Συμμόρφωση με τον ευρωπαϊκό κανονισμό GDPR

Τι είναι ο General Data Protection Regulation GDPR; Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων

Η μεταρρύθμιση της προστασίας των δεδομένων αποτελεί νομοθετική δέσμη με σκοπό την επικαιροποίηση και τον εκσυγχρονισμό των υφιστάμενων κανόνων της προστασίας των δεδομένων.

Περιλαμβάνει δύο νομοθετικές πράξεις: **τον Γενικό Κανονισμό Προστασίας των Δεδομένων** (που αντικαθιστά την οδηγία 95/46/ΕΚ) και **την οδηγία προστασίας των δεδομένων** στον τομέα της επιβολής του νόμου (που αντικαθιστά την απόφαση-πλαίσιο του 2008 για την προστασία των δεδομένων).

Ποιους επηρεάζει ο GDPR ;

Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων αφορά και επηρεάζει όλες τις επιχειρήσεις που συλλέγουν , αποθηκεύουν , επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα φυσικών προσώπων .

Τι είναι προσωπικά δεδομένα ;

- Προσωπικά δεδομένα είναι κάθε στοιχείο που αφορά φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί όπως ονοματεπώνυμο, διεύθυνση κατοικίας , ηλικία , οικογενειακή κατάσταση , επάγγελμα , βιολογική ,οικονομική κατάσταση, γενετικά, βιομετρικά κλπ.

Πότε τίθεται σε ισχύ;

- Ο νέος Γενικός Κανονισμός για τα Προσωπικά Δεδομένα (Κανονισμός Ε.Ε., 2016/679) τίθεται σε ισχύ στις 25 Μαΐου 2018 και αφορά όλες τις επιχειρήσεις και τους φορείς, ιδιωτικούς και δημόσιους που επεξεργάζονται προσωπικά δεδομένα Ευρωπαίων πολιτών.

Ποια είναι τα πρόστιμα ;

Σύμφωνα με τις διατάξεις του GDPR οι αρχές μπορούν να επιβάλλουν πρόστιμα έως

- €10.000.000 ή έως 2% του ετήσιου κύκλο εργασιών του προηγούμενου οικονομικού έτους
- €20.000.000 ή έως το 4% του παγκόσμιου ετήσιου κύκλο εργασιών του προηγούμενου οικονομικού έτους

Ο GDPR στον κλάδο τη Υγείας

Η ενημέρωση προς τα μέλη του Ιατρικού Συλλόγου Αθηνών σχετικά με τον υποχρεωτικό ή μη διορισμό Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer) ***Δημοσιεύθηκε 25 Απριλίου 2018***
(πηγή) http://www.isathens.gr/syndikal/7760-enimerwsi-meli-isa-gia-diorismo-dpo.html

ΣΥΜΠΕΡΑΣΜΑΤΑ για την πρωτοβάθμια φροντίδα υγείας από το ΔΣ του Ιατρικού Συλλόγου Αθηνών

1. *Ένα μέσο ιδιωτικό ιατρείο δεν χρειάζεται D.P.O.*
2. *Μια μεγάλη κλινική ή νοσοκομείο χρειάζεται D.P.O*
3. *Για τις περιπτώσεις που δεν εμπίπτουν στις άνω 2 κατηγορίες (π.χ. πολυϊατρεία ή διαγνωστικά εργαστήρια με περισσότερους ιατρούς)* ***συνιστάται*** *να λάβουν νομική* ***συμβουλή*** *καθώς κάθε περίπτωση αξιολογείται ξεχωριστά με βάση τα χαρακτηριστικά της.*
4. *Ο κανονισμός ισχύει για όλους. Το ότι δεν χρειάζεται κάποιος D.P.O.* ***δεν σημαίνει ότι δεν οφείλει*** *να εφαρμόζει τον κανονισμό.*
5. *Κατευθύνσεις σχετικές με τις περιπτώσεις 3 και 4 θα εκδοθούν σύντομα και για τις οποίες ο ΙΣΑ θα συνδράμει τα μέλη του και με την διοργάνωση σεμιναρίων εκπαίδευσης όπου χρειάζεται.*

ΓΙΑ ΤΟ ΔΙΟΙΚΗΤΙΚΟ ΣΥΜΒΟΥΛΙΟ
ΤΟΥ ΙΑΤΡΙΚΟΥ ΣΥΛΛΟΓΟΥ ΑΘΗΝΩΝ
Ο ΠΡΟΕΔΡΟΣ *Ο ΓΕΝ. ΓΡΑΜΜΑΤΕΑΣ*
Γ. ΠΑΤΟΥΛΗΣ *ΑΛΕΞ. ΒΑΣΙΛΕΙΟΥ*

Τι πρέπει να κάνω για να εναρμονιστώ με τον GDPR

1. Να ενημερωθείτε από ειδικούς
2. Να γίνει Χαρτογράφηση και Διάγνωση της παρούσας κατάστασης
3. Να γίνει Ανάλυση των Αναγκών για τη Συμμόρφωση με τον Κανονισμό
4. Να δημιουργηθεί το Πλάνο για το Σχεδιασμό και την Υλοποίηση των πολιτικών
5. Να Εκπαιδευτεί το προσωπικό της επιχείρηση σας

Αποτελέσματα

Data flow mapping *Χαρτογράφηση ροής δεδομένων*	**Gap Analysis** *Μελέτη ανάλυσης ελλείψεων*	**Privacy Impact Assessment** *Εκτίμηση των επιπτώσεων*	**Design and implementation of a compliance plan** *Σχεδίαση και υλοποίηση προγράμματος συμμόρφωσης*