



ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Τρόπος αποστολής: Συστημένο

Δ/ση Γραμματείας - Τμήμα Ελεγκτών
Πληροφορίες : Ευφροσύνη Σιουγλέ,
Ιωάννης Λυκοτραφίτης
Λεωνίδας Ρούσσος
Κωνσταντίνος Λιμνιώτης
Τηλέφωνο : 2106475670-675-673-672
Email : sefrosini@dpa.gr
ilykotrafitis@dpa.gr
lroussos@dpa.gr
klimniotis@dpa.gr

Αθήνα, 25-11-2013

Αριθ. Πρωτ.: Γ/ΕΞ/233-1/25-11-2013

Προς

Μ. ΠΑΥΛΑΚΗΣ – Χ. ΜΟΣΧΟΣ
& ΣΥΝΕΡΓΑΤΕΣ

Φίλωνος 66 & Παλιάς Μεραρχίας
18535, Πειραιάς

(Πληρεξούσιοι των Ιατρικών Συλλόγων

Αργολίδος και Πατρών)

**ΘΕΜΑ: Επίπεδα ασφάλειας και άδεια του Συστήματος Ηλεκτρονικής
Συνταγογράφησης**

Σχετικό: Υπ' αριθμ. πρωτ. Γ/ΕΙΣ/233/16-01-2013 έγγραφό σας

Σε απάντηση του ανωτέρω σχετικού εγγράφου σας, με το οποίο παραθέτετε πλήθος ερωτημάτων αναφορικά με την υφιστάμενη κατάσταση της άδειας ίδρυσης και λειτουργίας αρχείου που έχει εκδώσει η Αρχή για το Σύστημα Ηλεκτρονικής Συνταγογράφησης, καθώς και με τα επίπεδα ασφαλείας αυτού, σας ενημερώνουμε για τα εξής:

Σύμφωνα με το άρθρο 6 του ν. 3892/2010, η Γενική Γραμματεία Κοινωνικών Ασφαλίσεων (εφεξής ΓΓΚΑ) είναι υπεύθυνη για τη δημιουργία και λειτουργία της βάσης δεδομένων της ηλεκτρονικής συνταγογράφησης. Περαιτέρω, ο φορέας «Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης – ΗΔΙΚΑ Α.Ε.» (εφεξής ΗΔΙΚΑ) τηρεί και συντηρεί την ανωτέρω βάση για λογαριασμό της ΓΓΚΑ. Συνεπώς η ΗΔΙΚΑ δεν είναι υπεύθυνος αλλά εκτελούσα την επεξεργασία, κατά την έννοια του άρθρου 2 στοιχ. η' του ν. 2472/1997.

Βάσει των ανωτέρω, και μετά από την υπ' αριθμ. πρωτ. ΓΝ/ΕΙΣ/1037/06-09-2010 γνωστοποίηση της ΓΓΚΑ προς την Αρχή, η Αρχή εξέδωσε την υπ' αριθμ. πρωτ. ΓΝ/ΕΞ/350/31-03-2011 και με αριθμό 1039 άδεια ίδρυσης και λειτουργίας αρχείου με ευαίσθητα δεδομένα προς τη ΓΓΚΑ για την επεξεργασία ευαίσθητων προσωπικών δεδομένων μέσω του ΣΗΣ. Στην ανωτέρω άδεια η Αρχή προσδιόρισε συγκεκριμένους όρους αναφορικά με τη νομιμότητα και την ασφάλεια της επεξεργασίας, τους οποίους οφείλει να ικανοποιήσει ο υπεύθυνος της επεξεργασίας (ΓΓΚΑ). Η εν λόγω άδεια είναι σε ισχύ μέχρι τις 28-02-2014, ενώ – όπως αναφέρεται σε όρο αυτής - ο υπεύθυνος επεξεργασίας θα πρέπει να υποβάλει αίτηση ανανέωσής της δύο μήνες πριν τη λήξη της.

Η Αρχή πραγματοποίησε διοικητικό έλεγχο στο Σύστημα Ηλεκτρονικής Συνταγογράφησης (εφεξής ΣΗΣ) αναφορικά με την προστασία και την ασφάλεια των προσωπικών δεδομένων. Επισημαίνεται ότι, καθώς η λειτουργία και διατήρηση του ΣΗΣ έχει ανατεθεί πλήρως στην ΗΔΙΚΑ από την ΓΓΚΑ, ο έλεγχος έλαβε χώρα εξ ολοκλήρου στις εγκαταστάσεις της ΗΔΙΚΑ (εκτελών την επεξεργασία) και υπεργολάβων αυτής. Ο ανωτέρω έλεγχος ξεκίνησε το Νοέμβριο του 2011 και κάλυψε τόσο την παλαιά έκδοση του συστήματος όσο και τη νέα, η οποία είναι σε λειτουργία από τα μέσα του 2012. Ο έλεγχος εστιάστηκε τόσο στις υποχρεώσεις του υπευθύνου επεξεργασίας ως προς τους όρους της άδειας που έχει εκδώσει από την Αρχή, όσο και σε λοιπά ζητήματα που άπτονται της ασφάλειας του συστήματος (οργάνωση – διαδικασίες ως προς την ασφάλεια, μέτρα φυσικής ασφάλειας, τεχνικά μέτρα ασφάλειας). Στο εμπιστευτικό πόρισμα του ελέγχου (αριθμ. πρωτ. Αρχής: Γ/ΕΙΣ/1792/11-03-2013), το οποίο κοινοποιήθηκε τόσο στη ΓΓΚΑ όσο και στην ΗΔΙΚΑ, καταγράφονται, μεταξύ άλλων, τα ευρήματα αναφορικά με ελλιπή μέτρα ασφάλειας ή διαδικασίες προστασίας προσωπικών δεδομένων που εντοπίστηκαν.

Σε συνέχεια των ανωτέρω, η ΓΓΚΑ κλήθηκε, ως υπεύθυνος επεξεργασίας, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/3887/06-06-2013 έγγραφο της Αρχής, νομίμως σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της Ολομέλειας την 20-06-2013 για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει διεξοδικά τις απόψεις της επί των ανωτέρω. Το ίδιο έγγραφο κοινοποιήθηκε και στην ΗΔΙΚΑ, με την επισήμανση ότι κρίνεται σκόπιμο να παρίστανται στην εν λόγω συνεδρίαση και εκπρόσωποί της. Κατά την ακρόαση, οι εκπρόσωποι των ανωτέρω φορέων εξέθεσαν προφορικά τις απόψεις τους, ενώ ακολούθως υποβλήθηκε και συμπληρωματικό υπόμνημα από την ΗΔΙΚΑ (αριθμ. πρωτ.

Αρχής: Γ/ΕΙΣ/4484/04-07-2013), όπου και καταγράφεται, για κάθε εύρημα που αναφέρεται στο πόρισμα του ελέγχου, οι απόψεις της, καθώς επίσης και τα μέτρα στα οποία προέβη για την αντιμετώπιση του κάθε σχετικού κινδύνου.

Μετά την εξέταση όλων των ανωτέρω, η Αρχή εξέδωσε τη με αριθμό 138/2013 Απόφαση (συνημμένη στην παρούσα), με την οποία απευθύνει συστάσεις προς τον υπεύθυνο επεξεργασίας για αντιμετώπιση διαφόρων ζητημάτων που άπτονται είτε της συμμόρφωσής του με τους όρους της άδειας της Αρχής είτε ειδικότερων μέτρων ασφάλειας (στο πλαίσιο της γενικότερης υποχρέωσης, τόσο του υπεύθυνου όσο και του εκτελούντος την επεξεργασία, για την ασφάλεια αυτής κατά το άρθρο 10 του ν. 2472/1997). Στην εν λόγω Απόφαση περιγράφεται αναλυτικά η διαδικασία του ελέγχου, καθώς και τα ευρήματα αυτού αναφορικά με τη συμμόρφωση του υπευθύνου επεξεργασίας με τους όρους της άδειας. Περαιτέρω, ειδικότερες συστάσεις για επί μέρους οργανωτικά και τεχνικά θέματα ασφαλείας εμπεριέχονται στο εμπιστευτικό παράρτημα της Απόφασης, για το οποίο η Αρχή έκρινε, κατά τη συνεδρίασή της την 06-11-2013, ότι για λόγους ασφαλείας δεν είναι σκόπιμο να γνωστοποιηθεί σε τρίτους, πέραν του υπευθύνου επεξεργασίας και του εκτελούντος.

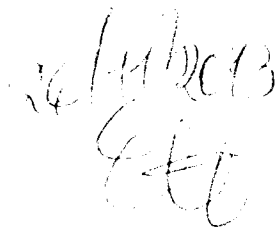
Παραμένουμε στη διάθεσή σας για κάθε συμπληρωματική πληροφορία.

Με εντολή Προέδρου
Το αναπληρωματικό μέλος της Αρχής

Ο εισηγητής ελεγκτής

Παναγιώτης Ροντογιάννης
Αναπλ. Καθηγητής ΕΚΠΑ

Δρ. Κωνσταντίνος Λιμνιώτης



Συνημμένα: Ένα (1) έγγραφο

1. Απόφαση 138/2013

