Το GDPR ως Πλεονέκτημα και Εξασφάλιση στη Λειτουργία των Επιχειρήσεων

Η υποχρεωτική εφαρμογή του GDPR αποτελεί κύριο στοιχείο αμοιβαίας εμπιστοσύνης μεταξύ των συναλλασσόμενων και ως εκ τούτου θεμελιώδες επιχειρησιακό πλεονέκτημα. Η υλοποίηση ενός ασφαλούς πλαισίου εφαρμογής είναι σύνθετη και απαιτεί την υποστήριξη των διοικήσεων και την υιοθέτηση της αντίστοιχης κουλτούρας στο σύνολο ενός οργανισμού. Αλέξανδρος Νίκλαν, ITGRC / GDPR Chief Consultant, SYNTAX Πληροφορική ΑΒΕΕ.

Με την έλευση του νέου κανονισμού του GDPR (2016/679) από τις 28.5.2018 όπου τέθηκε σε εφαρμογή παρουσιάστηκαν πολλά προβλήματα προσαρμογής και συμμόρφωσης. Ειδικά στην χώρα μας, όπου υπάρχει γενικότερη έλλειψη κουλτούρας στην τήρηση μέτρων και διαδικασιών ασφάλειας επί δεδομένων (προσωπικών και επιχειρησιακών) τα προβλήματα έχουν πολλαπλασιαστεί γιατί συνήθως δίνεται έμφαση μόνο στο κόστος.
Το πρόβλημα πολλαπλασιάζεται όταν θεωρείται (με μια ελαφρότητα) πώς δεν θα υπάρξει τελικά αυστηρότητα εφαρμογής, αντίληψη εντελώς λανθασμένη. Ειδικά αν δούμε τις πρόσφατες ανακοινώσεις άλλων κρατών και Αρχών της ΕΕ καθώς και τις σχετικές με παραβάσεις ποινές που επιβλήθηκαν, π.χ. υπόθεση Google. Υπενθυμίζεται εδώ πώς τα ποσά μπορεί να είναι εξοντωτικά σε μια μεγάλη παράβαση (ως 20.000.000€ ή 4% παγκοσμίου τζίρου εταιρίας, αναλόγως ποιο είναι το μεγαλύτερο). Ο ιδιωτικός και ο δημόσιος τομέας παραμένουν εν αγνοία, σε μεγάλο ποσοστό , με τον δημόσιο τομέα να έχει τα σοβαρότερα προβλήματα.

Συνοπτικά, είναι σημαντικό να τονιστούν τα εξής σημεία που φαίνεται να μην έχουν αναδειχθεί αρκετά.

1) Το GDPR ως πλαίσιο λειτουργιών, θα έπρεπε ήδη να είχε γίνει εργαλείο διαφήμισης ως ελκυστικός παράγοντας για την προστασία της ιδιωτικότητας, παρά ως μια υποχρεωτική και επί ποινή συμμόρφωση. Δυστυχώς στην Ελλάδα, ελάχιστες επιχειρήσεις γνωρίζουν πλήρως το πλαίσιο του κανονισμού ενώ ακόμα και σήμερα πολλές μεγάλες εταιρίες αδιαφορούν για το θέμα προσμένοντας ότι η ΑΠΔΠΧ δεν θα ενεργοποιηθεί πλήρως.

2) Όσον αφορά στην υλοποίηση ενός πλαισίου συμμόρφωσης είναι αναγκαίο να τονιστεί πώς οι ενέργειες ενός έργου είναι σύνθετες. Ένα έργο συμμόρφωσης σε GDPR χωρίζεται σε οργανωτικό/νομικό και τεχνικό μέρος. Εξορισμού αυτό απαιτεί συνδυασμό γνώσεων και συνεργασίας ειδικών συμβούλων, τόσο κατά την αξιολόγηση των ευπαθειών, όσο και κατά την υλοποίηση αλλά και στη συνέχεια τη διατήρηση και προσαρμογή του σε μελλοντικές επιχειρησιακές και τεχνολογικές εξελίξεις.

3) Πρέπει να γίνει κατανοητό πώς η συμμόρφωση μιας εταιρίας με το GDPR χρειάζεται σημαντικό χρονικό διάστημα προσαρμογής, καθώς ενδεχομένως να χρήζει αλλαγή εργασιακής κουλτούρας και επιχειρησιακών διαδικασιών. Οι ενέργειες συμμόρφωσης πρέπει να περιλαμβάνουν μια έκθεση αξιολόγησης ευπαθειών (Data Privacy Impact Assessment) καθώς και ένα σύνολο διαδικασιών και τεχνικών μέτρων που θα διασφαλίζουν τον οργανισμό από ακούσια ή εκούσια παράβαση του κανονισμού.

4) Τέλος πρέπει να ληφθεί σοβαρά υπόψη πώς το οικονομικό μέγεθος των επιχειρήσεων δεν παίζει κανένα ρόλο κατά την απαίτηση συμμόρφωσης με τον νέο κανονισμό. Το GDPR ορίζει πώς όσες επιχειρήσεις σε ιδιωτικό και δημόσιο τομέα, διαχειρίζονται μεγάλο όγκο προσωπικών δεδομένων και παρέχουν υπηρεσίες επεξεργασίας τους θα πρέπει να συμμορφωθούν προς τον κανονισμό.

Ως κατακλείδα η ανάγκη για συνεχή συμμόρφωση με τα άρθρα του Ευρωπαϊκού κανονισμού, όπως και με το επερχόμενο Ελληνικό νομοσχέδιο, οδηγεί σε επανεξέταση και άλλων θεμάτων που σχετίζονται με την ηλεκτρονική ασφάλεια και ιδιωτικότητα. Ήδη ψηφίστηκε νομοσχέδιο για την εφαρμογή της οδηγίας της ΕΕ για την ασφάλεια δεδομένων (2016/1148/ΕΕ), ενώ ακολουθεί πολύ σύντομα και νέος κανονισμός που θα αφορά την ιδιωτικότητα σε σχέση με τηλεπικοινωνίες και τους παρόχους αυτών (e-Privacy).

Αν μια επιχείρηση δεν κάνει άμεσα τις απαιτούμενες ενέργειες συμμόρφωσής της με το GDPR, ενδεχομένως να τεθεί εκτός αγοράς αφού θα αποτελεί πλέον προαπαιτούμενο συνεργασίας και παροχής υπηρεσιών, για τους οργανισμούς και τις εταιρίες που δραστηριοποιούνται εντός της ΕΕ, αλλά και των χωρών που θα ψηφίσουν παρόμοιες νομοθεσίες για να συνεχιστούν οι συναλλαγές σε διασυνοριακό επίπεδο (π.χ. Privacy Shield ΗΠΑ). Η έγκαιρη επένδυση για τη συμμόρφωση προς το GDPR μέσο-μακροπρόθεσμα θα εξασφαλίσει εξαιρετική απόδοση(R.O.I.).