ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

Eurobank

Secure HealthData

ΑΣΦΑΛΕΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΥΓΕΙΑ

"Ο νέος κανονισμός προστασίας δεδομένων"

Σταμπουλής Γεώργιος

Χημικός Μηχανικός, Οργανοτεχνική Α.Ε.

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Κανονισμός (ΕΕ) 2016/679

Γιώργος Σταμπουλής
Χημικός Μηχανικός (MSc)
Σύμβουλος Επιχειρήσεων

Η ΑΙΤΙΑ…

Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν

- **Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης**
- **Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης**

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΤΙ ΕΙΝΑΙ

- Ενιαίο νομικό πλαίσιο για τη προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ
- Θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων αυτών
- Δεν απαιτείται ενσωμάτωση στην εθνική νομοθεσία
- Υποχρεωτική εφαρμογή από 25 Μαΐου 2018

ΤΙ ΕΙΝΑΙ

- Ενιαίο νομικό πλαίσιο για τη προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ
- Θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων αυτών
- Δεν απαιτείται ενσωμάτωση στην εθνική νομοθεσία
- Υποχρεωτική εφαρμογή από 25 Μαΐου 2018

ΠΟΙΟΥΣ ΑΦΟΡΑ

- Όλους τους οργανισμούς, επιχειρήσεις και φορείς που επεξεργάζονται προσωπικά δεδομένα εργαζομένων, μελών, συνεργατών, πελατών, μετόχων ή άλλων φυσικών προσώπων που βρίσκονται στην Ευρωπαϊκή Ένωση, ανεξαρτήτως τόπου διαμονής και ιθαγένειας
- Αφορά τόσο τους οργανισμούς όσο και τους εκτελούντες την επεξεργασία
- Ελάχιστες παρεκκλίσεις για οργανισμούς και επιχειρήσεις που απασχολούν λιγότερο από 250 άτομα
- Δεν αφορά τήρηση δεδομένων στο πλαίσιο προσωπικής ή οικιακής δραστηριότητας (π.χ. προσωπικές ατζέντες τηλεφώνων)
- Δεν αφορά διαχείριση δεδομένων θανόντων προσώπων

ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

- Συλλογή
- Καταχώριση
- Οργάνωση
- Διάρθρωση
- Αποθήκευση
- Προσαρμογή ή μεταβολή
- Ανάκτηση
- Αναζήτηση πληροφοριών
- Χρήση
- Κοινολόγηση με διαβίβαση
- Διάδοση / Διάθεση
- Συσχέτιση ή συνδυασμός
- Περιορισμός
- Διαγραφή ή καταστροφή

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- **Περιορισμός του σκοπού**
- **Ελαχιστοποίηση των δεδομένων**
- **Χρονική διάρκεια**
- **Ρητή συγκατάθεση – Σύννομη επεξεργασία**
- **Σαφής πολιτική απορρήτου**
- **Σεβασμός ατομικών δικαιωμάτων**
- **Προστασία από το σχεδιασμό & εξ ορισμού**
- **Ασφάλεια επεξεργασίας**
- **Γνωστοποίηση παραβίασης**
- **Εκτίμηση αντικτύπου**
- **Υπεύθυνος προστασίας δεδομένων**
- **Εκπαίδευση προσωπικού**

Ο οργανισμός πρέπει να ορίζει ρητά τους σκοπούς για τους οποίους επεξεργάζεται τα δεδομένα και να περιορίζει την επεξεργασία μόνο για τους σκοπούς αυτούς

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Τα δεδομένα θα πρέπει να είναι κατάλληλα, συναφή και απολύτως αναγκαία για τους σκοπούς που ορίστηκαν

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Τα δεδομένα θα πρέπει να τηρούνται μόνο για το χρονικό διάστημα που απαιτείται, σύμφωνα με τους σκοπούς που ορίστηκαν

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Η επεξεργασία των δεδομένων θα πρέπει να είναι σύννομη. Η ρητή συναίνεση του υποκειμένου των δεδομένων είναι ένας από τους τρόπους νομιμοποίησης

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Οι οργανισμοί θα πρέπει να δηλώνουν με σαφήνεια και διαφάνεια την πολιτική απορρήτου που εφαρμόζουν (π.χ. είδος δεδομένων, σκοπός επεξεργασίας, τρόπος και χρονικό διάστημα διαχείρισης, μέθοδοι προστασίας τους κλπ)

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

- **Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα**
- **Δικαίωμα διόρθωσης**
- **Δικαίωμα διαγραφής (δικαίωμα στη λήθη)**
- **Δικαίωμα περιορισμού της επεξεργασίας**
- **Δικαίωμα στη φορητότητα**
- **Δικαίωμα εναντίωσης**

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Τα συστήματα (κυρίως μηχανογραφικά) και οι διαδικασίες προστασίας δεδομένων του οργανισμού πρέπει να είναι σχεδιασμένα με τρόπο ώστε να διασφαλίζουν τη μέγιστη προστασία των δεδομένων

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Ο οργανισμός οφείλει να εφαρμόζει τα απαραίτητα συστήματα, πολιτικές και διαδικασίες που εξασφαλίζουν την απαιτούμενη προστασία των δεδομένων π.χ. από παράνομη πρόσβαση, κατά λάθος απώλεια, δολιοφθορά, αλλοίωση κλπ

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Ο οργανισμός οφείλει να γνωστοποιεί περιστατικά παραβίασης της ασφάλειας των δεδομένων τις αρμόδιες Αρχές και, υπό προϋποθέσεις, και τα υποκείμενα των δεδομένων

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Ο οργανισμός οφείλει να διεξάγει μελέτες με σκοπό την εκτίμηση από τις επιπτώσεις της επεξεργασίας των δεδομένων, τον εντοπισμό των κινδύνων ασφαλείας και τους τρόπους αντιμετώπισής τους.

Η απαίτηση αυτή δεν ισχύει για όλες τις περιπτώσεις

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Ο οργανισμός έχει υποχρέωση να ορίζει υπεύθυνο προστασίας δεδομένων που θα παρακολουθεί τη διαρκή και επαρκή συμμόρφωσή του με τον Κανονισμό.

Η απαίτηση αυτή δεν ισχύει για όλες τις περιπτώσεις

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679

ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

- Περιορισμός του σκοπού
- Ελαχιστοποίηση των δεδομένων
- Χρονική διάρκεια
- Ρητή συγκατάθεση – Σύννομη επεξεργασία
- Σαφής πολιτική απορρήτου
- Σεβασμός ατομικών δικαιωμάτων
- Προστασία από το σχεδιασμό & εξ ορισμού
- Ασφάλεια επεξεργασίας
- Γνωστοποίηση παραβίασης
- Εκτίμηση αντικτύπου
- Υπεύθυνος προστασίας δεδομένων
- Εκπαίδευση προσωπικού

Ο οργανισμός οφείλει να εκπαιδεύσει το προσωπικό του στο πώς να εφαρμόζει καθημερινά την πολιτική προστασίας των προσωπικών δεδομένων και να ανασκοπεί την αποτελεσματικότητα του συστήματος προστασίας σε τακτική βάση

ΤΟ... "ΠΡΟΒΛΗΜΑ"

"Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και (πρέπει να) είναι σε θέση να αποδείξει τη συμμόρφωση" με τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (λογοδοσία)

ΚΑΙ… ΠΩΣ ΑΠΟΔΕΙΚΝΥΕΤΑΙ Η ΣΥΜΜΟΡΦΩΣΗ?

"Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και (πρέπει να) είναι σε θέση να αποδείξει τη συμμόρφωση" με τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (λογοδοσία)

- Σύνταξη εγχειριδίου συστήματος προστασίας
- Σχεδιασμός διαδικασιών και εντύπων
- Επεμβάσεις – βελτιώσεις στο μηχανογραφικό σύστημα
- Τήρηση των προαναφερθέντων. Ανασκοπήσεις

ΚΑΙ… ΠΩΣ ΑΠΟΔΕΙΚΝΥΕΤΑΙ Η ΣΥΜΜΟΡΦΩΣΗ?

"Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και (πρέπει να) είναι σε θέση να αποδείξει τη συμμόρφωση" με τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (λογοδοσία)

- Σύνταξη εγχειριδίου συστήματος προστασίας
- Σχεδιασμός διαδικασιών και εντύπων
- Επεμβάσεις – βελτιώσεις στο μηχανογραφικό σύστημα
- Τήρηση των προαναφερθέντων. Ανασκοπήσεις

ΚΑΙ… ΑΝ ΌΧΙ???

- Διοικητικά πρόστιμα μέχρι 10 εκατ. € ή 2% του τζίρου (όποιο είναι μεγαλύτερο), ή μέχρι 20 εκατ. € ή 4% του τζίρου (όποιο είναι μεγαλύτερο), ανάλογα με την περίπτωση
- Αποζημίωση των υποκειμένων των δεδομένων που πιθανώς να επιδικάσουν τα δικαστήρια

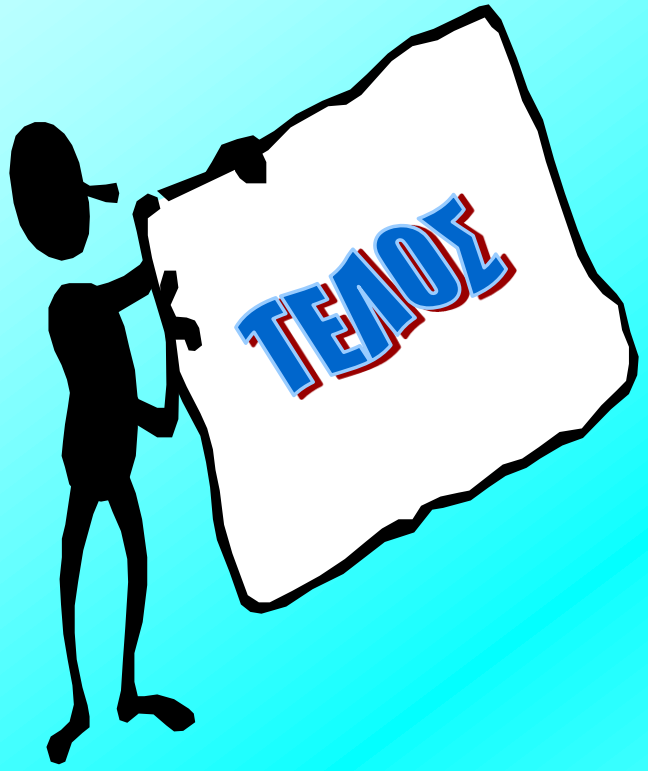
ΚΑΙ ΤΩΡΑ ΤΙ ΚΑΝΟΥΜΕ???

Παίρνουμε την απόφαση για το αν θα προχωρήσουμε στη δημιουργία συστήματος προστασίας δεδομένων προσωπικού χαρακτήρα…

… και αναλαμβάνουμε την ευθύνη

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΞΑΝΘΗΣ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΕΕ) 2016/679



Ευχαριστώ πολύ !!!