

ΗΛΕΚΤΡΟΝΙΚΗ ΜΗΝΙΑΙΑ ΕΝΗΜΕΡΩΣΗ



Κανονισμός Προστασίας Προσωπικών Δεδομένων

Από τις 25 Μαΐου 2018 έχει τεθεί σε υποχρεωτική εφαρμογή ο κανονισμός 2016/679/ΕΕ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ».

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation – γνωστός ως κανονισμός GDPR) δημιουργεί νέες υποχρεώσεις στις επιχειρήσεις (ενίσχυση του συστήματος εσωτερικού ελέγχου, θέσπιση νέων διαδικασιών διαχείρισης πληροφοριακών συστημάτων δίδοντας έμφαση στην προστασία / ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πληροφοριών).

Ειδικότερα, ο νέος κανονισμός εστιάζει στα εξής:

Δικαιώματα φυσικών προσώπων
Τα δικαιώματα των φυσικών

προσώπων συγκεκριμενοποιούνται και περιγράφονται αναλυτικά, τόσο ως προς το περιεχόμενό τους όσο και ως προς τον τρόπο άσκησής τους. Εισάγεται, επιπλέον, το δικαίωμα στην φορητότητα των δεδομένων, το δικαίωμα δηλαδή του φυσικού προσώπου να ζητήσει το σύνολο



των δεδομένων του, τα οποία έτυχαν επεξεργασίας ή γεννήθηκαν στα πλαίσια της επεξεργασίας.

Ορισμός Υπεύθυνου Διαχείρισης Πληροφοριών (Data Protection Officer - DPO)

Είναι υπεύθυνος για την εφαρμογή του κανονισμού. Ο DPO πρέπει να γνωρίζει το νομοθετικό και κανονιστικό περιβάλλον, τις διαδικασίες λειτουργίας της

επιχειρήσεις, να κατανοεί το μηχανογραφικό περιβάλλον και να λειτουργεί ως εκπρόσωπος της επιχείρησης έναντι των Αρχών, Εθνικών και Ευρωπαϊκών στα θέματα διαχείρισης προσωπικών δεδομένων. Επίσης, θα πρέπει να διασφαλίσει την αναμόρφωση της λειτουργίας της επιχείρησης σε ότι αφορά τις πολιτικές και τη μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα.

Θέσπιση Πολιτική Προστασίας Δεδομένων

Οι επιχειρήσεις στην πολιτική τους εντοπίζουν τα προσωπικά δεδομένα που διαχειρίζονται και καταγράφουν τις διαδικασίες επεξεργασίας τους ώστε να διασφαλίζεται, στο μέτρο του δυνατού, η προστασία τους.

Υποχρέωση λογοδοσίας με σαφή και κατανοητή γλώσσα για την πολιτική απορρήτου

Οι επιχειρήσεις πρέπει να μπο-

ρούν να αποδεικνύουν πως έχουν λάβει τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων που τηρούν και διαχειρίζονται. Επίσης πρέπει να υπάρχει σαφής συγκατάθεση από τα πρόσωπα για την τήρηση και επεξεργασία των προσωπικών τους δεδομένων.

Ανακοίνωση στην αρμόδια Αρχή των συμβάντων παραβίασης δεδομένων

Ιδιαίτερα σημαντική είναι η υποχρέωση γνωστοποίησης ύπαρξης παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή και ανακοίνωσης στο θιγόμενο από την παραβίαση φυσικό πρόσωπο. Ο υπεύθυνος για την προστασία των προσωπικών δεδομένων θα πρέπει εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος να υποβάλει γνωστοποίηση στην εποπτική αρχή και να ενημερώνει το φυσικό πρόσωπο, που αφορά η παραβίαση.

Αναθεώρηση προτύπου ISO 14001

Σε σύγκριση με την παλαιότερη έκδοση (2004), η νέα έκδοση (2015), η οποία τίθεται σε ισχύ από τις 15 Σε-

πτεμβρίου 2018, περιλαμβάνει τα εξής :

⇒ Εισάγονται νέοι ορισμοί όπως διακινδύνευση (risk), υποχρέωση συμμόρφωσης (compliance obligation), κύκλος ζωής (life cycle) κ.α.

⇒ Ο οργανισμός πρέπει να προσ-

διορίζει τα εσωτερικά και εξωτερικά θέματα, τις απαιτήσεις που μπορούν να έχουν επιπτώσεις στο σχεδιασμό του συστήματος διαχείρισης καθώς και τις ανάγκες και τις προσδοκίες των ενδιαφερόμενων μερών.

⇒ Υιοθετείται μια σαφώς διεργασιοκεντρική προσέγγιση για την εφαρμογή του συστήματος. Η ανώτατη διοίκηση πρέπει να προσδιορίζει ποσοτικά δεδομένα, δείκτες και στόχους για κάθε διεργασία, ως μέρος του στρατηγικού και επιχειρηματικού της σχεδιασμού.

⇒ Απαιτείται δέσμευση όχι μόνο για τη μείωση των περιβαλλοντικών επιπτώσεων αλλά και για τη

διαχείριση άλλων θεμάτων για την προστασία του περιβάλλοντος που περιλαμβάνονται στο πλαίσιο του οργανισμού, συμπεριλαμβανομένων και των αναγκών και των προσδοκιών των ενδιαφερόμενων μερών.

⇒ Πρέπει να προσδιορίζονται οι κίνδυνοι που συνδέονται με απειλές και ευκαιρίες όπως τυχόν προκύπτουν από τις περιβαλλοντικές πλευρές, τις απαιτήσεις συμμόρφωσης κλπ. Επίσης πρέπει να εμποδίζονται ή να μειώνονται όλα τα αποτελέσματα τα οποία εμποδίζουν τον οργανισμό για την επίτευξη των περιβαλλοντικών σκοπών του, συμπεριλαμβανο-

μένων και των δυνητικών περιβαλλοντικών επιπτώσεων.

⇒ Για τον καθορισμό των περιβαλλοντικών σκοπών και στόχων πρέπει να λαμβάνονται υπόψη εκτός από τα εσωτερικά και εξωτερικά κριτήρια καθώς και οι εντοπισμένες ευκαιρίες και απειλές.

⇒ Κατά τη διάρκεια του προγραμματισμού και του ελέγχου της αλυσίδας αξίας, η νέα έκδοση του προτύπου απαιτεί την εκτίμηση των περιβαλλοντικών επιπτώσεων όπως η μεταφορά των α' υλών, ο σχεδιασμός του προϊόντος ή της υπηρεσίας και η διάθεση των αποβλήτων ή η διάθεση του προϊόντος .