Προετοιμασία για τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)

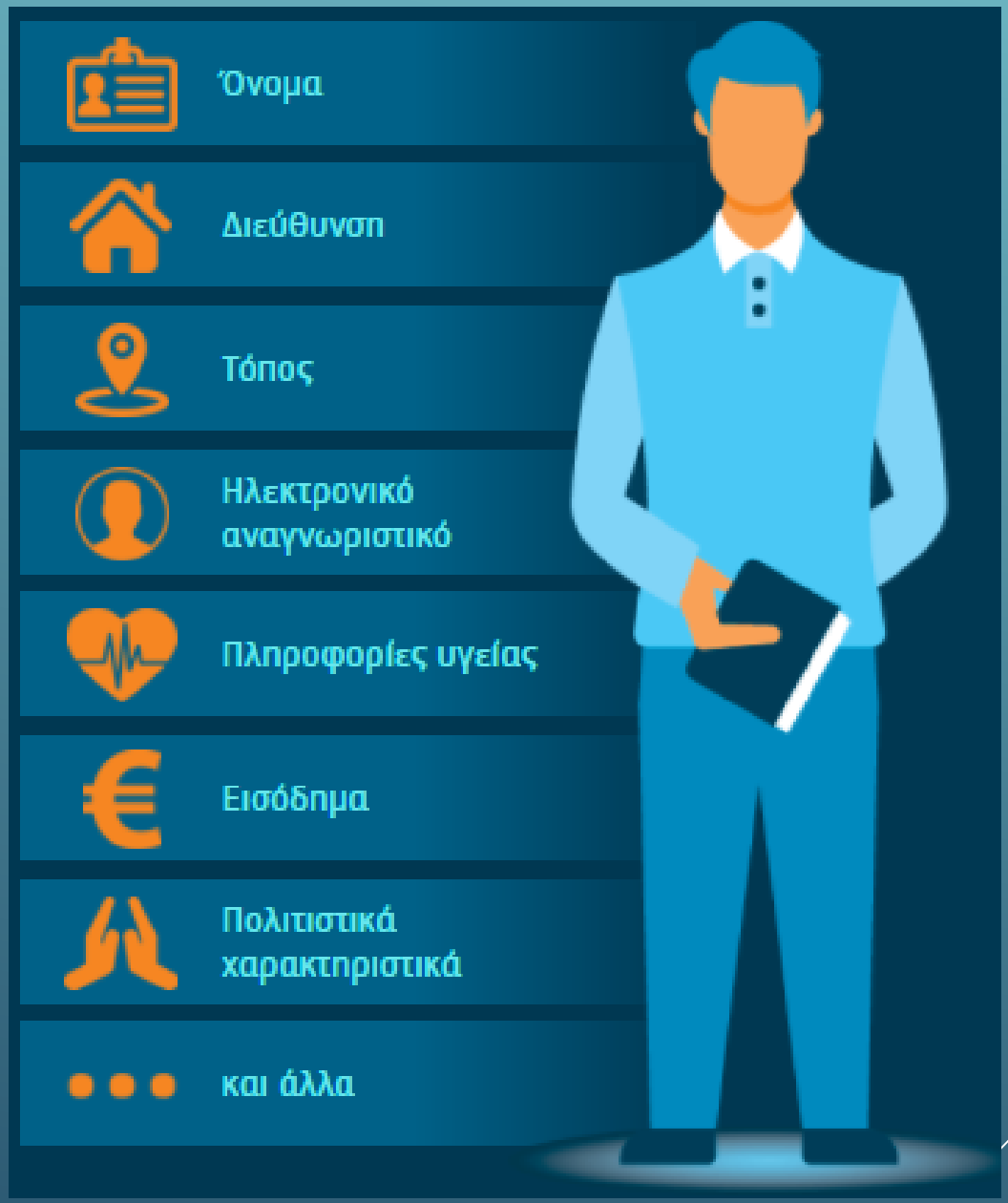
ΝΟΕΜΒΡΙΟΣ 2017

tms
AUDIT ◆ TAX ◆ ADVISORY

ΤΙ ΕΙΝΑΙ ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ο Ευρωπαϊκός Κανονισμός 2016/679 (General Data Protection Regulation, **GDPR**) ψηφίστηκε στις 27.04.2016 και τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο, χωρίς να απαιτείται περαιτέρω παρέμβαση της εθνικής νομοθεσίας.

ΤΙ ΕΙΝΑΙ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ?



Τα "προσωπικά δεδομένα" ορίζονται στον GDPR ως κάθε πληροφορία σχετική με «το πρόσωπο» που μπορεί να εντοπιστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε στοιχεία όπως όνομα, ΑΜΚΑ, ΑΦΜ, δεδομένα θέσης (GPS), ηλεκτρονικό αναγνωριστικό (user name) ή σε έναν ή περισσότερους παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του προσώπου.

Έτσι, σε πολλές περιπτώσεις, τα αναγνωριστικά ηλεκτρονικού ταχυδρομείου, συμπεριλαμβανομένης της διεύθυνσης IP, των cookies κ.λπ., θα θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα και αν καταγράφονται θα πρέπει να υπάρχει νομική συγκατάθεση.

- ✓ Για να είμαστε σαφείς, δεν υπάρχει διάκριση μεταξύ των προσωπικών δεδομένων σχετικά με τους ιδιώτες στους ιδιωτικούς, δημόσιους ή εργασιακούς τους ρόλους. **Το πρόσωπο είναι πρόσωπο**.

ΓΙΑΤΙ Ο GDPR ΜΑΣ ΑΦΟΡΑ ΟΛΟΥΣ ?

Ο GDPR ισχύει για όλες τις εταιρείες παγκοσμίως οι οποιές επεξεργάζονται προσωπικά δεδομένα πολιτών της Ευρωπαϊκής Ένωσης (Ε.Ε.).

Συνεπώς κάθε εταιρεία που συνεργάζεται/συναλλάσσεται με πολίτες της Ε.Ε. θα πρέπει να συμμορφώνεται με τις απαιτήσεις του GDPR.

ΟΙ ΚΑΝΟΝΕΣ ΤΟΥ GDPR

Οι εταιρείες οφείλουν :

- να τηρούν τις βασικές αρχές προστασίας των προσωπικών δεδομένων, συλλέγοντας για συγκεκριμένο νόμιμο σκοπό μόνο όσα εξ' αυτών είναι απαραίτητα.
- να μην τα υποβάλουν σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με το σκοπό συλλογής τους, να τα επικαιροποιούν και να τα αποθηκεύουν για το ελάχιστο χρονικό διάστημα που απαιτείται. Για αυτή τη διαδικασία πρέπει να λαμβάνουν κατά περίπτωση την ελεύθερη και σαφή συγκατάθεση των φυσικών προσώπων
- να τα μεταφέρουν σε χώρες εκτός Ε.Ε. μόνον όταν συντρέχουν συγκεκριμένες προϋποθέσεις
- να χορηγούν πρόσβαση στα προσωπικά δεδομένα σε συνεργάτες τους μόνον υπό συγκεκριμένες συνθήκες και εφόσον αυτοί αποδεικνύουν τη συμμόρφωσή τους με το GDPR

ΟΙ ΚΑΝΟΝΕΣ ΤΟΥ GDPR

- να αναπτύξουν ηλεκτρονικά εργαλεία για την έγκαιρη και δωρεάν ανταπόκριση σε αιτήματα που αφορούν :
  - ανάκληση της συγκατάθεσης
  - πρόσβαση στα δεδομένα
  - διόρθωση των δεδομένων ή διαγραφή τους
  - περιορισμό της επεξεργασίας
  - παράδοση των δεδομένων σε ηλεκτρονική μορφή
  - μεταφορά των δεδομένων σε άλλο φορέα
- να εξασφαλίζουν την ασφάλεια των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους
- να τηρούν σε αρχείο και να γνωστοποιούν κάθε παραβίαση των δεδομένων στην «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» εντός 72 ωρών και στα φυσικά πρόσωπα με απευθείας ενημέρωση ή δημόσια ανακοίνωση
- να αποδεικνύουν ότι τηρούν όλες τις απαιτήσεις του Κανονισμού.
- να γνωστοποιούν κατάλληλα και εγκαίρως στα φυσικά πρόσωπα τα δικαιώματά τους

ΟΙ ΚΑΝΟΝΕΣ ΤΟΥ GDPR

- να λαμβάνουν τα απαιτούμενα **τεχνικά και οργανωτικά μέτρα** που περιλαμβάνονται σε διεθνή πρότυπα, σε κώδικες δεοντολογίας και σε συστάσεις αρμοδίων κοινοτικών και εθνικών οργάνων
- να διενεργούν μελέτη εκτίμησης των επιπτώσεων **(Privacy Impact Assessment)**, στην οποία θα αξιολογούν τους κινδύνους για τα προσωπικά δεδομένα που διαχειρίζονται και με βάση αυτή θα οδηγούνται στη λήψη των απαραίτητων μέτρων περιορισμού των κινδύνων
- να ορίσουν Υπεύθυνο Προστασίας Δεδομένων (DaTa Protection Officer)
- να δημιουργήσουν και να επικαιροποιούν το μητρώο επεξεργασίας, όπου θα απεικονίζουν τη ροή, τους αποδέκτες και το είδος των προσωπικών δεδομένων που διαχειρίζονται
- να αναπτύξουν **πολιτικές και διαδικασίες** προστασίας και ασφάλειας των προσωπικών δεδομένων
- να συμμορφώνονται με κώδικες δεοντολογίας ή να διαθέτουν **πιστοποιήσεις** που αποδεικνύουν τη συμμόρφωσή τους με τον Κανονισμό.

ΣΥΝΕΠΕΙΕΣ

Οι αρχές θα πραγματοποιούν ελέγχους και οι εταιρείες σε περίπτωση μη συμμόρφωσης, υποχρεούνται στην καταβολή υψηλών πρόστιμων.
Ανάλογα με το είδος και το μέγεθος της παράβασης, τα πρόστιμα ανέρχονται έως τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών.

Για τον έλεγχο και τον καταλογισμό των προστίμων την Ελλάδα αρμόδια αρχή είναι η «Αρχή Προστασίας Προσωπικών Δεδομένων».

ΚΟΙΝΟΠΟΙΗΣΗ ΠΑΡΑΒΙΑΣΕΩΝ

- Ο GDPR εναρμονίζει τους διάφορους νόμους κοινοποίησης παραβιάσεων δεδομένων στην Ευρώπη και αποσκοπεί στο να διασφαλίσει ότι οι εταιρείες παρακολουθούν συνεχώς τις παραβιάσεις των προσωπικών δεδομένων.
- Οι εταιρείες πρέπει να εξασφαλίσουν ότι διαθέτουν την τεχνολογία και τις διαδικασίες που θα τους επιτρέψουν να ανιχνεύσουν και να ανταποκριθούν σε μια παραβίαση δεδομένων. Αυτό μπορεί να απαιτεί εκπαίδευση των στελεχών που διαχειρίζονται τις πληροφορίες αυτές.
- Ενδέχεται επίσης να απαιτήσει αλλαγές στις εσωτερικές πολιτικές ασφάλειας δεδομένων, ώστε να διασφαλιστεί ότι οι παραβιάσεις δεδομένων γίνονται σωστά κατανοητές και αναγνωρίζονται εύκολα.

Τα οφέλη των επιχειρήσεων από τη συμμόρφωση με τον GDPR

- Οι επιχειρήσεις θα κατηγοριοποιήσουν τα δεδομένά τους και θα εστιάσουν σε τι πραγματικά χρειάζονται.
- Θα δημιουργήσουν κατάλληλους εσωτερικούς κανονισμούς και πολιτικές
- Θα αναβαθμίσουν την ασφάλεια των δεδομένων και των συστημάτων τους καθιστώντας τα πιο ασφαλή και σύγχρονα
- Θα πρέπει να αναφέρονται μόνο σε μία εποπτική αρχή αντί σε μια διαφορετική για κάθε κράτος της Ε.Ε.

Πώς μπορούμε να βοηθήσουμε?

Έχοντας συστήσει μια ειδική ομάδα αποτελούμενη από νομικούς συμβούλους και συμβούλους πληροφορικής με πιστοποίηση από τον ISACA σας παρέχουμε τις παρακάτω εξειδικευμένες υπηρεσίες με στόχο τη συμμόρφωση με τις απαιτήσεις του GDPR. Ενδεικτικά οι υπηρεσίες μας είναι :

- Καταγραφή και κατηγοριοποίηση δεδομένων
- Αποτίμηση Ρίσκου (Risk impact and Risk assessment)
- Ανάλυση τις μηχανογράφησης και όπου απαιτείται συγκεκριμένες προτάσεις για βελτίωση και συμμόρφωση
- Compliance plan
- Impact assessment
- Νομικές συμβάσεις
- Δημιουργία εταιρικής πολιτικής

ΕΥΧΑΡΙΣΤΟΥΜΕ

TMS ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΟΡΚΩΤΩΝ ΕΛΕΓΚΤΩΝ ΛΟΓΙΣΤΩΝ
Μιχαλακοπούλου 91, 115 28 Αθήνα,
τηλ: 210 72 53 580-581

ΥΠΕΥΘΥΝΗ ΕΠΙΚΟΙΝΩΝΙΑΣ :
ΕΛΙΝΑ ΦΑΡΑΝΤΟΥ
info@tms-auditors.gr