LEGAL INSIGHT

Η ΣΥΜΜΟΡΦΩΣΗ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΠΡΟΣ ΤΟΝ ΝΕΟ ΕΥΡΩΠΑΪΚΟ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ- Η ΑΝΤΙΣΤΡΟΦΗ ΜΕΤΡΗΣΗ ΓΙΑ ΤΟΝ GDPR

Γιώργος Πανταζής
ΜΔΕ

Σε λιγότερο από 60 ημέρες, ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation- GDPR No 679/2016) τίθεται άμεσα σε εφαρμογή. Στις 25 Μαΐου ο GDPR τίθεται εν ισχύ, αλλάζοντας τον τρόπο του τρόπου λειτουργίας της επιχείρησής σας. Στον νέο Κανονισμό προβλέπεται μία σειρά προδιαγραφών που πρέπει να τηρηθούν από τις επιχειρήσεις, προκειμένου να αποδείξουν ότι σέβονται τα προσωπικά δεδομένα τόσο των πελατών τους, όσο και των εργαζομένων τους.

ΑΠΡΙΛΙΟΣ 2018

Σε λιγότερο από 60 ημέρες, ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation- GDPR No 679/2016) τίθεται άμεσα σε εφαρμογή. Στις 25 Μαΐου ο GDPR τίθεται εν ισχύ, αλλάζοντας τον τρόπο του τρόπου λειτουργίας της επιχείρησής σας. Στον νέο Κανονισμό προβλέπεται μία σειρά προδιαγραφών που πρέπει να τηρηθούν από τις επιχειρήσεις, προκειμένου να αποδείξουν ότι σέβονται τα προσωπικά δεδομένα τόσο των πελατών τους, όσο και των εργαζομένων τους.

Οι γνωστοποιήσεις επεξεργασίας προσωπικών δεδομένων και οι άδειες επεξεργασίας που εξασφάλιζαν οι επιχειρήσεις από την αρμόδια εποπτική αρχή, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), σύμφωνα με το νέο νομοθετικό πλαίσιο, καταργούνται.

- Η προστασία της ιδιωτικής ζωής και το πνεύμα επιχειρησιακής ηθικής του Νέου Κανονισμού

Γενεσιουργός λόγος του μεγαλεπήβολου Ευρωπαϊκού Κανονισμού είναι η ραγδαία αύξηση του κινδύνου παραβίασης της ιδιωτικότητας σε μια εποχή τεχνολογικών αλμάτων. Σε μια εποχή που η τεχνολογική εξέλιξη είναι αδύνατον να συλληφθεί ή να προβλεφτεί από τον ανθρώπινο νου – έτσι και από τον νου του ανθρώπου νομοθέτη-, το δικαίωμα του ατόμου στην ιδιωτική του ζωή, ή άλλως το δικαίωμα στη «μοναξιά» -όπως γλαφυρά επισημαίνεται στην διεθνή βιβλιογραφία, με την έννοια του δικαιώματος σε ένα μοναχικό, προσωπικό πεδίο που καθορίζει για τον εαυτό του το ίδιο το άτομο-, κινδυνεύει κατ' ουσίαν να μην υφίσταται.

Ο GDPR αποσκοπεί στην «αυτορρύθμιση» των επιχειρήσεων ως προς τις εγγυήσεις προστασίας της ιδιωτικότητας. Αποσκοπεί να καλλιεργήσει ένα πνεύμα προστασίας της ιδιωτικότητας, που

θα διέπει ολόκληρη την επιχειρηματική πρακτική. Δηλαδή, οι επιχειρήσεις οφείλουν να υιοθετήσουν τις κατάλληλες διαδικασίες προστασίας των προσωπικών δεδομένων που διαχειρίζονται, ώστε ανά πάσα στιγμή να μπορούν να αποδείξουν ότι είναι σύμφωνες με τον GDPR σε έναν ενδεχόμενο έλεγχο από την ΑΠΔΠΧ.

Η Συμμόρφωση προς τον GDPR θυμίζει διαδικασία πιστοποίησης ποιότητας -τύπου ISO-, αλλά δεν παύει να είναι ένα αυστηρό νομικό κείμενο. Η συμμόρφωση προς αυτόν δεν επαφίεται στην προαίρεση των επιχειρήσεων, αλλά είναι επιβεβλημένη. Κανένα πρότυπο ποιότητας δεν μπορεί να αποτελέσει επαρκή απόδειξη για την πλήρη συμμόρφωση προς τον GDPR. Για παράδειγμα, η πιστοποίηση μιας επιχείρησης κατά το πρότυπο 27001 ISO "Information Security Management System" συνιστά απλώς μία ένδειξη μερικής συμμόρφωσης προς τον GDPR. Οι προδιαγραφές του GDPR είναι κάτι πολύ παραπάνω. Η τήρησή τους απαιτεί μία διττή επαναπροσέγγιση του τρόπου λειτουργίας της επιχείρησής σας:

1. Ένα νομικό έλεγχο για την συναρμογή της επιχειρηματικής σας δράσης προς τις νομοθετικές ρυθμίσεις περί προστασίας προσωπικών δεδομένων

2. Έναν έλεγχο τεχνικό, ήτοι έναν έλεγχο ασφάλειας των τηρουμένων εντός της επιχείρησής σας πληροφοριών.

Τα πρόστιμα σε περίπτωση ενδεχόμενης παραβίασης είναι υψηλά και μπορούν να αγγίξουν το υπέρογκο ποσό των 20 εκατομμυρίων ευρώ (20.000.000€) ή το 4% του παγκόσμιου ετήσιου τζίρου της επιχείρησης.

- Ο διττός προσανατολισμός προστασίας της ιδιωτικότητας του GDPR

Ο νέος Ευρωπαϊκός Κανονισμός αποσκοπεί στην υιοθέτηση διαδικασιών προστασίας της ιδιωτικότητας, που έχουν αντίκτυπο εντός και εκτός της επιχείρησης, ήτοι η επιχείρηση οφείλει να αποδεικνύει τον έμπρακτο σεβασμό της στην ιδιωτική ζωή του ατόμου, είτε ως εργαζομένου (εντός της επιχείρησης προστασία) είτε ως πελάτη (εκτός της επιχείρησης προστασία).

Ως προς τον πελάτη, η επιχείρηση πρέπει να καταγράψει:
- ποια προσωπικά δεδομένα πελατών συλλέγει,
- για πόσο τα διατηρεί,
- από ποιες πηγές τα συλλέγει -ήτοι από τον ίδιο τον πελάτη, από τρίτες επιχειρήσεις κλπ., προς ποιους τρίτους αποδέκτες τα δημοσιοποιεί -ήτοι, προς τρίτες επιχειρήσεις στο πλαίσιο συνεργασίας, ή προς συνδεδεμένες επιχειρήσεις πχ. στην περίπτωση του ομίλου ξενοδοχείων-,
- κατά πόσον ενημερώνει τον πελάτη για την συλλογή των προσωπικών του στοιχείων και κατά πόσον εξασφαλίζεται σύννομα η συγκατάθεσή του για την μελλοντική χρήση τους.

Ως προς τον εργαζόμενο η επιχείρηση πρέπει να δράσει ανάλογα, δηλαδή:
- να καταγράψει ποια προσωπικά δεδομένα συλλέγει,
- για πόσο τα διατηρεί,

- ποιοι έχουν πρόσβαση σε αυτά,
- κατά πόσον ο εργαζόμενος συναινεί και είναι ενημερωμένος για την συλλογή και την αξιοποίησή τους.

Ο φάκελος του εργαζομένου ενδέχεται να περιέχει και ευαίσθητες πληροφορίες που χρήζουν αυξημένης προστασίας με βάση τον GPDR (πχ. αποτελέσματα ιατρικών εξετάσεων, μισθοδοσία).

- Μια νέα θέση εργασίας- Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων

Οι επιχειρήσεις που στην καθημερινή τους δραστηριότητα επεξεργάζονται τακτικά και συστηματικά προσωπικά δεδομένα (πχ. ξενοδοχειακές μονάδες), ή επεξεργάζονται ειδικές κατηγορίες προσωπικών δεδομένων (πχ. επεξεργασία δεδομένων υγείας από επιχειρήσεις υγείας, όπως διαγνωστικά/ κλινικές κλπ.), αποτελούν, μεταξύ άλλων, επιχειρήσεις που υποχρεούνται να διορίσουν Υπεύθυνο Προστασίας Προσωπικών Δεδομένων (Data Protection Officer- DPO).

Ο Ευρωπαϊκός Κανονισμός δεν ορίζει συγκεκριμένα προσόντα για τον διορισμό του εν λόγω προσώπου. Επισημαίνει, ωστόσο, ότι πρέπει να διαθέτει νομικές γνώσεις στον τομέα της προστασίας της ιδιωτικότητας, καθώς και τεχνολογικές γνώσεις. Δύσκολα συνδυάζονται τα προσόντα του DPO σε ένα και μόνο πρόσωπο. Ο DPO επιβλέπει και γνωμοδοτεί για την έγκυρη τήρηση προδιαγραφών του Κανονισμού και είναι ο υπεύθυνος για την διενέργεια διαβουλεύσεων (πχ. σχετικά με καταγγελίες παραβίασης προσωπικών δεδομένων πελάτη, εργαζομένου κλπ.) με την Αρχή Προστασίας Προσωπικών Δεδομένων. Στην πράξη ο καταλληλότερος να αναλάβει την επιτυχή εκπλήρωση των εν λόγω καθηκόντων είναι ένας έμπειρος δικηγόρος. Ο Κανονισμός, βέβαια, προβλέπει πέραν από τις νομικές διαδικασίες συμμόρφωσης, την ανάληψη τεχνολογικών πρωτοβουλιών (πχ. μέτρων ασφαλείας των υπολογιστικών συστημάτων), οπότε στην περίπτωση αυτή απαιτούνται οι γνώσεις μηχανικού πληροφορικής. Οι περισσότερες, βέβαια, επιχειρήσεις συνεργάζονται ήδη με IT-Managers που επιβλέπουν την ορθή λειτουργία των τεχνολογικών υποδομών τους. Προκειμένου να ολοκληρωθεί με επιτυχία το Project Συμμόρφωσης προς τον GDPR η συνεργασία του αρμόδιου δικηγόρου και του μηχανικού πληροφορικής θεωρείται αναγκαία, και επιδοκιμάζεται από τον Κανονισμό, καθότι προβλέπει ότι ο DPO μπορεί -και καλό θα είναι- να συνεπικουρείται από λοιπούς εργαζομένους ή συνεργάτες της επιχείρησης κατά την εκτέλεση των καθηκόντων του.

Στην πράξη οι περισσότερες επιχειρήσεις επιλέγουν έναν εξωτερικό σύμβουλο ως DPO, παρά διορίζουν στην εν λόγω νέα θέση εργασίας έναν υπάρχοντα εργαζόμενο. Σε περίπτωση που μια επιχείρηση διορίσει έναν εργαζόμενο ως DPO επιβάλλεται η εξόπλισή του με πληθώρα προνομίων, όπως η μισθολογική αναπροσαρμογή του (= αποτελεί ένδειξη παροχής των κατάλληλων πόρων για την συμμόρφωση της επιχείρησης, και απόδειξη της ανεξαρτησίας του). Ο DPO είναι και δεν είναι εργαζόμενος της επιχείρησης. Είναι αντικειμενικός, ανεξάρτητος (δεν μπορεί να είναι μέλος της Διοίκησης!), και δεν απολύεται για την ορθή εκτέλεση των καθηκόντων του. Επιπλέον, μιας και ο DPO δεν είναι υπεύθυνος για την παραβίαση των προσωπικών

δεδομένων που διαχειρίζεται η επιχείρηση, αλλά το πρόστιμο βαρύνει αποκλειστικά την επιχείρηση, η τελευταία πρέπει να είναι εντελώς βέβαιη ότι ο διορισμός ενός ήδη εργαζομένου σε DPO θα φέρει το επιθυμητό αποτέλεσμα και δεν θα δημιουργήσει επιπρόσθετα επιχειρηματικά βάρη. Σε περίπτωση που ο εργαζόμενος δεν μπορεί να αποδείξει ακαδημαϊκή, ή πρακτική επαγγελματική εμπειρία στην προστασία των προσωπικών δεδομένων, η επιχείρηση που επιθυμεί να τον επιφορτίσει με αυτόν τον ρόλο, πρέπει να επενδύσει στην κατάλληλη επιμόρφωσή του.

- Σε τι υποχρεούνται στο εξής οι επιχειρήσεις σύμφωνα με τον GDPR;

Οι επιχειρήσεις που στο πλαίσιο της δραστηριότητά τους συλλέγουν και εν γένει επεξεργάζονται τακτικά και σε ευρεία κλίμακα προσωπικά δεδομένα σε συμμόρφωση προς τον GDPR πρέπει:

- Να τηρούν αρχεία καταγραφής που να περιγράφουν την ροή των προσωπικών δεδομένων εντός της επιχείρησης, ήτοι τις υφιστάμενες διαδικασίες συλλογής αυτών (Data Mapping).
- Να αξιολογήσουν τις ως άνω διαδικασίες διαπιστώνοντας τα κενά ασφαλείας και τους ενδεχόμενους κινδύνους (Gap Analysis & Risk Analysis).
- Να καταρτίσουν Έγγραφες Πολιτικές προστασίας προσωπικών δεδομένων, που θα περιγράφουν την σύννομη πολιτική της επιχείρησης σχετικά με την προστασία της ιδιωτικότητας των πελατών και των εργαζομένων της, καθώς και τις ενέργειες που πρέπει να ακολουθηθούν για τον μετριασμό του κινδύνου σε ενδεχόμενη παραβίαση των συστημάτων τήρησης των προσωπικών πληροφοριών (Security Policy, Security Incident Response Plan).
- Να επισκοπήσουν και ενδεχομένως να αναθεωρήσουν συμβάσεις που έχει συνάψει η επιχείρηση με τρίτες επιχειρήσεις, καθώς και με τους εργαζομένους της.
- Να αναθεωρήσουν έγγραφα που προορίζονται για τον πελάτη (πχ. φόρμες ενημέρωσης πελάτη, φόρμες συγκατάθεσης συλλογής προσωπικών του στοιχείων).
- Να διορίσουν Υπεύθυνο Προστασίας Προσωπικών Δεδομένων (Data Protection Officer-DPO), που θα συντονίσει ολόκληρο το έργο συμμόρφωσης της επιχείρησης με το νέο νομοθετικό πλαίσιο και θα λειτουργεί ως «contact point» με την ΑΠΔΠΧ.

- Υπάρχει Παράταση Συμμόρφωσης;

Προθεσμία παράτασης δεν υπάρχει με βάση το γράμμα του Κανονισμού, ούτε και η Αρμόδια Εποπτική Αρχή (ΑΠΔΠΧ) έχει δηλώσει κάτι τέτοιο επισήμως. Το Υπό Διαβούλευση Νομοσχέδιο θέτει συμπληρωματικές επιπρόσθετες υποχρεώσεις των επιχειρήσεων, και αναμένουμε τις εξελίξεις της ψήφισής του. Ο GDPR απαιτεί, ωστόσο, την εξασφάλιση ενός minimum επιπέδου προστασίας της ιδιωτικότητας, η συμμόρφωση προς τον οποίο πρέπει να ολοκληρωθεί άμεσα.

Για περισσότερες πληροφορίες και για εγγραφή στην λίστα ενημερώσεών μας επικοινωνήστε μαζί μας:

ΓΙΑΝΝΑΤΣΗΣ ΚΑΙ ΨΑΡΑΚΗΣ
ΔΙΚΗΓΟΡΙΚΗ ΕΤΑΙΡΕΙΑ

WWW.YIANNATSIS.GR
38, ΚΑΡΝΕΑΔΟΥ, ΚΟΛΩΝΑΚΙ
106 76, ΑΘΗΝΑ
ΕΛΛΑΔΑ
T: (+30) 210 7231076
F: (+30) 210 7231075