Αθηναϊκή Αναπτυξιακή Α.Ε.
ΣΥΜΒΟΥΛΟΙ ΔΙΟΙΚΗΣΗΣ & ΑΝΑΠΤΥΞΗΣ

Νέος ευρωπαϊκός κανονισμός για την προστασία των προσωπικών δεδομένων

Εισαγωγή

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 την ανάγκη ψήφισης εθνικής νομοθεσίας και καταργώντας την υφιστάμενη νομοθεσία. Ο νέος κανονισμός **αυξάνει σημαντικά τις υποχρεώσεις των επιχειρήσεων**, ενώ το μέγεθος των προβλεπόμενων προστίμων τον τοποθετεί πολύ υψηλά στην ατζέντα της ανώτατης διοίκησης.

Αντικείμενο του Γενικού Κανονισμού 2016/679

Η διαμόρφωση ενός ενιαίου νομικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, που θέτει μία σειρά περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με:

1. την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους,
2. τη δυνατότητα μεταφοράς τους σε άλλες χώρες,
3. την προστασία των δικαιωμάτων των φυσικών προσώπων,
4. την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και
5. τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.

Σε περίπτωση παράβασης προβλέπονται σημαντικά αυξημένα πρόστιμα, που ανάλογα με το είδος και το μέγεθός της, φθάνουν έως τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών.

Ποιους αφορά

Όλες τις ιδιωτικές και δημόσιες επιχειρήσεις, καθώς και τις κρατικές αρχές που με οποιοδήποτε τρόπο συγκεντρώνουν, επεξεργάζονται και εν γένει διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, σχετιζόμενων με τους πελάτες τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων. Ως εκ τούτου, ο νέος κανονισμός αφορά πρακτικά όλες τις επιχειρήσεις, εντός και εκτός Ευρωπαϊκής Ένωσης, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες.

Υποχρεώσεις που ανακύπτουν

Οι επιχειρήσεις και οργανισμοί που υπόκεινται στην τήρηση του κανονισμού θα πρέπει:

1. Να τηρούν τις βασικές αρχές προστασίας των προσωπικών δεδομένων, δηλαδή να τα συλλέγουν για συγκεκριμένο νόμιμο σκοπό και μόνο όσα εξ' αυτών είναι απαραίτητα,
2. να μην τα υποβάλουν σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με το σκοπό, να τα επικαιροποιούν,
3. να τα αποθηκεύουν για το μικρότερο δυνατό χρονικό διάστημα που απαιτείται, να λαμβάνουν - κατά περίπτωση - την ελεύθερη και σαφή συγκατάθεση των φυσικών προσώπων,
4. να τα μεταφέρουν σε χώρες εκτός ΕΕ μόνον υπό συγκεκριμένες προϋποθέσεις, να δίνουν πρόσβαση στα προσωπικά δεδομένα σε συνεργάτες τους μόνον υπό συγκεκριμένες συνθήκες και εφόσον αυτοί αποδεικνύουν τη συμμόρφωσή τους με τον νέο κανονισμό,

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

<u>Προβλήματα που πρέπει να αντιμετωπιστούν</u>

Οι επιχειρήσεις και οργανισμοί που υπόκεινται στην τήρηση του κανονισμού έχουν να αντιμετωπίσουν στα πλαίσια του νέου κανονισμού τα ακόλουθα προβλήματα:

1. Ακριβής γνώση για το ποια δεδομένα συλλέγουν και επεξεργάζονται σε κάθε φάση των δραστηριοτήτων τους, ποιοι εμπλέκονται και με ποια εργαλεία και με ποιες διαδικασίες γίνεται η επεξεργασία αυτή,

2. Ακριβής καθορισμός και διαχωρισμός των επιχειρησιακών αναγκών, ώστε να διασφαλίζονται όλες οι απαιτούμενες συγκαταθέσεις του υποκειμένου και να μη γίνεται πλεονάζουσα επεξεργασία,
3. Συστηματικός έλεγχος για την κάλυψη των απαιτήσεων του κανονισμού σε κάθε στάδιο επεξεργασίας των δεδομένων,
4. Αξιολόγηση των κινδύνων που ενδέχεται να οδηγήσουν σε παραβίαση των προσωπικών δεδομένων, με αποτέλεσμα βαρύτατες οικονομικές κυρώσεις και επιπτώσεις στην εταιρική φήμη,
5. Λήψη αποτελεσματικών ψηφιακών - με χρήση τεχνητής νοημοσύνης - μέτρων για τον περιορισμό του κινδύνου παραβιάσεων του κανονισμού, χωρίς να θίγονται οι επιχειρησιακές προτεραιότητες της επιχείρησης.

Υπηρεσίες της Αθηναϊκής Αναπτυξιακής

Η **Αθηναϊκή Αναπτυξιακή** έχει διαμορφώσει μία ομάδα εργασίας και με την εμπειρία της σε παροχή ολοκληρωμένων υπηρεσιών σε μεγάλες ως επί το πλείστον επιχειρήσεις και οργανισμούς σας υποστηρίζει με τις ακόλουθες υπηρεσίες:

- **Διάγνωση** και αποτύπωση του επιπέδου συμμόρφωσης με τον νέο κανονισμό με δημιουργία αρχείου δραστηριοτήτων επεξεργασίας,
- **Αξιολόγηση επιπτώσεων** (Privacy Impact Assessment) σχετικά με την προστασία δεδομένων για τον εντοπισμό των σημαντικότερων κινδύνων,
- **Πρόταση μέτρων αντιμετώπισης** (Compliance Plan), υποστήριξη και καθοδήγηση στην υλοποίησή τους για ολιστική συμμόρφωση,
- **Ανάπτυξη πολιτικών** και **διαδικασιών** προστασίας προσωπικών δεδομένων, σε ένα πλήρες Σύστημα Διαχείρισης Προσωπικών Δεδομένων,
- **Επιθεωρήσεις ετοιμότητας** (Compliance Audit) ως προς τον νέο κανονισμό,
- **Εκπόνηση διαδικασιών** για **πιστοποίηση** και **επαλήθευση** της συμμόρφωσης με βάση τα διεθνή πρότυπα που παρατίθενται.

ΓΙΑ ΤΗΝ ΑΘΗΝΑΙΚΗ ΑΝΑΠΤΥΞΙΑΚΗ

ΑΠΟΣΤΟΛΑΚΗΣ ΗΛΙΑΣ

ΠΡΟΕΔΡΟΣ Δ.Σ. & ΔΙΕΥΘΥΝΩΝ ΣΥΜΒΟΥΛΟΣ