

Σχετικές Σκέψεις αναφορικά με τη λανθασμένη Σχεδιαστική Επιλογή στην πλατφόρμα ehealth

29/05/2026

Λευτέρης Χελιουδάκης,
Εκτελεστικός Διευθυντής Homo Digitalis

Σύμφωνα με το Άρθρο 35-36 του Ν.4816/2021 και το Άρθρο 3 της υπ. Αριθ. ΚΥΑ 4062/2021, το Υπουργείο Υγείας αποτελεί τον Υπεύθυνο Επεξεργασίας, ενώ η ΗΔΙΚΑ Α.Ε., ως Εκτελών την Επεξεργασία έχει την υποχρέωση λήψης και διαρκούς τήρησης των κατάλληλων και αναγκαίων τεχνικών και οργανωτικών μέτρων ασφάλειας των υπό επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Μάλιστα, το ίδιο άρθρο ρητά αναφέρει ότι, κατ' ελάχιστον, η ΗΔΙΚΑ Α.Ε. έχει ως υποχρέωση να καταγράφει και να παρακολουθεί τις προσβάσεις, να διασφαλίζει την ιχνηλασιμότητα και την προστασία των διακινούμενων δεδομένων από κάθε παραβίαση καθώς και από κάθε σκόπιμη ή τυχαία απειλή.

Φυσικά, επιπροσθέτως, των ως άνω, και σύμφωνα με τις διατάξεις του ΓΚΠΔ και του Ν.4624/2019, το Υπουργείο Υγείας, ως Υπεύθυνος Επεξεργασίας έχει την ευθύνη της τήρησης της αρχής της προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, με βάση το Άρθρο 25 ΓΚΠΔ, ενώ και οι 2 φορείς έχουν υποχρέωση να εξασφαλίζουν την ασφάλεια της επεξεργασίας, με βάση το Άρθρο 32 ΓΚΠΔ.

Σύμφωνα με τα πραγματικά περιστατικά, κάποιο άτομο, ενημέρωσε την κα. Τριανταφύλλου για το σχεδιαστικό κενό, καθώς μπόρεσε να αποκτήσει πρόσβαση σε βεβαιώσεις άλλων προσώπων. Αφού η ΗΔΙΚΑ, δεν κατόρθωσε να το αντιληφθεί, δεν εξασφαλίζεται η υποχρέωση της να καταγράφει και να παρακολουθεί τις προσβάσεις σε βεβαιώσεις, καθώς και να διασφαλίζει την ιχνηλασιμότητα και την προστασία των διακινούμενων δεδομένων από κάθε παραβίαση και από κάθε σκόπιμη ή τυχαία απειλή.

Άρα, η ΗΔΙΚΑ Α.Ε. δεν έχει λάβει κανένα πραγματικό τεχνικό ή οργανωτικό μέτρο προκειμένου να μπορεί να επιβεβαιώσει ότι πράγματι η έκταση του περιστατικού είναι περιορισμένη. Αντιθέτως, και αφού σύμφωνα με το Άρθρο 5 της ΚΥΑ 4062/2021, η εφαρμογή τέθηκε σε παραγωγική λειτουργία στις 2 Αυγούστου του 2021, από τότε έως και τις 18 Μαΐου 2026, δηλαδή για περισσότερο από 4 χρόνια και 9 μήνες, το Υπουργείο Υγείας και η ΗΔΙΚΑ Α.Ε. δεν κατόρθωσαν να τηρήσουν τις υποχρεώσεις τους και επομένως απροσδιόριστος αριθμός βεβαιώσεων τρίτων προσώπων μπορεί να έχουν φτάσει στα χέρια κακόβουλων χρηστών.

Ένα απλό μέτρο, το οποίο θα μπορούσε να λάβει η ΗΔΙΚΑ Α.Ε. και το Υπουργείο Υγείας, θα ήταν εκείνο των καταχωρήσεων, το οποίο κανονικά υποχρεωτικά εφαρμόζεται σε πράξεις επεξεργασίας που αφορούν την Οδηγία 2016/680 (αστυνομικές αρχές κοκ). Ένα μέτρο όπως αυτό, θα μπορούσε ανά

πάσα στιγμή να δίνει τη δυνατότητα την ΗΔΙΚΑ Α.Ε. να καταχωρεί ποιος λογαριασμός αιτήθηκε ποια βεβαίωση και να χρησιμοποιείται αποκλειστικά για τον έλεγχο της νομιμότητας της επεξεργασίας, την αυτοπαρακολούθηση, καθώς και τη διασφάλιση της ακεραιότητας και της ασφάλειας των δεδομένων. Πχ, σε περίπτωση που και οι κωδικοί taxis κάποιου πολίτη είχαν πέσει σε λάθος χέρια, και κάποιος κακόβουλος χρησιμοποιούσε τα στοιχεία του για να αντλήσει βεβαιώσεις τρίτων, οι καταχωρήσεις θα μπορούσαν να φανούν πολύ χρήσιμες για την παράνομη αυτή πράξη.

Σε καμία περίπτωση δεν μπορεί να υποβαθμιστεί το σημαντικό σχεδιαστικό κενό που υπήρχε, αποτέλεσμα των λανθασμένων σχεδιαστικών επιλογών των αρμόδιων φορέων, ώστε να θεωρηθεί πως δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όπως φαίνεται η ΗΔΙΚΑ Α.Ε. δεν έχει καμία αντίληψη για το ποιος κατεβάζει ποιανού την βεβαίωση. Μόνο μετά από email της κας. Τριανταφύλλου κατάλαβε ότι η ίδια ήταν σε θέση να κατεβάσει βεβαίωση άλλου ατόμου, απλά καταχωρόντας άλλους αριθμούς βεβαιώσεων.