GDPR για επιχειρήσεις
…με λόγια απλά

Δρ Γιώργος Δρόσος

Προϊστάμενος Τμήματος Υποστήριξης Πολιτικών Επιχειρηματικής Καινοτομίας

Εθνικός Εκπρόσωπος στην Ε.Ε. για τον Ψηφιακό Μετασχηματισμό των Επιχειρήσεων

23 Μαΐου 2018

Τι αφορά και ποιους καλύπτει ο νέος Κανονισμός;

- Στις 25 Μαΐου 2018 ξεκινά η εφαρμογή του νέου Ευρωπαϊκού Γενικού Κανονισμού για την Προστασία των Δεδομένων (General Data Protection Regulation – GDPR) 2016/679
- Ο νέος Κανονισμός ρυθμίζει την επεξεργασία (συλλογή, χρήση και αποθήκευση) από άτομα, εταιρείες ή οργανισμούς των δεδομένων προσωπικού χαρακτήρα που αφορούν άτομα στην ΕΕ.
- Δεν υπάγεται σε αυτόν η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποθανόντων προσώπων ή νομικών προσώπων.
- Για την Ελλάδα η αρμόδια εποπτεύουσα αρχή είναι η ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Πότε δεν θα εφαρμόζεται ο κανονισμός;

- Οι νέοι κανόνες δεν εφαρμόζονται σε δεδομένα που υποβάλλονται σε επεξεργασία από ένα άτομο για αυστηρά προσωπικούς λόγους ή για δραστηριότητες που διενεργούνται κατ' οίκον, εφόσον δεν συνδέονται με επαγγελματική ή εμπορική δραστηριότητα.
- Δεν θα εφαρμόζονται αν π.χ. ένα άτομο χρησιμοποιεί το ιδιωτικό του βιβλίο διευθύνσεων για να προσκαλέσει φίλους μέσω ηλεκτρονικού μηνύματος σε μια γιορτή που διοργανώνει.
- Αν η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν αποτελεί βασικό μέρος της επιχειρηματικής δραστηριότητας και η δραστηριότητά δεν δημιουργεί κινδύνους για φυσικά πρόσωπα, τότε ορισμένες από τις υποχρεώσεις του GDPR δεν ισχύουν.

Ποιά θεωρούνται δεδομένα προσωπικού χαρακτήρα;

- Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο.
- Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα, αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου, παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του GDPR.
- Ο GDPR προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία. Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε ψηφιακή ή έντυπη μορφή.

Χαρακτηριστικά παραδείγματα δεδομένων προσωπικού χαρακτήρα

- όνομα και επώνυμο
- διεύθυνση κατοικίας
- ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com
- αναγνωριστικός αριθμός κάρτας
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
- αναγνωριστικό cookie
- δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

Ποιά <u>ΔΕΝ</u> θεωρούνται δεδομένα προσωπικού χαρακτήρα;

- Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα έτσι ώστε το άτομο να μην είναι ταυτοποιήσιμο, δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα.

- Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη.

Παραδείγματα δεδομένων που <u>ΔΕΝ</u> θεωρούνται προσωπικού χαρακτήρα

- αριθμός μητρώου εταιρείας
- ηλεκτρονική διεύθυνση του τύπου πληροφορίες@εταιρεία.com
- ανώνυμα δεδομένα

Οι παρακάτω ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα θεωρούνται «ευαίσθητες» και λαμβάνουν ειδική προστασία σύμφωνα με τον GDPR

- φυλετική ή εθνοτική καταγωγή
- πολιτικά φρονήματα
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- συμμετοχή σε συνδικαλιστική οργάνωση
- επεξεργασία γενετικών δεδομένων
- βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου·
- υγεία
- σεξουαλική ζωή ή γενετήσιος προσανατολισμός.

Ευαίσθητα δεδομένα προσωπικού χαρακτήρα

Ο γενικός κανόνας είναι ότι η επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα **απαγορεύεται.**

Ωστόσο, υπάρχουν ορισμένες εξαιρέσεις βάσει των οποίων μια εταιρεία ή ένας οργανισμός μπορεί ενδεχομένως να επεξεργάζεται ευαίσθητα δεδομένα προσωπικού χαρακτήρα, όταν για παράδειγμα:

- ο πολίτης έχει προδήλως δημοσιοποιήσει τα ευαίσθητα δεδομένα του
- ο πολίτης έχει δώσει ρητή συγκατάθεση
- υπάρχει νόμος ο οποίος διέπει έναν συγκεκριμένο τύπο επεξεργασίας δεδομένων για συγκεκριμένο σκοπό που αφορά το δημόσιο συμφέρον ή τη δημόσια υγεία

Τι αποτελεί επεξεργασία δεδομένων;

Ο όρος «επεξεργασία» καλύπτει ένα ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα.

Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

Παραδείγματα δεδομένων στα οποία θεωρείται ότι γίνεται επεξεργασία:

- διαχείριση προσωπικού και μισθοδοσία
- προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα
- αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων
- καταστροφή διά τεμαχισμού εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα
- δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο
- αποθήκευση διευθύνσεων IP
- μαγνητοσκόπηση (τηλεόραση κλειστού κυκλώματος).

Ένα σωστά προσδιορισμένο πρόβλημα έχει λυθεί κατά 50%

Albert Einstein

Οι σημαντικότερες δυσκολίες που έχουν να αντιμετωπίσουν οι επιχειρήσεις είναι (1/2):

- Η ακριβής γνώση για το ποια δεδομένα συλλέγουν και επεξεργάζονται σε κάθε φάση των δραστηριοτήτων τους, ποιοι εμπλέκονται και με ποια εργαλεία και διαδικασίες γίνεται η επεξεργασία.
- Ο καθορισμός και διαχωρισμός των επιχειρησιακών αναγκών, ώστε να διασφαλίζονται όλες οι απαιτούμενες συγκαταθέσεις του υποκειμένου και να μη γίνεται πλεονάζουσα επεξεργασία.
- Ο συστηματικός έλεγχος για την κάλυψη των απαιτήσεων του GDPR σε κάθε στάδιο επεξεργασίας των δεδομένων.

Οι σημαντικότερες δυσκολίες που έχουν να αντιμετωπίσουν οι επιχειρήσεις είναι (2/2):

- Η αξιολόγηση των κινδύνων που ενδέχεται να οδηγήσουν σε παραβίαση των προσωπικών δεδομένων, με αποτέλεσμα βαρύτατες οικονομικές κυρώσεις και επιπτώσεις στην εταιρική φήμη.
- Η παρουσίαση των σημαντικότερων κινδύνων και των τρόπων αντιμετώπισής τους στη Διοίκηση με πρακτικό τρόπο, ώστε να αποφασισθεί ένα ρεαλιστικό πλάνο και προϋπολογισμός συμμόρφωσης.
- Η λήψη αποτελεσματικών και οικονομικών μέτρων για τον περιορισμό του κινδύνου παραβιάσεων του GDPR, χωρίς να θίγονται οι επιχειρησιακές προτεραιότητες.

Τα δικαιώματα των χρηστών με τον GDPR:

- να λαμβάνουν σαφείς και κατανοητές πληροφορίες για το ποιός επεξεργάζεται τα προσωπικά δεδομένα τους και γιατί
- να ζητούν από όλες τις εταιρείες να έχουν οι ίδιοι πρόσβαση και να μαθαίνουν ποιά ακριβώς στοιχεία οι εταιρείες διατηρούν γι' αυτούς
- να έχουν το δικαίωμα στη «λήθη», δηλαδή, αν θέλουν, θα απαιτούν αυτά τα δεδομένα να διαγραφούν από τις βάσεις δεδομένων των εταιρειών.
- να ζητήσουν αποζημίωση προσφεύγοντας στη δικαιοσύνη εάν κάποιος έχει υποστεί ζημία, πχ κλοπή στοιχείων από κυβερνοεπιθέσεις χάκερ κατά εταιρειών
- να ενημερωθουν από την εταιρεία μέσα σε 72 ώρες αν online προσωπικά δεδομένα χαθούν ή κλαπούν

Υποχρεώσεις των επιχειρήσεων με τον GDPR:

Τη στιγμή της συλλογής δεδομένων, πρέπει να παρέχονται με σαφήνεια στα άτομα πληροφορίες οπωσδήποτε για τα εξής (1/2):

- ποια είναι η εταιρεία ή ο οργανισμός (τα στοιχεία επικοινωνίας και τα στοιχεία του Υπεύθυνου Προστασίας Δεδομένων, εάν υπάρχει)
- τον λόγο για τον οποίο θα χρησιμοποιηθούν τα παρεχόμενα δεδομένα προσωπικού χαρακτήρα (σκοποί)
- τις κατηγορίες των σχετικών δεδομένων προσωπικού χαρακτήρα
- τη νομική αιτιολόγηση για την επεξεργασία των δεδομένων των ατόμων
- το χρονικό διάστημα για το οποίο θα φυλαχθούν τα δεδομένα
- ποιοι άλλοι μπορεί να τα λάβουν

Υποχρεώσεις των επιχειρήσεων με τον GDPR:

Τη στιγμή της συλλογής δεδομένων, πρέπει να παρέχονται με σαφήνεια στα άτομα πληροφορίες οπωσδήποτε για τα εξής (2/2):

- εάν τα δεδομένα τους προσωπικού χαρακτήρα θα διαβιβαστούν σε αποδέκτη εκτός της ΕΕ
- ότι τα άτομα έχουν δικαίωμα να λάβουν αντίγραφο των δεδομένων (δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα) και άλλα βασικά δικαιώματα στον τομέα της προστασίας δεδομένων
- το δικαίωμα υποβολής καταγγελίας ενώπιον αρχής προστασίας δεδομένων (ΑΠΔ)
- το δικαίωμα ανάκλησης της συγκατάθεσής τους οποιαδήποτε στιγμή
- ενδεχομένως, την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων και τη λογική αυτής, συμπεριλαμβανομένων των σχετικών συνεπειών

Υποχρεώσεις των επιχειρήσεων με τον GDPR:

Η αρχή της λογοδοσίας αποτελεί ομπρέλα υπό την οποία τίθενται όλες οι πράξεις επεξεργασίας και τονίζει τόσο την υποχρέωση συμμόρφωσης όσο και απόδειξης της συμμόρφωσής του αυτής

Για παράδειγμα όταν η επεξεργασία βασίζεται στην συγκατάθεση, ο υπεύθυνος πρέπει να μπορεί να αποδείξει ότι η συγκατάθεση έλαβε χώρα

Υποχρεώσεις των επιχειρήσεων με τον GDPR:

Η επιχείρηση, προκειμένου να συμμορφώνεται με τις επιταγές του Κανονισμού και να αποδεικνύει την συμμόρφωση της, λαμβάνει **κατάλληλα τεχνικά και οργανωτικά μέτρα**, όπως:

- ψευδωνυμοποίηση,
- μέτρα σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων και
- μέτρα σχεδιασμένα, ώστε να προάγουν την διαφάνεια, όσον αφορά τις λειτουργίες και τις επεξεργασίες δεδομένων, προκειμένου να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφαλείας

Υποχρεώσεις των επιχειρήσεων με τον GDPR:

Γνωστοποίηση Παραβίασης δεδομένων προσωπικού χαρακτήρα

Εντός 72 ωρών από την στιγμή της απόκτησης γνώσης του γεγονότος της παραβίασης, ο υπεύθυνος οφείλει να την γνωστοποιήσει στην αρμόδια Εποπτική Αρχή. Αυτό δεν είναι υποχρεωτικό όταν δεν ενδέχεται να προκληθεί κίνδυνος από την παραβίαση. Την απουσία κινδύνου οφείλει να αποδείξει ο υπεύθυνος. Επίσης, οφείλει να δικαιολογήσει την παραβίαση βάσει πραγματικών περιστατικών και να αναφερθεί στις συνέπειες και τα ληφθέντα διορθωτικά μέτρα, δίνοντας την δυνατότητα στην Εποπτική Αρχή να επαληθεύσει την συμμόρφωση.

Υποχρεώσεις των επιχειρήσεων με τον GDPR:

Εκτίμηση Αντικτύπου σχετικά με την προστασία των δεδομένων

Ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

Υποχρεώσεις των επιχειρήσεων με τον GDPR:

Ορισμός Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer)

Οι επιχειρήσεις και οι οργανισμοί ορισμένης κλίμακας και δραστηριότητας οφείλουν να ορίζουν έναν υπεύθυνο προστασίας δεδομένων (DPO) στα καθήκοντα του οποίου περιλαμβάνεται και η παρακολούθηση η συμμόρφωσης με τον Κανονισμό και τις πολιτικές προστασίας προσωπικών δεδομένων του υπευθύνου ή εκτελούντος την επεξεργασία. Επίσης, αναλαμβάνει την ανάθεση αρμοδιοτήτων και την ευαισθητοποίηση και κατάρτιση των υπαλλήλων, που διαχειρίζονται και επεξεργάζονται προσωπικά δεδομένα ενώ, παράλληλα, προβαίνει και στους απαραίτητους ελέγχους.

Το Πρότυπο ISO/IEC 27001:2013 - Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management Systems)

Ο GDPR ενθαρρύνει τη χρήση συστημάτων πιστοποίησης όπως το Πρότυπο ISO/IEC 27001:2013 για να επιδείξει η επιχείρηση ότι διαχειρίζεται ενεργά την ασφάλεια των δεδομένων της σύμφωνα με τις διεθνείς βέλτιστες πρακτικές.

Το Πρότυπο ISO / IEC 27001: 2013 καθορίζει τις απαιτήσεις για τη δημιουργία, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών.

Τα επιχειρησιακά οφέλη με τον GDPR:

- Ανάπτυξη σχέσης εμπιστοσύνης με τους πελάτες
- Βελτίωση της εταιρικής εικόνας και φήμης
- Βελτίωση της διαχείρισης των δεδομένων
- Βελτίωση της ασφάλειας των πληροφοριών
- Βελτίωση ανταγωνιστικού πλεονεκτήματος

Ε Υ Χ Α Ρ Ι Σ Τ Ω

ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ !

Τηλέφωνο / FAX : 2 1 0 - 3 8 9 3 9 4 5
E-mail : drososg@ggb.gr