

Στις αρχές του 2016 το Ευρωπαϊκό Κοινοβούλιο ενέκρινε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων 2016/679/ΕΕ (General Data Protection Regulation - GDPR)

Ο **GDPR** είναι ο νόμος για την **προστασία των προσωπικών δεδομένων** και τίθεται σε υποχρεωτική εφαρμογή από όλα τα κράτη – μέλη της Ε.Ε. στις **25 Μαΐου 2018, καταργώντας κάθε αντίθετη εθνική ρύθμιση.**

Το νομοθέτημα αυτό αλλάζει ριζικά το τοπίο στον χώρο της Προστασίας των Προσωπικών Δεδομένων επιβάλλοντας πρόσθετες υποχρεώσεις σε Υπεύθυνους Επεξεργασίας και Εκτελούντες την Επεξεργασία προσωπικών δεδομένων ανάμεσα στις οποίες είναι ο υποχρεωτικός διορισμός Data Protection Officer.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης καθορίζει μέτρα που θα πρέπει να ακολουθηθούν προκειμένου να εξασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των προσωπικών δεδομένων. **Καθορίζεται ο τρόπος με τον οποίο οι οργανισμοί θα διαχειρίζονται τα δεδομένα των υπαλλήλων, πελατών και συνεργατών τους** και αφορά όλα τα πρόσωπα που διαμένουν στην Ευρωπαϊκή Οικονομική Ζώνη.

Ειδικότερες υποχρεώσεις εκ του Κανονισμού:

- **Υπεύθυνος προστασίας δεδομένων:** Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική Αρχή.

- **Ευθύνη:** Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδεικνύει ότι λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και ότι συμμορφώνεται με τον Κανονισμό.

- **Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design»):** Ο Κανονισμός επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων σας. Για παράδειγμα, στις υπηρεσίες ηλεκτρονικής κοινωνικής δικτύωσης πρέπει να σας δίνεται η δυνατότητα να επιλέγετε ρυθμίσεις που θα προστατεύουν περισσότερο τα προσωπικά σας δεδομένα.

- **Προστασία δεδομένων εξ ορισμού («Data protection by default»):** Ο Κανονισμός επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, *εξ ορισμού*, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.
- **Ασφάλεια επεξεργασίας:** Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.
- **Γνωστοποίηση παραβιάσεων δεδομένων:** Ο υπεύθυνος επεξεργασίας έχει υποχρέωση, μόλις αντιληφθεί παραβίαση, να ενημερώσει τις αρμόδιες εποπτικές Αρχές και εσάς, εφ' όσον η παραβίαση σας θέτει σε σοβαρό κίνδυνο.
- **Εκτίμηση επιπτώσεων και προηγούμενη διαβούλευση:** Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων («Data protection impact assessment»). Όταν βάσει της διενεργηθείσας εκτίμησης επιπτώσεων και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εποπτική Αρχή.

Στους υπευθύνους επεξεργασίας δεδομένων μπορεί να επιβληθεί πρόστιμο που μπορεί να ανέλθει σε 20 εκατ. € ή στο 4% του συνολικού ετήσιου κύκλου εργασιών τους. Ενόψει τούτου, θα πρέπει να υπάρξει άμεσα πλήρης νομική και τεχνική συμμόρφωση προς τις απαιτήσεις του GDPR για να διασφαλιστεί η αποτελεσματική προστασία των υποκειμένων των δεδομένων.