ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 05-02-2014

Αριθ. Πρωτ.: Γ/ΕΞ/761/05-02-2014

Α Π Ο Φ Α Σ Η 17/2014

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε σε σύνθεση Τμήματος, στην έδρα της, την 14.01.2014 και ώρα 10:00, μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν ο Αν. Πρόεδρος της Αρχής, Γεώργιος Μπατζαλέξης, κωλυομένου του Προέδρου Πέτρου Χριστόφορου και τα αναπληρωματικά μέλη Σπυρίδων Βλαχόπουλος, Γρηγόριος Λαζαράκος, ως εισηγητής 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. Παρούσες χωρίς δικαίωμα ψήφου ήταν οι Α. Μπούρκα ειδική επιστήμονας - πληροφορικός και η Ε. Μαραγκού, ειδική επιστήμονας - δικηγόρος, ως βοηθοί εισηγητού και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη τα ακόλουθα:

Το Κέντρο Μελετών Ασφαλείας (ΚΕΜΕΑ) και η εταιρεία παροχής υπηρεσιών ασφαλείας G4S TELEMATIX ΑΕ, εταίροι στο χρηματοδοτούμενο από το ΕΣΠΑ έργο ΒΙΟΤΑΥΤΟΤΗΤΑ (Ασφαλείς και Ανακλήσιμες Βιομετρικές Ταυτότητες για Χρήση σε Περιβάλλοντα Διάχυτης Νοημοσύνης), ζήτησαν, με την υπ. αρ. πρωτ. ΓΝ/ΕΙΣ/1437/208-10-2013 γνωστοποίησή τους, την άδεια της Αρχής για την λειτουργία δύο πιλοτικών εφαρμογών πειραματικού βιομετρικού συστήματος ελέγχου

πρόσβασης σε εγκαταστάσεις αποκλειστικά για ερευνητικό σκοπό και για περιορισμένο χρονικό διάστημα.

Σύμφωνα με την ανωτέρω γνωστοποίηση, το έργο ΒΙΟΤΑΥΤΟΤΗΤΑ στοχεύει στην ανάπτυξη μίας μεθόδου πολυτροπικής (multimodal) βιομετρίας, η οποία στηρίζεται στο συνδυασμό βιομετρικών δεδομένων που εξάγονται μέσω πολλαπλών φυσικών χαρακτηριστικών του ατόμου, καθώς και χαρακτηριστικών που σχετίζονται με τη συμπεριφορά του ή/και τις αντιδράσεις του σε συγκεκριμένα εξωτερικά ερεθίσματα («συμπεριφορικά» χαρακτηριστικά). Ειδικότερα, η τελική «βιομετρική υπογραφή» του ατόμου παράγεται βάσει των στατικών και δυναμικών χαρακτηριστικών του προσώπου (π.χ. μορφασμοί, γκριμάτσες), του τρόπου βαδίσματος, καθώς και φυσικών ή άλλων χαρακτηριστικών που σχετίζονται με την εξωτερική του εμφάνιση (π.χ. ύψος, βάρος, χρώμα ματιών, χρώμα μαλλιών, μουστάκι, γυαλιά, κλπ). Η παραπάνω μέθοδος εξετάζεται πειραματικά ως εναλλακτική/συμπληρωματική των συνήθων βιομετρικών πρακτικών (π.χ. βάσει δακτυλοσκόπησης, ιριδοσκόπησης ή γεωμετρίας προσώπου) με στόχο την αποδοτικότερη και ακριβέστερη εξαγωγή και χρήση βιομετρικών δεδομένων κατά την χρήση τους ιδίως σε συστήματα ελέγχου πρόσβασης σε κρίσιμες εγκαταστάσεις με ιδιαίτερα υψηλές απαιτήσεις ασφαλείας.

Η λειτουργία των δύο πιλοτικών εφαρμογών, στο πλαίσιο του έργου ΒΙΟΤΑΥΤΟΤΗΤΑ, θα γίνει, σύμφωνα με τη γνωστοποίηση, με σκοπό τη δοκιμή της ανωτέρω πειραματικής μεθόδου, ώστε να διερευνηθούν τυχόν σφάλματα ή προβλήματα κατά την χρήση της. Οι δοκιμές θα γίνουν με την προσομοίωση συγκεκριμένων σεναρίων χρήσης σε προκαθορισμένους ειδικούς χώρους των ΚΕΜΕΑ και G4S TELEMATIX ΑΕ, οι οποίοι θα διαμορφωθούν κατάλληλα ώστε να προσομοιάζουν πραγματικούς χώρους υψηλής ασφάλειας (ψευδοχώροι). Η δοκιμαστική λειτουργία του βιομετρικού συστήματος, στο πλαίσιο των δύο πιλοτικών εφαρμογών, θα έχει ως εξής: κατά τη φάση της εγγραφής στο βιομετρικό σύστημα, οι συμμετέχοντες στο πείραμα θα κληθούν -υπό την καθοδήγηση της ερευνητικής ομάδας του έργου- να εκτελέσουν συγκεκριμένες καθημερινές ενέργειες (π.χ. βάδισμα, χειρισμός του πίνακα ελέγχου, κ.α). Το σύστημα, βάσει της προαναφερθείσας μεθόδου πολυτροπικής βιομετρίας, θα εξάγει στη συνέχεια τα αντίστοιχα βιομετρικά δεδομένα (π.χ. από τα δυναμικά χαρακτηριστικά του προσώπου, τον τρόπο βαδίσματος, κλπ) και θα παράγει τις «βιομετρικές υπογραφές» των συμμετεχόντων. Τα πρωτογενή δεδομένα (π.χ. εικόνες, σήματα από ανιχνευτές βαδίσματος, κ.α.) θα καταστρέφονται αμέσως μετά από την παραγωγή των

«βιομετρικών υπογραφών». Οι «βιομετρικές υπογραφές» θα αποθηκεύονται, αφού πρώτα κρυπτογραφηθούν, σε έξυπνες κάρτες, καθώς και σε βάση δεδομένων, μαζί με τα κωδικοποιημένα στοιχεία ταυτοποίησης των συμμετεχόντων. Τα τελευταία θα προέρχονται από ειδικές φόρμες που συμπληρώνουν οι συμμετέχοντες πριν από την έναρξη της πιλοτικής δοκιμής (και περιέχουν στοιχεία όπως π.χ. ηλικία, θέση εργασίας, φυσικά χαρακτηριστικά, κ.α.). Στη συνέχεια, για τις ανάγκες των πιλοτικών εφαρμογών, οι συμμετέχοντες στα πειράματα θα κληθούν να προσομοιώσουν περιπτώσεις εισόδου στους συγκεκριμένους χώρους των πιλοτικών, καθώς και στον εγκατεστημένο λογικό εξοπλισμό, ώστε να ελεγχθεί η εγκυρότητα και αποδοτικότητα των «βιομετρικών υπογραφών» ως μέσων ταυτοποίησης.

Η δοκιμή της πιλοτικής εφαρμογής στον χώρο του ΚΕΜΕΑ θα γίνει με συμμετοχή υπαλλήλων του Υπουργείου Δημόσιας Τάξης, ενώ η δοκιμή της πιλοτικής εφαρμογής στον χώρο της εταιρείας G4S TELEMATIX A.E. θα γίνει με συμμετοχή υπαλλήλων της ίδιας της εταιρείας. Και στις δύο περιπτώσεις η συμμετοχή των υπαλλήλων είναι σε εθελοντική βάση και θα γίνει μετά από κατάλληλη ενημέρωσή τους και εφόσον έχουν εκ των προτέρων δηλώσει τη ρητή και ειδική συγκατάθεσή τους (αντίγραφα του εντύπων ενημέρωσης και λήψης συγκατάθεσης έχουν υποβληθεί μαζί με την γνωστοποίηση).

Το συνολικό χρονικό διάστημα διεξαγωγής των δοκιμών και ανάλυσης των αποτελεσμάτων στο πλαίσιο λειτουργίας των πιλοτικών εφαρμογών θα είναι δέκα (10) ημέρες. Μετά το πέρας του ανωτέρω χρονικού διαστήματος όλα τα δεδομένα του πιλοτικού συστήματος (κάρτες, βάσεις δεδομένων, φόρμες με προσωπικά δεδομένα συμμετεχόντων) θα καταστραφούν. Τυχόν περαιτέρω επεξεργασία των αποτελεσμάτων των πειραμάτων θα γίνονται μόνο με ανώνυμα δεδομένα.

Η Αρχή, μετά από εξέταση των στοιχείων της υπόθεσης, αφού άκουσε τον εισηγητή και τις βοηθούς εισηγητού, οι οποίες στη συνέχεια αποχώρησαν, κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Το άρθρο 2 του ν. 2472/1997, ορίζει ότι «δεδομένα προσωπικού χαρακτήρα» είναι «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων». «Υποκείμενο των δεδομένων» είναι «το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί,

δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική». Όπως έχει κατ' επανάληψη κρίνει η Αρχή με προηγούμενες αποφάσεις της, τα βιομετρικά δεδομένα αποτελούν δεδομένα προσωπικού χαρακτήρα καθώς μπορούν να θεωρηθούν τόσο ως περιεχόμενο πληροφοριών που χαρακτηρίζει συγκεκριμένες βιολογικές ιδιότητες, φυσιολογικά χαρακτηριστικά ή/και προσωπικά γνωρίσματα που είναι μοναδικά για ένα άτομο, όσο και ως στοιχείο αντιστοίχισης μιας πληροφορίας με το άτομο αυτό και κατ' επέκταση ως στοιχείο αναγνώρισης του εν λόγω ατόμου.

2. Στην περίπτωση του έργου ΒΙΟΤΑΥΤΟΤΗΤΑ, οι δύο πιλοτικές εφαρμογές αποτελούνται από πειραματικό βιομετρικό σύστημα ελέγχου πρόσβασης. Για την πρώτη πιλοτική εφαρμογή υπεύθυνος επεξεργασίας είναι το ΚΕΜΕΑ, ενώ για τη δεύτερη η εταιρεία G4S TELEMATIX Α.Ε. Κατά την λειτουργία των πιλοτικών εφαρμογών, πραγματοποιείται, σύμφωνα με τα παραπάνω, επεξεργασία προσωπικών δεδομένων των συμμετεχόντων στις δοκιμές και ειδικότερα βιομετρικών τους δεδομένων που βασίζονται στον συνδυασμό πολλαπλών φυσικών και «συμπεριφορικών» τους χαρακτηριστικών. Επίσης, στο πλαίσιο διεξαγωγής των ερευνητικών δοκιμών, τηρούνται ειδικά έντυπα με προσωπικά δεδομένων των συμμετεχόντων (προσωπικά στοιχεία, επαγγελματική κατάσταση, προσωπικά χαρακτηριστικά), τα οποία συμπληρώνουν οι ίδιοι πριν από την έναρξη των πειραμάτων.

3. Σύμφωνα με το αρ. 4 παρ. 1 του ν. 2472/1997, κριτήριο για τη νομιμότητα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι η αρχή της αναλογικότητας, κατά την οποία πρέπει κάθε φορά να εξετάζεται αν η επεξεργασία των συγκεκριμένων δεδομένων είναι αναγκαία για τον επιδιωκόμενο σκοπό, ο οποίος δεν μπορεί να επιτευχθεί με λιγότερο επαχθή για το πρόσωπο μέσα. Ειδικότερα, τα προσωπικά δεδομένα πρέπει α) να συλλέγονται με τρόπο θεμιτό και νόμιμο, για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών, β) να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας, γ) να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση και δ) να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των

υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την πραγματοποίηση το σκοπού της επεξεργασίας.

Στο πλαίσιο του έργου ΒΙΟΤΑΥΤΟΤΗΤΑ, ο σκοπός της επεξεργασίας των δύο πειραματικών βιομετρικών συστημάτων είναι αποκλειστικά η επιστημονική έρευνα με ειδικότερο αντικείμενο την εξέταση μεθόδου πολυτροπικής βιομετρίας βάσει φυσικών και «συμπεριφορικών» χαρακτηριστικών του ατόμου. Λαμβάνοντας υπόψη α) τον παραπάνω ερευνητικό χαρακτήρα του σκοπού που έχει ως απώτερο στόχο την βελτίωση της αποδοτικότητας και ακρίβειας των βιομετρικών συστημάτων όταν αυτά χρησιμοποιούνται σε πραγματικές συνθήκες, β) το γεγονός ότι η αποδοτικότητα και η ακρίβεια είναι σημαντικοί παράγοντες της αποτελεσματικής λειτουργίας των βιομετρικών συστημάτων, τα οποία σε ορισμένες περιπτώσεις ιδιαίτερα κρίσιμων εγκαταστάσεων και υποδομών μπορεί να κριθούν ως απαραίτητα μέσα για την προάσπιση της ασφάλειας προσώπων και αγαθών, και γ) το γεγονός ότι τα δεδομένα των πιλοτικών διατηρούνται για διάστημα αποκλειστικά δέκα (10) ημερών, μετά από το οποίο καταστρέφονται, κρίνεται ότι η παραπάνω αρχή της αναλογικότητας ικανοποιείται. Κατά τον τρόπο αυτό έχει, άλλωστε, κρίνει η Αρχή και στο παρελθόν τη νομιμότητα λειτουργίας συναφών βιομετρικών συστημάτων αποκλειστικά για ερευνητικό σκοπό (βλ. αποφάσεις 27/2010 και 31/2010).

4. Επισημαίνεται ότι σε συνθήκες πραγματικής λειτουργίας (δηλαδή αν ο σκοπός δεν ήταν πια ερευνητικός αλλά αφορούσε π.χ. τον έλεγχο πρόσβασης σε εγκαταστάσεις), η νομιμότητα της παραπάνω επεξεργασίας θα έπρεπε να επανεξεταστεί βάσει του αρ. 4 του ν. 2472/1997, λαμβάνοντας υπόψη τα εξής κριτήρια: i) την κρισιμότητα και τις απαιτήσεις ασφαλείας των συγκεκριμένων εγκαταστάσεων, ii) την επεμβατικότητα στην ιδιωτική ζωή της επιλεγμένης βιομετρικής μεθόδου σε σχέση με άλλες (π.χ. δακτυλοσκόπηση, ιριδοσκόπηση, κλπ), και iii) την χρήση μοντέλων φιλικών προς την ιδιωτικότητα για την αρχιτεκτονική του βιομετρικού συστήματος (π.χ. αποθήκευση σε κάρτα, κρυπτογράφηση των βιομετρικών δεδομένων). Με βάσει τα κριτήρια αυτά, άλλωστε, η Αρχή έχει ήδη εξετάσει εφαρμογές βιομετρικών συστημάτων σε πραγματικές συνθήκες και ιδίως συστημάτων για τον έλεγχο πρόσβασης εργαζομένων σε εγκαταστάσεις και σε ορισμένες περιπτώσεις έχει επιβάλει τη διακοπή της λειτουργίας τους, ως υπερβαίνουσα το σκοπό της επεξεργασίας (βλ. αποφάσεις 245/9/2000, 52/2003, 50/2007, 74/2009, 127/2012), ενώ σε άλλες έχει επιτρέψει την λειτουργία τους υπό όρους (βλ. αποφάσεις 9/2003, 52/2008, 56/2009). Στην προκειμένη περίπτωση τα

ανωτέρω κριτήρια δεν εξετάστηκαν διεξοδικά, καθώς η λειτουργία γίνεται βάσει σεναρίων προσομοίωσης και όχι σε πραγματικές συνθήκες. Ενδεικτικά αναφέρεται, ως προς την αποθήκευση των βιομετρικών δεδομένων, ότι σε συνθήκες πραγματικής λειτουργίας ο προσφορότερος τρόπος θα ήταν τοπικά σε έξυπνες κάρτες (και όχι σε βάση δεδομένων) που παρέχουν στα υποκείμενα των δεδομένων μεγαλύτερη δυνατότητα ελέγχου των προσωπικών τους δεδομένων. Στις υπό εξέταση συνθήκες πιλοτικής δοκιμής, όμως, δεν μπορεί να θεωρηθεί η επεξεργασία των δεδομένων σε κεντρική βάση ως μη πρόσφορος τρόπος, καθώς αυτή αποτελεί απαραίτητη προϋπόθεση για την διεξαγωγή της έρευνας, με την προϋπόθεση ότι ο υπεύθυνος επεξεργασίας λαμβάνει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των δεδομένων, σύμφωνα το αρ. 10 του ν. 2472/1997.

5. Η επεξεργασία δεδομένων στο πλαίσιο των δύο πιλοτικών βιομετρικών συστημάτων πραγματοποιείται κατά το άρθρ. 5 παρ. 1 του ν. 2472/1997, με τη συγκατάθεση των υποκειμένων των δεδομένων. Σύμφωνα δε, με το αρ. 2 του ν. 2472/1997 ως συγκατάθεση νοείται «κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως που εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο της επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν». Στην περίπτωση του έργου ΒΙΟΤΑΥΤΟΤΗΤΑ, τα υποκείμενα των δεδομένων συμμετέχουν εθελοντικά στις πιλοτικές δοκιμές. Επίσης, οι δοκιμές πραγματοποιούνται σε ειδικούς ψευδοχώρους που δεν αποτελούν πραγματικούς χώρους εργασίας, ενώ το πιλοτικό σύστημα δεν θα αντικαταστήσει τα υπάρχοντα συστήματα ελέγχου πρόσβασης των υπεύθυνων επεξεργασίας. Η συγκατάθεση δηλώνεται μέσω ειδικών εντύπων που παρέχουν και τη βασική ενημέρωση των συμμετεχόντων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων στο πλαίσιο των πιλοτικών εφαρμογών.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή αποφαίνεται ότι η εγκατάσταση του παραπάνω βιομετρικού συστήματος αποκλειστικά για ερευνητικούς σκοπούς δεν αντίκειται στις διατάξεις του ν.2472/1997, εφόσον τηρούνται οι παρακάτω όροι:

1. Οι υπεύθυνοι επεξεργασίας (ΚΕΜΕΑ, G4S TELEMATIX Α.Ε) οφείλουν να εφαρμόζουν όλα τα απαιτούμενα μέτρα γα το απόρρητο και την ασφάλεια της

επεξεργασίας, σύμφωνα με το άρθρο 10 ν. 2472/1997. Προς τούτο, θα πρέπει να αναπτύξουν πολιτική και σχέδιο ασφαλείας και να τα υποβάλουν στην Αρχή πριν από την έναρξη των πιλοτικών εφαρμογών.

2. Οι υπεύθυνοι επεξεργασίας οφείλουν να ενημερώσουν την Αρχή για την καταστροφή των βιομετρικών δεδομένων, καθώς και των λοιπών προσωπικών δεδομένων που έχουν συλλεχθεί στο πλαίσιο λειτουργίας των δύο πιλοτικών συστημάτων, μετά το πέρας της περιόδου των δέκα (10) ημερών που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Η ενημέρωση πρέπει να γίνει εντός δεκαπέντε (15) ημερών από την πραγματοποίησή της, επισυνάπτοντας και το σχετικό πρωτόκολλο καταστροφής.

3. Τα έντυπα ενημέρωσης πρέπει να τροποποιηθούν κατάλληλα ώστε να αναφέρουν με μεγαλύτερη σαφήνεια για το κάθε πιλοτικό την ταυτότητα του υπεύθυνου επεξεργασίας, τον σκοπό της επεξεργασίας, τις κατηγορίες των προσωπικών δεδομένων που υφίστανται επεξεργασία, καθώς και τον τρόπο με τον οποίο τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματα πρόσβασης και αντίρρησής τους, σύμφωνα με τα άρθρα 12 και 13 αντίστοιχα του ν. 2472/1997. Στα έντυπα πρέπει να αναφέρεται ρητά ότι δεν υπάρχουν αποδέκτες των δεδομένων πλην των εξουσιοδοτημένων υπαλλήλων των υπεύθυνων επεξεργασίας.

4. Απαγορεύεται η οποιαδήποτε επέκταση λειτουργιών ή άλλη τεχνική αλλαγή ή μεταβολή διαδικασιών σχετικά με την εφαρμογή και λειτουργία του βιομετρικού συστήματος, χωρίς προηγούμενη ενημέρωση και έγκριση της Αρχής.

Ο Πρόεδρος **Η Γραμματέας**

Γεώργιος Μπατζαλέξης **Ειρήνη Παπαγεωργοπούλου**