ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 14-07-2015

Αριθ. Πρωτ.: Γ/ΕΞ/1001-1/14-07-2015

Γ Ν Ω Μ Ο Δ Ο Τ Η Σ Η 3/2015

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε μετά από πρόσκληση του Προέδρου της σε συνεδρίαση την 30-6-2015 στην έδρα της προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας.

Παρέστησαν ο Πρόεδρος, Π. Χριστόφορος, και τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Α.–Ι. Μεταξάς, Δ. Μπριόλας και Α. Συμβώνης και Π. Τσαντίλας, ως εισηγητές. Το μέλος Κ. Χριστοδούλου, αν και είχε προσκληθεί νομίμως, δεν παρέστη λόγω κωλύματος. Στη συνεδρίαση, χωρίς δικαίωμα ψήφου, παρέστησαν επίσης, με εντολή του Προέδρου, οι Φ. Μίτλεττον, Γ. Παναγοπούλου, Κ. Λιμνιώτης, ειδικοί επιστήμονες –ελεγκτές, ως βοηθοί εισηγητή. Παρέστη, επίσης, με εντολή του Προέδρου, η Γεωργία Παλαιολόγου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή συνεδρίασε προκειμένου να γνωμοδοτήσει, σύμφωνα με το άρθρο 19 παρ. 1 στοιχ. θ΄ του ν. 2472/1997, επί του σχεδίου διάταξης νόμου του Υπουργείου Υγείας σχετικά με την εφαρμογή του Συστήματος διαχείρισης και επιχειρηματικής ευφυΐας ΕΣΥ.

Στη συνεδρίαση παρέστησαν και παρείχαν διασαφηνίσεις για τη λειτουργία του συστήματος εκ μέρους του Υπουργείου Υγείας οι Α, υπεύθυνη συντονισμού έργου και μέλος της Ομάδας Διοίκησης έργου (ΟΔΕ), η Β, τεχνική υπεύθυνη έργου και μέλος της ΟΔΕ, η Γ, εκπρόσωπος της Διεύθυνσης Δημόσιας Υγείας και μέλος της ΟΔΕ καθώς και εκ μέρους της αναδόχου του έργου εταιρείας PricewaterhouseCoopers οι Δ, διαχειριστής

έργου/υπεύθυνος ανάλυσης και Ε, τεχνικός υπεύθυνος ασφαλείας.

Το Υπουργείο Υγείας, με τα με αρ. πρωτ. Γ/ΕΙΣ/1001/16-2-2015, Γ/ΕΙΣ/2239/8-4-2015, Γ/ΕΙΣ/2738/13-5-2015 έγγραφα απέστειλε στην Αρχή προτεινόμενη διάταξη νόμου, την αιτιολογική της έκθεση καθώς και τη μελέτη εφαρμογής για το έργο «Σύστημα διαχείρισης και επιχειρηματικής ευφυΐας ΕΣΥ».

Με σκοπό τη διερεύνηση της ύπαρξης νομικής βάσης, καθώς και του προτεινόμενου από το Υπουργείο τρόπου επεξεργασίας και ιδίως των μέτρων ασφαλείας που εφαρμόζονται για την προστασία των προσωπικών δεδομένων, πραγματοποιήθηκαν συναντήσεις μεταξύ στελεχών του Υπουργείου και της Αρχής στις οποίες συζητήθηκαν δυνατές λύσεις αναφορικά με την ψευδωνυμοποίηση των δεδομένων του συστήματος.

Λαμβάνοντας υπόψη το περιεχόμενο των συναντήσεων αυτών έγιναν από το Υπουργείο αλλαγές στο προτεινόμενο σχέδιο νόμου και στην αιτιολογική έκθεση που το συνοδεύει. Το προτεινόμενο σχέδιο νόμου επί του οποίου ζητείται η γνωμοδότηση της Αρχής εστάλη με μήνυμα ηλεκτρονικού ταχυδρομείου στις 25-06-2015 με αρ. πρωτ. Αρχής Γ/ΕΙΣ/3829/6-7-2015.

Κατόπιν αυτού η Ολομέλεια της Αρχής επιλαμβάνεται των θεμάτων του διαβιβασθέντος σχεδίου νόμου.

Η Αρχή, αφού άκουσε τους εισηγητές και τις διασαφηνίσεις των βοηθών εισηγητών, οι οποίοι στη συνέχεια αποχώρησαν, και κατόπιν διεξοδικής συζήτησης, εκδίδει την ακόλουθη

Γ Ν Ω Μ Ο Δ Ο Τ Η Σ Η

1. Από τις διατάξεις των άρθρων 2, 4 παρ. 1 και 7 παρ. 2 του ν. 2472/1997 προκύπτει ότι η επεξεργασία ευαίσθητων προσωπικών δεδομένων επιτρέπεται μετά από άδεια της Αρχής, η οποία εκδίδεται στην περίπτωση που ο σκοπός της γνωστοποιηθείσας επεξεργασίας είναι νόμιμος, σαφής και καθορισμένος, τα δεδομένα τα οποία τυγχάνουν επεξεργασίας είναι συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτούνται για την επίτευξη του σκοπού της επεξεργασίας και επιπλέον συντρέχει μία από τις προϋποθέσεις

που προβλέπονται στο άρθρο 7 παρ. 2 του προαναφερθέντος νόμου.

2. Η συλλογή και περαιτέρω επεξεργασία ευαίσθητων προσωπικών δεδομένων υγείας από το Υπουργείο Υγείας, πρέπει να λειτουργεί και αναπτύσσει τις συνέπειές της στο πλαίσιο του κράτους δικαίου και της αρχής της νομιμότητας. Όπως παγίως γίνεται δεκτό, η αρχή της νομιμότητας λειτουργεί ως περιοριστικό όριο της διοικητικής δράσης, ή, με αντίστροφο συλλογισμό, η διοικητική ενέργεια πρέπει να είναι σύμφωνη προς τον κανόνα δικαίου που διέπει τη δράση της Διοίκησης. Στην προκειμένη περίπτωση, επομένως, θα πρέπει καταρχήν να εξετασθεί κατά πόσον η ενέργεια της συλλογής και περαιτέρω επεξεργασίας από το Υπουργείο Υγείας ευαίσθητων δεδομένων συνάδει προς τους σχετικούς κανόνες δικαίου που διέπουν τη δράση του Υπουργείου αυτού.

Για να είναι νόμιμη η αιτούμενη επεξεργασία πρέπει να προβλέπεται σε διάταξη τυπικού νόμου όπου θα περιγράφονται τα βασικά χαρακτηριστικά της επεξεργασίας των προσωπικών δεδομένων των ασθενών που συνδέονται με τις αρμοδιότητες του Υπουργείου Υγείας, ο υπεύθυνος επεξεργασίας, ο σκοπός της επεξεργασίας, τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα που είναι αναγκαίο να τύχουν επεξεργασίας, ιδιαίτερα δε τα ευαίσθητα δεδομένα, κατά τρόπο ώστε να προκύπτει σαφώς ότι τα συγκεκριμένα δεδομένα είναι αναγκαία και πρόσφορα σε σχέση με τον σκοπό της επιδιωκόμενης επεξεργασίας κατ' εφαρμογή της αρχής της αναλογικότητας, προσέτι δε θα αναφέρεται ο χρόνος τήρησης των δεδομένων, οι τυχόν αποδέκτες των δεδομένων αυτών και να παρέχεται ειδικώς η αναγκαία νομοθετική εξουσιοδότηση για τη ρύθμιση ειδικότερων, τεχνικών ή λεπτομερειακών θεμάτων, όπως ο σχεδιασμός του συγκεκριμένου συστήματος και τα εν γένει οργανωτικά και τεχνικά μέτρα για την ασφάλεια της επεξεργασίας των δεδομένων.

3. Υπό τις παραπάνω προϋποθέσεις, η συλλογή και περαιτέρω επεξεργασία των δεδομένων υγείας από το Υπουργείο Υγείας μπορεί να πραγματοποιηθεί βάσει του άρθρου 7 παρ. 2 περ. ε υποπεριπτώσεις γγ και δδ του ν. 2472/1997, η οποία επιτρέπει την επεξεργασία ευαίσθητων προσωπικών δεδομένων, μετά από άδεια της Αρχής, εφόσον «η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία γγ) για λόγους προστασίας της δημόσιας υγείας είτε δδ) για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών».

4. Λαμβάνοντας υπόψη την κρισιμότητα των προσωπικών δεδομένων (ευαίσθητα δεδομένα υγείας), καθώς και το γεγονός ότι η επεξεργασία αφορά σε ένα πολύ μεγάλο αριθμό υποκειμένων, η απαιτούμενη άδεια της Αρχής πρέπει να θέτει ειδικούς όρους και προϋποθέσεις για την πραγματοποίηση της επεξεργασίας, ιδίως σύμφωνα με τα άρθρα 4 (χαρακτηριστικά δεδομένων προσωπικού χαρακτήρα) και 10 (απόρρητο και ασφάλεια της επεξεργασίας) ν. 2472/1997.

i. Σκοπός επεξεργασίας, Αναλογικότητα, Ορισμός υπευθύνου επεξεργασίας

Στο σχέδιο νόμου προβλέπονται 3 επιμέρους σκοποί επεξεργασίας:

- Η προστασία και προαγωγή της δημόσιας υγείας.
- Η αποτελεσματικότερη παρακολούθηση της λειτουργίας των μονάδων υγείας του ΕΣΥ και της στελέχωσης και κατανομής του ανθρώπινου δυναμικού αλλά και των υπόλοιπων εποπτευόμενων από το Υπουργείο Υγείας φορέων.
- Η παρακολούθηση της οικονομικής λειτουργίας και ο έλεγχος δαπανών υγείας.

Οι ανωτέρω επιμέρους σκοποί εντάσσονται στις αρμοδιότητες του Υπουργείου Υγείας ως επιτελικού, συντονιστικού και ελεγκτικού οργάνου για τη χάραξη της γενικότερης πολιτικής υγείας σε εθνικό επίπεδο και τον προγραμματισμό των επιμέρους δράσεων στον τομέα αυτόν.

Στη συγκεκριμένη περίπτωση όμως πρόκειται για μια περαιτέρω επεξεργασία που πραγματοποιείται μέσω του Συστήματος διαχείρισης και επιχειρηματικής ευφυΐας ΕΣΥ η οποία έγκειται στην ηλεκτρονική διαβίβαση από τις μονάδες υγείας και τις ΥΠΕ, την ηλεκτρονική συλλογή από το Υπουργείο και την περαιτέρω επεξεργασία για τους ανωτέρω αναφερόμενους επιμέρους σκοπούς για την οποία απαιτείται ειδική προηγούμενη άδεια της Αρχής για συλλογή και επεξεργασία ευαίσθητων δεδομένων υγείας.

Όπως γίνεται σαφές από το σχέδιο Εισηγητικής Έκθεσης, η μεγάλης κλίμακας αυτή επεξεργασία δικαιολογείται από την έλλειψη ενός ευρέως φάσματος αξιόπιστων και άμεσα αξιοποιήσιμων πληροφοριών η οποία δεν επιτρέπει στο Υπουργείο να σχεδιάσει και να υλοποιήσει στοχευμένες πολιτικές υγείας προς όφελος του δημοσίου

συμφέροντος. Όπως αναφέρεται, οι σχετικές πληροφορίες βρίσκονται σήμερα κατακερματισμένες σε διάφορους εποπτευόμενους από το Υπουργείο Υγείας φορείς και υπάρχει ανάγκη να ενσωματωθούν σε μια ενιαία κωδικοποιημένη βάση δεδομένων ώστε να είναι εφικτή η αποτελεσματικότερη διαχείρισή τους.

Στο κρινόμενο σχέδιο νομοθετικής διάταξης φαίνεται ότι καταρχήν πληρούνται οι ανωτέρω αναφερόμενες προϋποθέσεις, καθόσον

α) η περιγραφόμενη επεξεργασία συνάδει με τις αρμοδιότητες του Υπουργείου

β) περιγράφονται επαρκώς οι σκοποί της επεξεργασίας, τα βασικά χαρακτηριστικά της, οι επιμέρους αρμόδιες γενικές διευθύνσεις που επεξεργάζονται τα δεδομένα που θα συλλέγονται για λογαριασμό του υπεύθυνου επεξεργασίας, τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα που είναι αναγκαίο να τύχουν επεξεργασίας, ιδιαίτερα δε τα ευαίσθητα δεδομένα, ο χρόνος τήρησης των δεδομένων, οι αποδέκτες των δεδομένων και παρέχεται ειδικώς η αναγκαία νομοθετική εξουσιοδότηση για τη ρύθμιση ειδικότερων, τεχνικών ή λεπτομερειακών θεμάτων.

Παρ' όλα αυτά στο σχέδιο νόμου δεν είναι σαφές ποιες συγκεκριμένες κατηγορίες συλλεγόμενων δεδομένων από τις αναφερόμενες στην παράγραφο 2 του σχεδίου απαιτείται να επεξεργάζεται κάθε μία από τις αρμόδιες γενικές διευθύνσεις. Το στοιχείο αυτό είναι απαραίτητο προκειμένου να εκδοθούν οι αντίστοιχες άδειες συλλογής και επεξεργασίας ευαίσθητων δεδομένων, δεν είναι όμως απαραίτητο να αναφέρεται στη διάταξη νόμου, καθώς μπορεί να αποτελεί αντικείμενο ρύθμισης της υπουργικής απόφασης η έκδοση της οποίας προβλέπεται στο σχέδιο νόμου.

Από το σχέδιο διάταξης σε συνδυασμό με την αιτιολογική έκθεση προκύπτει ότι δεν συλλέγονται ονομαστικά στοιχεία ή άλλα μοναδικά αναγνωριστικά, αλλά δεδομένα τα οποία είτε αποστέλλονται κωδικοποιημένα από την πηγή τους (μονάδες υγείας και ΥΠΕ), όταν πρόκειται για αναλυτικά στοιχεία, είτε πρόκειται για συγκεντρωτικά στοιχεία. Ως εκ τούτου, εφόσον παρεμποδίζεται η εξακρίβωση της ταυτότητας των υποκειμένων, και λαμβάνοντας υπόψη ότι προς τούτο η Αρχή επιφυλάσσεται να θέσει ειδικότερες προϋποθέσεις κατά την έκδοση της απαιτούμενης άδειας επεξεργασίας, κρίνεται καταρχήν ότι πληρούται η αρχή της αναλογικότητας του άρθρου 4 του ν. 2472/1997.

Στην παρ. 4 που αναφέρεται στον υπεύθυνο επεξεργασίας, πρέπει να αναφέρεται ότι υπεύθυνος επεξεργασίας είναι το Υπουργείο Υγείας και όχι κάθε μια αρμόδια γενική διεύθυνση ξεχωριστά, καθώς σε αυτό τηρείται το σύνολο των δεδομένων και οι επιμέρους γενικές διευθύνσεις τελούν υπό την εποπτεία του.

Ως εκ τούτου η παρ. 4 του σχεδίου διάταξης πρέπει να τροποποιηθεί ως εξής:
«Υπεύθυνος επεξεργασίας των κατά το παρόν άρθρο τηρούμενων στοιχείων ορίζεται το Υπουργείο Υγείας διά των εκάστοτε αρμοδίων Γενικών Διευθύνσεων».

i. Απόρρητο και ασφάλεια της επεξεργασίας

Στο προτεινόμενο σχέδιο νόμου (εδ. 10) υπάρχει πρόβλεψη για την έκδοση υπουργικής απόφασης στην οποία *«… ρυθμίζονται, ειδικότερα, τεχνικά ή λεπτομερειακά θέματα τήρησης, επεξεργασίας στοιχείων και δεδομένων, τόσο σε έντυπη όσο και σε ηλεκτρονική μορφή γενικότερα, κάθε οργανωτικό και τεχνικό μέτρο για την ασφάλεια της επεξεργασίας των δεδομένων …»*

Δεδομένου ότι η κωδικοποίηση των δεδομένων δεν συνεπάγεται, καταρχήν, την ανωνυμοποίησή τους, προτείνεται η συμπλήρωση του εδ. 10 με την αναφορά στη χρήση τεχνικών ανωνυμοποίησης[1]. Προτεινόμενη διατύπωση:

«*Με απόφαση του Υπουργού Υγείας ρυθμίζονται, ειδικότερα, τεχνικά ή λεπτομερειακά θέματα τήρησης, επεξεργασίας στοιχείων και δεδομένων, τόσο σε έντυπη όσο και σε ηλεκτρονική μορφή γενικότερα, κάθε οργανωτικό και τεχνικό μέτρο για την ασφάλεια της επεξεργασίας των δεδομένων, συμπεριλαμβανομένης της χρήσης τεχνικών ανωνυμοποίησης, θέματα οργάνωσης και λειτουργίας της Επιτροπής Διαχείρισης Ηλεκτρονικών Αρχείων καθώς και κάθε άλλο ειδικότερο θέμα*».

Επίσης υπάρχει ειδική αναφορά στον τρόπο με τον οποίο κωδικοποιούνται τα στοιχεία ταυτοποίησης του ατόμου που στηρίζονται στον ΑΜΚΑ (εδ. 7).

«7. Τα στοιχεία ταυτοποίησης του ατόμου στηρίζονται στον ΑΜΚΑ και κωδικοποιούνται με τη χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού από τον

[1] Βλέπε και σχετική Γνώμη της Ομάδας Εργασίας του Άρθρου 29 «Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης».

υπεύθυνο επεξεργασίας των κατά τόπο πληροφοριακών συστημάτων των Μονάδων Υγείας πριν αποσταλούν στο Υπουργείο Υγείας.»

Στο σχέδιο αιτιολογικής έκθεσης, στην παρ. 7 αναφέρεται ότι:

«*Παράγραφος 7: Για λόγους διασφάλισης της ανωνυμίας του ασθενούς σε κεντρικό επίπεδο, τα στοιχεία ταυτοποίησης πρέπει να μην είναι αναγνώσιμα από το Υπουργείο Υγείας το οποίο θα συλλέγει ορισμένες αναλυτικές πληροφορίες. Για το λόγο αυτό, επιβάλλεται η κωδικοποίηση των στοιχείων ταυτοποίησής τους (ΑΜΚΑ) με χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού (cryptographic hash function) στην πηγή (κατά τόπους Μονάδες Υγείας), οι οποίες εγγυώνται ότι η έξοδος της εφαρμογής της συνάρτησης για κάθε διαφορετική είσοδο είναι μοναδική και συνεπώς επιτρέπουν την καταγραφή και παρακολούθηση των κινήσεων επαναεισαγωγής ενός ασθενούς σε διαφορετικό χρόνο ή/και τόπο. Η διασφάλιση της ανωνυμίας του ασθενούς στο σύστημα Επιχειρηματικής Ευφυίας ΕΣΥ του Υπουργείου Υγείας, ολοκληρώνεται με τη διπλή κρυπτογράφηση των ήδη κατακερματισμένων στοιχείων ταυτοποίησης (ΑΜΚΑ) με χρήση συμμετρικών κλειδιών, αρχικά στο επίπεδο της εφαρμογής (application layer) και κατόπιν στο επίπεδο της σχεσιακής βάσης δεδομένων (database layer). Οι πολιτικές ασφαλείας της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης του Υπουργείου Υγείας διασφαλίζουν τη μη γνωστοποίηση των δύο συμμετρικών κλειδιών που χρησιμοποιούνται για την κρυπτογράφηση στο σύστημα Επιχειρηματικής Ευφυΐας ΕΣΥ του Υπουργείου Υγείας στο ίδιο φυσικό πρόσωπο.»*

Δεδομένου ότι η προβλεπόμενη υπουργική απόφαση θα ορίσει στη λεπτομέρειά τους τα μέτρα ασφάλειας, προτείνεται στο εδ. 7 του σχεδίου νόμου να υπάρχει μία γενικότερη αναφορά στη χρήση της κωδικοποίησης και στο σκοπό αυτής, και όχι στην τεχνική υλοποίησής της, η οποία προτείνεται να περιγραφεί αναλυτικά στην προβλεπόμενη υπουργική απόφαση. Ειδικότερα, προτείνεται η εξής διατύπωση για το σχέδιο νόμου:

«Ως στοιχείο ταυτοποίησης του ατόμου τηρείται μοναδικός κωδικός ο οποίος προκύπτει με κατάλληλη επεξεργασία (κωδικοποίηση) του ΑΜΚΑ και αποσκοπεί στην πλήρη παρεμπόδιση της εξακρίβωσης της ταυτότητας των υποκειμένων.»

Όσον αφορά τα αναφερόμενα στο σχέδιο αιτιολογικής έκθεσης που περιγράφουν

ειδικά τον τρόπο κωδικοποίησης του ΑΜΚΑ, η Αρχή επιφυλάσσεται να γνωμοδοτήσει σχετικά με το ειδικό αυτό θέμα, όταν θα υποβληθεί προς γνωμοδότηση το σχέδιο της προβλεπόμενης υπουργικής απόφασης στο οποίο περιλαμβάνεται η περιγραφή των οργανωτικών και τεχνικών μέτρων για την ασφάλεια της επεξεργασίας των δεδομένων, καθώς και των τεχνικών ανωνυμοποίησης.

Το Υπουργείο Υγείας πρέπει:

i. να υποβάλει γνωστοποίηση για την επεξεργασία ευαίσθητων προσωπικών δεδομένων

ii. να υποβάλει το σχέδιο της προβλεπόμενης από το άρθρο 13^{A} του ν. 3370/2005 απόφασης του Υπουργού Υγείας προκειμένου να η Αρχή να προχωρήσει στην έκδοση της σχετικής Άδειας.

Ο Πρόεδρος	**Η Γραμματέας**
Π. Χριστόφορος	**Γ. Παλαιολόγου**