**Νέος ευρωπαϊκός Κανονισμός 679/2016 για την Προστασία των Προσωπικών Δεδομένων**

**Γενικά**

Ο νέος Κανονισμός ενισχύει τα δικαιώματα των πολιτών και επιβάλλει μια σειρά νέων υποχρεώσεων στους υπευθύνους επεξεργασίας.

Οι νέες αυτές υποχρεώσεις απορρέουν από τις βασικές αρχές και κυρίως από την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, τήρησης και γενικά της επεξεργασίας των δεδομένων και τη νέα αρχή της λογοδοσίας, σύμφωνα με την οποία οι υπεύθυνοι επεξεργασίας **φέρουν την ευθύνη και θα πρέπει να είναι σε θέση να αποδείξουν τη συμμόρφωσή τους με όλες τις Αρχές** που διέπουν την επεξεργασία προσωπικών δεδομένων.

Ο Κανονισμός θέτει νέες υποχρεώσεις στους οργανισμούς, οι οποίοι θα πρέπει να εφαρμόσουν ένα ευρύ φάσμα μέτρων προκειμένου να διασφαλίσουν τη συμμόρφωσή τους:

* Εφαρμογή κατάλληλων μέτρων και πολιτικών ασφαλείας.
* Διενέργεια εκτίμησης επιπτώσεων των σχεδιαζόμενων πράξεων (impact assessment), για επεξεργασίες που παρουσιάζουν υψηλό κίνδυνο και σχετίζονται με αξιολόγηση προσωπικών πτυχών, αφορούν σε δεδομένα μεγάλης κλίμακας ή σε παρακολούθηση δημοσίου χώρου. Το impact assessment έχει ως στόχο τον εντοπισμό και την ελαχιστοποίηση των κινδύνων μη συμμόρφωσης.
* Τήρηση αρχείου δραστηριοτήτων επεξεργασίας: ο Οργανισμός διατηρεί πλέον λεπτομερή, εσωτερικά αρχεία αναφορικά με τις δραστηριότητες προστασίας δεδομένων, εγγράφως ή ηλεκτρονικά.
* Ορισμός Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ): ο ΥΠΔ είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης με τον Κανονισμό, ενημερώνει για τις υποχρεώσεις, παρέχει συμβουλές σχετικά με το πότε και πώς θα πρέπει να διενεργηθεί εκτίμηση των επιπτώσεων της σχεδιαζόμενης πράξης και αποτελεί το σημείο επαφής μεταξύ του Οργανισμού και του Γραφείου της Επιτρόπου Προστασίας Προσωπικών Δεδομένων.
* Εφαρμογή της Αρχής «Privacy by Design»: ο Οργανισμός οφείλει να δημιουργεί δομή, τεχνολογία και διαδικασίες που θα ανταποκρίνονται στις απαιτήσεις του Κανονισμού. Αυτό σημαίνει ότι, ο αρχικός σχεδιασμός κάθε υπηρεσίας ή προϊόντος θα πρέπει να δημιουργεί φιλικές συνθήκες για την προστασία των δεδομένων. Αυτή η προσέγγιση πλέον είναι ρητή απαίτηση, παρότι προηγουμένως αποτελούσε βέλτιστη πρακτική.
* Εφαρμογή της Αρχής «Privacy by Default»: ο Οργανισμός οφείλει να εφαρμόζει κατάλληλα μέτρα που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας χώρου. Το impact assessment έχει ως στόχο τον εντοπισμό και την ελαχιστοποίηση των κινδύνων μη συμμόρφωσης.
* Προετοιμασία για την πιθανότητα παραβίασης της ασφάλειας των δεδομένων π.χ. παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα που διαβιβάζονται, αποθηκεύονται ή επεξεργάζονται με οποιονδήποτε τρόπο.
* Οι Οργανισμοί θα πρέπει να θέσουν σαφείς πολιτικές και διαδικασίες, έτσι ώστε να διασφαλιστεί ότι θα μπορούν να αντιδράσουν και να γνωστοποιήσουν κάθε παραβίαση δεδομένων εντός 72 ωρών από τη στιγμή που αποκτούν γνώση του γεγονότος. Μάλιστα, η παραβίαση ανακοινώνεται αμέσως στο επηρεαζόμενο άτομο όταν υπάρχει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες του.
* Επομένως, οι Οργανισμοί ενθαρρύνονται να υιοθετούν διαδικασίες γνωστοποίησης και ανακοίνωσης ενδεχόμενων παραβιάσεων στο Γραφείο της Επιτρόπου Προστασίας Προσωπικών Δεδομένων.
* Σύναψη σύμβασης ανάθεσης εργασίας μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, η οποία θα καθορίζει τις υποχρεώσεις των μερών. Ο νέος Κανονισμός θέτει αυστηρές υποχρεώσεις ΚΑΙ στους εκτελούντες, όπως, για παράδειγμα, η τήρηση αρχείου δραστηριοτήτων και η λήψη των ενδεδειγμένων τεχνικών και οργανωτικών μέτρων ασφάλειας.
* Σε περίπτωση που διεξάγει Οργανισμός διασυνοριακή επεξεργασία, εντός της ΕΕ, πρέπει να ορίσει το κράτος μέλος της κύριας εγκατάστασης, του οποίου η εποπτεύουσα αρχή θα είναι αρμόδια ως επικεφαλής αρχή, για την εποπτεία της νομιμότητας της επεξεργασίας εντός της ΕΕ.
* Οργανισμός που διαβιβάζει προσωπικά δεδομένα σε τρίτη χώρα οφείλει να λάβει την Άδεια της Επιτρόπου Προσωπικών Δεδομένων, εάν επιλέξει ως νομική βάση για τη διαβίβαση συμβατικές ρήτρες που θα ετοιμάσει και θα εγκριθούν από το Γραφείο μου. Εάν από τη διαβίβαση επηρεάζονται και πολίτες κρατών μελών, οι συμβατικές ρήτρες θα εγκριθούν στα πλαίσια του μηχανισμού συνεκτικότητας.

1. **Η επεξεργασία απλών προσωπικών δεδομένων είναι νόμιμη όταν:**

* Έχει δοθεί η συναίνεση του ατόμου
* Για εκτέλεση σύμβασης
* Για έννομη υποχρέωση του Οργανισμού
* Για διαφύλαξη ζωτικού συμφέροντος του ατόμου
* Για δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας
* Για το έννομο συμφέρον του οργανισμού ή του τρίτου

1. **Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων:**

**Κατά κανόνα απαγορεύεται η επεξεργασία τους και επιτρέπεται όταν:**

(α) υπάρχει συγκατάθεση,

(β) στον τομέα του εργατικού δικαίου, δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας,

(γ) για ζωτικό συμφέρον,

(δ) για δραστηριότητες ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο – αφορά στα μέλη ή τα πρώην μέλη του ή πρόσωπα που έχουν τακτική επικοινωνία μαζί του και τα δεδομένα δεν κοινοποιούνται σε τρίτους,

(ε) για δεδομένα που έχουν δημοσιοποιηθεί από το άτομο,

(στ) για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων,

(ζ) για λόγους ουσιαστικού δημόσιου συμφέροντος,

(η) για προληπτική ή επαγγελματική ιατρική, εκτίμηση ικανότητας εργασίας, ιατρική διάγνωση, υγειονομική ή κοινωνική περίθαλψη ή θεραπεία ή διαχείριση υγειονομικών και κοινωνικών συστημάτων δυνάμει νόμου ή σύμβασης με επαγγελματία στον τομέα της υγείας που τηρεί το επαγγελματικό απόρρητο,

(θ) για λόγους δημόσιου συμφέροντος,

(ι) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

1. **Τα υφιστάμενα δικαιώματα των πολιτών ενδυναμώνονται και εισάγονται νέα:**

* Δικαίωμα ενημέρωσης. Η συγκατάθεση πρέπει με την ίδια ευκολία να δίδεται και να ανακαλείται. οι γονείς πρέπει να συγκατατίθενται για τη συμμετοχή των παιδιών τους σε υπηρεσίες του διαδικτύου
* Δικαίωμα πρόσβασης. Το άτομο έχει δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα προσωπικά του δεδομένα υφίστανται επεξεργασία και, εάν κάτι τέτοιο συμβαίνει, έχει το δικαίωμα να λάβει (και σε αντίγραφα) αρκετές πληροφορίες, όπως, για παράδειγμα, τον σκοπό της επεξεργασίας, τις κατηγορίες προσωπικών δεδομένων κ.λπ. Δεν χρεώνεται το άτομο για τη συμμόρφωση με το αίτημα του και θα πρέπει σε ένα μήνα ο Οργανισμός να συμμορφωθεί.
* Δικαίωμα διόρθωσης
* Δικαίωμα διαγραφής «Δικαίωμα στη λήθη» (διαγραφή δεδομένων)
* Δικαίωμα περιορισμού
* Δικαίωμα στη φορητότητα των δεδομένων. Νέο δικαίωμα που εισάγεται στον Κανονισμό και επέκταση του δικαιώματος στην απαίτηση για παροχή προσωπικών δεδομένων σε μια ευρέως χρησιμοποιούμενη ηλεκτρονική μορφή (format). Συγκεκριμένα, απαιτείται από τον οργανισμό να παρέχει τις σχετικές πληροφορίες σε μια δομημένη, κοινή και αναγνώσιμη από μηχανή μορφή.
* Δικαίωμα εναντίωσης. Μπορεί να ασκηθεί από το άτομο με σκοπό να περιοριστούν συγκεκριμένες επεξεργασίες και να μην υποβληθούν προσωπικά του δεδομένα σε επεξεργασία για σκοπούς απευθείας (άμεσης) εμπορικής προώθησης. Μόλις ένα άτομο αρνηθεί, τα στοιχεία του δεν θα πρέπει να υποβάλλονται σε επεξεργασία για περαιτέρω απευθείας εμπορική προώθηση.
* Δικαίωμα αντίρρησης σε αυτοματοποιημένη απόφαση περιλαμβανομένης της κατάρτισης προφίλ.

1. **Υποχρεώσεις Υπεύθυνων Επεξεργασίας**

* Φέρει το βάρος της απόδειξης όσον αφορά στην παροχή συγκατάθεσης (Άρθρο 7).
* Λήψη συγκατάθεσης για ανήλικους κάτω των 16 σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών (Άρθρο 8).
* Υποχρέωση κατασκευαστών στο στάδιο του σχεδιασμού και εξ΄ορισμού (privacy by default and by design) (Άρθρο 25).
* Υποχρέωση καθορισμού ευθυνών μέσω συμφωνίας όταν υπάρχουν από κοινού υπεύθυνοι επεξεργασίας (Άρθρο 26).
* Υποχρέωση εκπροσώπησης υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση (Άρθρο 27).
* Επιλογή εκτελούντων την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων (Άρθρο 28).
* Τήρηση αρχείων των δραστηριοτήτων επεξεργασίας (Άρθρο 30).
* Υποχρέωση τήρησης της ασφάλειας της επεξεργασίας (Άρθρο 32).
* Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας (Άρθρο 33).
* Υποχρέωση ανακοίνωσης παραβιάσεων ασφάλειας (Άρθρο 34).
* Τήρηση κώδικα δεοντολογίας (Άρθρα 40 – 41).
* Πιστοποίηση (Άρθρα 42-43).

1. **Τι καταργείται με το νέο Κανονισμό**

* Γνωστοποιήσεις Σύστασης και Λειτουργίας Αρχείου/Έναρξης Επεξεργασίας – αντικαθίστανται με την τήρηση Αρχείου Δραστηριοτήτων της επεξεργασίας.
* Άδεια για επεξεργασία ευαίσθητων δεδομένων *(νυν ειδικών κατηγοριών προσωπικών δεδομένων)* στον τομέα του εργατικού δικαίου.
* Άδεια για διασύνδεση αρχείων: οι διασυνδέσεις θα πρέπει να γίνονται μέσω της ΚΑΠ. Η κάθε ΔΥ πρέπει να ενημερώσει το ΤΥΠ για υφιστάμενες και μελλοντικές ανάγκες Διασύνδεσης.
* Έκδοση Απόφασης από την Επίτροπο για άρση της υποχρέωσης ενημέρωσης των υποκειμένων των δεδομένων
* Καταβολή τέλους των €17 από τα υποκείμενα για άσκηση του δικαιώματος πρόσβασης και αντίρρησης

1. **Τι αλλάζει με το νέο Κανονισμό**

* Άδειες διαβίβασης σε τρίτες χώρες – όμως η ΑΠΔΠΧ εγκρίνει τη νομική βάση της διαβίβασης π.χ. τυποποιημένες συμβατικές ρήτρες, δεσμευτικούς εταιρικούς κανόνες, κώδικα δεοντολογίας, μηχανισμό πιστοποίησης.
* Με εφαρμοστικές διατάξεις, η ΑΠΔΠΧ μπορεί να περιορίσει την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων και δεδομένων που αφορούν στην υγεία.

1. **Ορθή τηλεξυπηρέτηση κοινού**

Δεν πρέπει να δίνονται δεδομένα μέσω τηλεφώνου. αφού δεν επιβεβαιώνεται ότι τα δεδομένα ανακοινώνονται στα άτομα στα οποία αναφέρονται τα δεδομένα.