικαλείται ότι το μέτρο της καταγραφής των ενεργειών των χρηστών στις εφαρμογές του ήταν απαραίτητο για την εξασφάλιση της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας του πληροφοριακού του συστήματος, δεν είχε εφαρμόσει ανάλογα προληπτικά μέτρα ασφάλειας (π.χ. λεπτομερή διαβάθμιση χρηστών, φίλτρα επεξεργασίας επερωτημάτων, διαχωρισμό περιβάλλοντος ανάπτυξης, δοκιμών και παραγωγής των εφαρμογών, κτλ.) που να εμποδίζουν την προσβολή της ασφάλειας, ώστε η εκτενής καταγραφή ενεργειών των χρηστών να καθίσταται ήσσονος σημασίας για την επίτευξη του σκοπού της προστασίας του εν λόγω αγαθού.

β) Το Ταμείο, ως υπεύθυνος επεξεργασίας, δεν είχε ενημερώσει με τρόπο πρόσφορο και σαφή τους υπαλλήλους του για την καταγραφή των ιστοσελίδων στις οποίες πλοηγούνται.

γ) Στους περισσότερους υπολογιστές της κεντρικής Υπηρεσίας, αλλά και καταστημάτων, του Ταμείου είναι εγκατεστημένο λογισμικό παρακολούθησης σταθμού εργασίας τύπου «Εικονικού Δικτυακού Υπολογισμού» (Virtual Network Computing - VNC), το οποίο προβάλει σε απομακρυσμένο χρήστη το ηλεκτρονικό περιβάλλον εργασίας και τις κινήσεις του χρήστη, στον σταθμό εργασίας του οποίου έχει εγκατασταθεί, χωρίς κάτι τέτοιο να απαιτείται. Το Ταμείο, ως υπεύθυνος επεξεργασίας, δεν είχε ενημερώσει με τρόπο πρόσφορο και σαφή τους υπαλλήλους στους σταθμούς εργασίας των οποίων είχε εγκατασταθεί λογισμικό παρακολούθησης, για το γεγονός ότι η λειτουργία του σταθμού τους δύναται να παρακολουθείται.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή :

1. Απευθύνει προειδοποίηση βάσει του άρθρου 21 παρ. 1 στοιχ. α’ του ν. 2472/1997 στο Ταμείο Παρακαταθηκών και Δανείων, ως υπεύθυνο επεξεργασίας, να λαμβάνει όλα τα αναγκαία μέτρα για την ασφάλεια των δεδομένων ώστε να αποφεύγεται η μη νόμιμη διαβίβαση προσωπικών δεδομένων σε τρία μη δικαιούμενα φυσικά ή νομικά πρόσωπα.

2.. Καλεί το Ταμείο Παρακαταθηκών και Δανείων, ως υπεύθυνο επεξεργασίας να συμμορφωθεί με τις ακόλουθες συστάσεις και να ενημερώσει για την εφαρμογή τους την Αρχή εντός τριών (3) μηνών από την κοινοποίηση της παρούσας Απόφασης:

α. Ο υπεύθυνος επεξεργασίας οφείλει να εκπονήσει μελέτη επικινδυνότητας ασφαλείας, με βάση την οποία θα σχεδιάσει και θα υλοποιήσει τα κατάλληλα μέτρα ασφαλείας που θα μεγιστοποιήσουν την ασφάλεια του πληροφοριακού του συστήματος.

β. Ειδικά, ως αποτέλεσμα και της μελέτης, ο υπεύθυνος επεξεργασίας οφείλει να αναθεωρήσει την πολιτική καταγραφής ενεργειών των χρηστών στις εφαρμογές και τις ΒΔ, ώστε αυτή να είναι η ελάχιστη που απαιτείται για τον εν λόγω σκοπό, σε συνδυασμό με την ανάπτυξη κατάλληλων προληπτικών μέτρων ασφάλειας, όπως παρουσιάστηκε στο σκεπτικό της παρούσης.

γ. Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει με τρόπο πρόσφορο και σαφή τα υποκείμενα, των οποίων οι ενέργειες στις εφαρμογές και τις ΒΔ καταγράφονται για τον σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης.

δ. Στο πλαίσιο της ως άνω μελέτης, ο υπεύθυνος επεξεργασίας οφείλει να επανεξετάσει την αναγκαιότητα καταγραφής των ιστοσελίδων των χρηστών. Απαγορεύεται η γενική, συστηματική και προληπτική συλλογή και καταχώριση των δεδομένων που αφορούν τις επισκέψεις που αναφέρονται παραπάνω. Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει με τρόπο πρόσφορο και σαφή τους υπαλλήλους του για την καταγραφή των ιστοσελίδων στις οποίες πλοηγούνται. Επίσης, σύμφωνα με την οδηγία 115/2001 της Αρχής, ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει προσιτά στους εργαζόμενους τηλεπικοινωνιακά μέσα για τις προσωπικές επικοινωνίες τους.

ε. Απαγορεύεται η εγκατάσταση και χρήση λογισμικού παρακολούθησης σταθμού εργασίας τύπου VNC (π.χ. TightVNC) σε μόνιμη βάση και σε κάθε περίπτωση χωρίς την σύμφωνη γνώμη του εργαζομένου. Στα πλαίσια των αρχών της αναγκαιότητας και αναλογικότητας της επεξεργασίας, ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόσει εναλλακτικές μεθόδους υποστήριξης των χρηστών. Λόγω της φύσεως της σχέσεως απασχόλησης αλλά και της έντασης της προσβολής, σύμφωνα και με την Οδηγία 115/2001 της Αρχής, οι εκπρόσωποι των εργαζομένων πρέπει να ενημερώνονται και να διατυπώνουν γνώμη πριν από την εισαγωγή μεθόδων ελέγχου και παρακολούθησης των εργαζομένων, όπως αυτός. Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει με τρόπο πρόσφορο και σαφή τους υπαλλήλους στους σταθμούς εργασίας των οποίων είχε εγκατασταθεί λογισμικό παρακολούθησης, για το γεγονός ότι η λειτουργία του σταθμού τους δύναται να παρακολουθείται.

.

Ο Πρόεδρος **Η γραμματέας**

Πέτρος Χριστόφορος **Ειρήνη Παπαγεωργοπούλου**