ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ (ΓΚΠΔ)

GENERAL DATA PROTECTION REGULATION

2016/679

Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 *«για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών»* , ευρύτερα γνωστός ως **Γενικός Κανονισμός για την Προστασία Δεδομένων - ΓΚΠΔ** (General Data Protection Regulation - GDPR), θα έχει **άμεση υποχρεωτική εφαρμογή σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25 Μαΐου 2018**.

Με τη θέση του σε εφαρμογή καταργεί την Οδηγία 95/46/ΕΚ και την εθνική νομοθεσία που την ενσωμάτωσε, δηλαδή τον Νόμο 2472/1997. **Σύμφωνα με το Σχέδιο Νόμου για τον Ελληνικό Νόμο για την Προστασία Δεδομένων**, του οποίου η δημόσια διαβούλευση ολοκληρώθηκε στις 5 Μαρτίου 2018 και θα εισέλθει στη Βουλή για ψήφιση, ο Νόμος 2472/1997 επίσης θα καταργηθεί στο σύνολό του.

Ο νέος Γενικός Κανονισμός (ΕΕ) 2016/679 δεν παρεκκλίνει ουσιωδώς από τις γενικές αρχές του υφιστάμενου πλαισίου προστασίας των προσωπικών δεδομένων, αλλά προχωράει ένα βήμα παραπάνω και επιχειρεί να δημιουργήσει ένα αυστηρότερο θεσμικό πλαίσιο επεξεργασίας των προσωπικών δεδομένων και κατ' επέκταση προστασίας τους, ώστε να προκύψει ένα ισχυρό και πιο συνεκτικό πλαίσιο προστασίας δεδομένων στην Ευρώπη.

Α. Βασικές Έννοιες (άρθρο 4 ΓΚΠΔ)

- **Δεδομένα Προσωπικού Χαρακτήρα:** κάθε πληροφορία που αφορά φυσικό πρόσωπο εν ζωή και μπορεί να χρησιμοποιηθεί για την άμεση ή έμμεση ταυτοποίησή του (λ.χ. όνομα, επώνυμο, e-mail, Α.Δ.Τ., διεύθυνση κατοικίας). **ΔΕΝ αφορά δεδομένα νομικών προσώπων παρά μόνο δεδομένα μονοπρόσωπων εταιριών και ατομικών επιχειρήσεων, που νομικά αντιμετωπίζονται ως φυσικά πρόσωπα.**
- **Ευαίσθητα Προσωπικά Δεδομένα:** προσωπικά δεδομένα που αφορούν πιο ευαίσθητες πτυχές ενός ατόμου που προστατεύονται με αυστηρότερες ρυθμίσεις (λ.χ. πολιτικά φρονήματα, θρησκευτικές πεποιθήσεις, κατάσταση υγείας)
- **Επεξεργασία:** κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η

οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή

- **Υπεύθυνος Επεξεργασίας:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα
- **Εκτελών την Επεξεργασία:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας
- **Αποδέκτης:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι
- **Τρίτος:** οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα
- **Συγκατάθεση Υποκειμένου Δεδομένων:** κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και σε πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

Β. Προϋποθέσεις Νόμιμης Επεξεργασίας Προσωπικών Δεδομένων (άρθρο 6 ΓΚΠΔ)

Η επεξεργασία των προσωπικών δεδομένων είναι σύννομη **μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:**

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί. Το στοιχείο αυτό δεν εφαρμόζεται όταν η επεξεργασία διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

Γ. Ποιους αφορά ο ΓΚΠΔ

- **Όλες τις εταιρίες & όλους τους Δημόσιους Φορείς** που επεξεργάζονται προσωπικά δεδομένα Ευρωπαίων πολιτών είτε συναλλασσόμενων είτε εργαζόμενων, ανεξαρτήτως του πού έχουν την εγκατάστασή τους.
- **Υπεύθυνους Επεξεργασίας & Εκτελούντες** αυτή για λογαριασμό των υπευθύνων
- Δεδομένα που τηρούνται σε **φυσική & ηλεκτρονική μορφή**

Δ. Βήματα Συμμόρφωσης με τον Κανονισμό

- Κατανόηση των ζητημάτων που ανακύπτουν από τον Κανονισμό **(Awareness)**
- Καταγραφή των δεδομένων **(Data Inventory)** και των διαδικασιών, συστημάτων και αρχείων (φυσικών και ψηφιακών) που τα περιέχουν **(Data Mapping)**
- Ανάλυση της απόκλισης από την συμμόρφωση με τον Κανονισμό **(Gap Analysis)**
- Σχεδιασμός (ή ανασχεδιασμός) των κατάλληλων πολιτικών ροών δεδομένων και των επεξεργασιών που διενεργούνται, ώστε ο φορέας να είναι σε θέση να παρακολουθεί και να δημιουργήσει σύστημα τήρησης αρχείων

Ε. Βασικές Διαφοροποιήσεις από το ισχύον νομικό καθεστώς – Καινοτομίες

Ο νέος Κανονισμός ενδυναμώνει και θωρακίζει περαιτέρω τα δικαιώματα του υποκειμένου των δεδομένων με την ανάληψη αυστηρότερων υποχρεώσεων των υπευθύνων και την πρόβλεψη αποτελεσματικότερων κυρώσεων σε περίπτωση μη τήρησης των σχετικών διατάξεων. Κάποιες από τις βασικότερες διαφοροποιήσεις από το ισχύον νομοθετικό καθεστώς και καινοτομίες που προβλέπει είναι οι ακόλουθες:

- **Ενδυνάμωση Δικαιωμάτων Υποκειμένων (αρ. 12-22 ΓΚΠΔ):** Παροχή αιτηθέντων πληροφοριών στο υποκείμενο των δεδομένων εντός 1 μηνός (με δικαίωμα παράτασης 2 μηνών) ή ενημέρωση για τους λόγους τυχόν άρνησης - **Δικαίωμα πρόσβασης** υποκειμένου στα δεδομένα που τηρούνται σε σχέση με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων – κατάρτισης προφίλ - **Δικαίωμα εναντίωσης** του στην ανωτέρω επεξεργασία, ιδίως για σκοπούς απευθείας εμπορικής προώθησης – **Δικαίωμα διόρθωσης** χωρίς αδικαιολόγητη καθυστέρηση – **Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)** σε περίπτωση που ισχύουν οι προβλεπόμενες στον Κανονισμό προϋποθέσεις - **Δικαίωμα στη φορητότητα των δεδομένων**
- **Αρχή Λογοδοσίας (αρ. 5 παρ.2 ΓΚΠΔ):** «Ομπρέλα» υπό την οποία τίθενται όλες οι πράξεις επεξεργασίας. Η αρχή αυτή αναλύεται σε πολλές επιμέρους ενέργειες που πρέπει να πραγματοποιεί ο Υπεύθυνος Επεξεργασίας ο οποίος *«φέρει την ευθύνη και (πρέπει να) είναι σε θέση να αποδείξει τη συμμόρφωση»* του με τις λοιπές γενικές αρχές που προβλέπει ο Κανονισμός, πράγμα που σημαίνει ότι έχει την υποχρέωση όχι μόνο να συμμορφώνεται αλλά και να μπορεί ανά πάσα στιγμή να αποδείξει τη συμμόρφωσή του.
- **Υπεύθυνος Προστασίας Δεδομένων (αρ. 37-39 ΓΚΠΔ):** Εισαγωγή υποχρέωσης ορισμού Υπευθύνου Προστασίας Δεδομένων για κάποιες κατηγορίες Υπευθύνων Επεξεργασίας & Εκτελούντων την επεξεργασία στη βάση συγκεκριμένων ποιοτικών κριτηρίων, που περιλαμβάνουν τη διενέργεια συγκεκριμένων τύπων επεξεργασιών. Ο ρόλος του είναι ενημερωτικός και συμβουλευτικός αλλά και επιτελικός αφού αυτός ελέγχει τη συμμόρφωση με τον Κανονισμό και συνεργάζεται με την εποπτική αρχή. Προβλέπονται περιπτώσεις όπου ο διορισμός του είναι υποχρεωτικός (Δημόσιες Αρχές & Φορείς, όταν για την επεξεργασία απαιτείται τακτική και συστηματική παρακολούθηση υποκειμένων δεδομένων σε μεγάλη κλίμακα και επεξεργασία ειδικών δεδομένων) και φυσικά είναι νοητή και η περίπτωση διορισμού σε εθελοντική βάση.

- **Κατάργηση Υποχρέωσης Γνωστοποίησης & Θέσπιση Υποχρέωσης Εκτίμησης Αντίκτυπου (αρ. 35 ΓΚΠΔ):** Με το νέο Κανονισμό καταργείται η υποχρέωση γνωστοποίησης της επεξεργασίας στην εποπτική αρχή και του προληπτικού ελέγχου και αντικαθίσταται από διαδικασίες που επικεντρώνονται στις πράξεις επεξεργασίας που ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Ένα τέτοιο μέτρο είναι η Υποχρέωση Εκτίμησης Αντίκτυπου, σύμφωνα με την οποία ο Υπεύθυνος Επεξεργασίας σε συγκεκριμένες περιπτώσεις πρέπει να διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.
- **Κώδικες Δεοντολογίας & Μηχανισμοί Πιστοποίησης (αρ. 40-43 ΓΚΠΔ):** Ενθαρρύνεται η σύνταξη Κωδίκων Δεοντολογίας από ενώσεις και άλλους φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία προκειμένου να προσδιορίσουν την εφαρμογή του ΓΚΠΔ, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά διάφορων τομέων επεξεργασίας και τις ειδικές ανάγκες των πολύ μικρών, μικρών και μεσαίων επιχειρήσεων, καθώς και η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων, με σκοπό την απόδειξη συμμόρφωσης προς το ΓΚΠΔ. Σημειώνεται βέβαια, ότι αμφότερες οι περιπτώσεις αυτές δεν λειτουργούν ως απαλλακτικοί λόγοι ευθύνης.
- **Αυξημένα Επαπειλούμενα Διοικητικά Πρόστιμα (αρ. 83 ΓΚΠΔ):** Ο Κανονισμός προβλέπει τη δυνατότητα επιβολής κυρώσεων για ενίσχυση των κανόνων του επιπροσθέτως ή αντί των διορθωτικών μέτρων που επιβάλλονται από την εποπτική αρχή. Μάλιστα, σε συγκεκριμένες περιπτώσεις διαπίστωσης παράβασης των διατάξεων του Κανονισμού, το ύψος των προστίμων μπορεί να ανέλθει και έως τα 20.000.000 € ή σε περίπτωση επιχειρήσεων έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (όποιο είναι υψηλότερο).