



Προς  
Μέλη Ι.Σ.Ρ.  
Ελεύθερους Επαγγελματίες

**Θέμα: " Συνοπτικές Οδηγίες για το Νέο Κανονισμό της Ευρωπαϊκής Ένωσης  
για τα προσωπικά δεδομένα (GDPR)"**

Αγαπητοί συνάδελφοι,

Στο πλαίσιο προσαρμογής και συμμόρφωσης στο νέο κανονισμό της Ευρωπαϊκής Ένωσης, για τα προσωπικά δεδομένα (GDPR) σας παραθέτουμε συνοπτικές οδηγίες, για ένα απλό ιδιωτικό ιατρείο.

**ΚΥΡΙΑ\* ΒΗΜΑΤΑ ΣΥΜΜΟΡΦΩΣΗΣ ΑΠΛΟΥ ΙΔΙΩΤΙΚΟΥ ΙΑΤΡΕΙΟΥ**

**ΠΟΥ ΤΗΡΕΙ ΗΛΕΚΤΡΟΝΙΚΟ ΑΡΧΕΙΟ ΑΣΘΕΝΩΝ**

**ΜΕ ΤΟ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)**

1

**Ο ιατρός οφείλει:**

Να τηρεί Αρχείο Επεξεργασίας για τα ευαίσθητα δεδομένα υγείας των ασθενών του (βλ. Συνημμένο Υπόδειγμα Αρχείου Επεξεργασίας).

Να διαθέτει έντυπο ενημέρωσης και να λαμβάνει συναίνεση των ασθενών του εάν πρόκειται να κάνει χρήση δεδομένων και για άλλους σκοπούς πέραν της τήρησης ιατρικού αρχείου: Εάν τα προσωπικά δεδομένα των ασθενών πρόκειται να χρησιμοποιηθούν και για άλλους σκοπούς (π.χ. αποστολή μηνύματος για υπενθύμιση επανελέγχου, τηλεφωνική κλήση για ραντεβού, χρήση στοιχείων για κλινική έρευνα, παροχή στοιχείων ασθενών σε τρίτους για άλλους σκοπούς), τότε ο ιατρός οφείλει:

α) Να ενημερώσει με σαφήνεια τον ασθενή για την περαιτέρω χρήση των δεδομένων του και για το σκοπό αυτής.

β) Να μην προχωρήσει στην περαιτέρω χρήση τους, αν δεν λάβει τη συναίνεση του ασθενούς για κάθε σκοπό ξεχωριστά.



### Να αναγνωρίζει και να σέβεται τα δικαιώματα των Ασθενών:

3.1. Ο ασθενής, αναφορικά με τα προσωπικά του δεδομένα, έχει τα εξής δικαιώματα:

#### α) Δικαίωμα πρόσβασης στα δεδομένα του:

Το δικαίωμα να γνωρίζει αν τα δεδομένα του υφίστανται επεξεργασία, πώς και για ποιο σκοπό.

#### β) Δικαίωμα διόρθωσης των δεδομένων του:

Το δικαίωμα να ζητήσει διόρθωση των προσωπικών του δεδομένων αν αυτά είναι ανακριβή ή ελλιπή.

#### γ) Δικαίωμα διαγραφής των δεδομένων του:

Το δικαίωμα να ζητήσει διαγραφή ή κατάργηση των προσωπικών του δεδομένων υπό ορισμένες προϋποθέσεις. Προσοχή: Εάν ο ασθενής ζητήσει διαγραφή των δεδομένων του κατά την περίοδο που ο ιατρός έχει νόμιμη υποχρέωση να τηρεί αρχείο (10ετία από την τελευταία επίσκεψη), ο ιατρός οφείλει να απαντήσει ότι δεν μπορεί να τα διαγράψει λόγω της νόμιμης υποχρέωσης διατήρησής τους στο αρχείο.

2

#### δ) Δικαίωμα περιορισμού της επεξεργασίας των δεδομένων του:

Το δικαίωμα να ζητάει τον περιορισμό της επεξεργασίας των προσωπικών του δεδομένων όταν συντρέχουν ορισμένες προϋποθέσεις.

#### ε) Δικαίωμα στη φορητότητα των δεδομένων του:

Το δικαίωμα του ασθενή να ζητήσει να αποσταλούν τα στοιχεία του σε τρίτο (π.χ. άλλο γιατρό).

3.2 Όταν ένας ασθενής υποβάλλει ένα αίτημα ασκώντας κάποιο από τα παραπάνω δικαιώματα, ο ιατρός οφείλει να απαντήσει εντός 1 μηνός είτε ικανοποιώντας το δικαίωμα (π.χ. δίνοντας στον ασθενή αντίγραφο του ιατρικού φακέλου) είτε απορρίπτοντας αιτιολογημένα το αίτημα (π.χ. αρνούμενος αίτημα διαγραφής, λόγω του ότι ο νόμος υποχρεώνει τον ιατρό να το διατηρήσει για 10 χρόνια) είτε εξηγώντας τους λόγους καθυστέρησης. Σε περίπτωση καθυστέρησης οφείλει πάντως να απαντήσει θετικά ή αρνητικά εντός 3 μηνών από το αίτημα.

### Να εφαρμόζει τεχνικά μέτρα ασφαλείας:

Να χρησιμοποιεί ισχυρό - δύσκολο password (π.χ. όχι «1234») για την είσοδο στα συστήματα και στις εφαρμογές και ανά τακτά χρονικά διαστήματα αλλαγή τους.

Απενεργοποίηση λειτουργίας μέσω αποθήκευσης (π.χ. USB) όπου αυτή δεν χρειάζεται (π.χ. PC γραμματείας).

Χρήση μοντέρνων λειτουργικών συστημάτων υπολογιστή και συνεχόμενη ενημέρωσή τους.

Χρήση λογισμικού προστασίας από κακόβουλο λογισμικό (antivirus).

Ενεργοποίηση Τείχους Προστασίας (Firewall) στον υπολογιστή.

Αποφυγή χρήσης λογισμικού ελεύθερης χρήσης (free download).

Αποφυγή χρήσης και παραχώρησης προνομιακών δικαιωμάτων πρόσβασης στον απλό χρήστη (δικαιώματα Local Administrator).





ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ  
**Ιατρικός Σύλλογος Ρόδου**



Λήψη αντιγράφων ασφάλειας σε τακτά χρονικά διαστήματα.

Αποφυγή χρήσης ελευθέρων e-mail, π.χ. Yahoo, για αποστολή και λήψη ευαίσθητων δεδομένων, π.χ. ιατρικών εξετάσεων.

Κρυπτογράφηση τοπικού δίσκου υπολογιστή μέσω του λειτουργικού συστήματος.

Κρυπτογράφηση εξωτερικών μονάδων αποθήκευσης (π.χ. εξωτερικός σκληρός δίσκος, USB κ.ο.κ.).

\* **ΠΡΟΣΟΧΗ:** Τα παραπάνω είναι οι ελάχιστες υποχρεώσεις κάθε απλού ιατρού. Σας συμβουλεύουμε να εξετάσετε τα ανωτέρω ως ενδεικτικά μέτρα, καθώς και να λάβετε υπ' όψιν ότι έχει μεγάλη σημασία και η σωστή εφαρμογή τους. Ενδεικτικά, η χρήση ισχυρού password αποτελεί ενδεδειγμένο μέτρο, αλλά εάν το password δεν φυλάσσεται σωστά και βρίσκεται σημειωμένο δίπλα στον υπολογιστή ή σε σημείο εύκολα προσβάσιμο, δεν προσφέρει κάποια πρόσθετη εξασφάλιση.

Σε κάθε περίπτωση, επισημαίνεται ότι τα παραπάνω αφορούν αλλαγές που φέρνει ο νέος Κανονισμός στους ιατρούς που ούτως ή άλλως δεσμεύονται από τον Κώδικα Ιατρικής Δεοντολογίας να διασφαλίζουν το ιατρικό απόρρητο και να προστατεύουν τα στοιχεία των ασθενών τους.

3

**Ο Ι.Σ.Ρ σας προσκαλεί στην ενημερωτική ομιλία που έχει προγραμματίσει για το συγκεκριμένο θέμα, με ομιλήτρια την κα Χρυσή Χρυσοχού - Δικηγόρο με εξειδίκευση στο Δίκαιο του internet και των Προσωπικών Δεδομένων.**

ΕΝΗΜΕΡΩΤΙΚΗ ΟΜΙΛΙΑ  
«ΝΕΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ»

25 MAY 2018

G Γενικός  
D Κανονισμός  
P Προστασίας  
R Δεδομένων

Ομιλήτρια: Χρυσή Χρυσοχού, Δικηγόρος  
(LLM) με Εξειδίκευση στο Δίκαιο του Internet & των Προσωπικών Δεδομένων

Σάββατο 19 Μαΐου 2018 & ώρα 19:00

Επιμελητήριο Δωδεκανήσου, Γρ. Λαμπράκη (Μαντράκι) Ρόδος

Για τον Ι.Σ.Ρ.

Ο Πρόεδρος  
**Χρήστος Απ. Μαντάς**

Ο Γεν. Γραμματέας  
**Ηλίας Ιωάν. Τσέρκης**

