MICHALOPOULOU & ASSOCIATES

Law under the microscope

Divani Caravel, 9 Νοεμβρίου 2017

Οι ΧΡΥΣΟΙ ΚΑΝΟΝΕΣ για τις ΕΤΑΙΡΕΙΕΣ ΣΥΜΜΟΡΦΩΣΗΣ ΑΣΘΕΝΩΝ υπό την σκέπη του GDPR

Michalopoulou & Associates | 40 Ag. Konstantinou st. | "Aithrio" Business Center (A 16-18) | 15 124 Marousi Athens Greece
T : +30 210 330 52 30 | F : +30 210 330 52 32 | info@lawgroup.gr | www.lawgroup.gr

"There's a lot in the GDPR you'll recognize from the current law, but make no mistake, this one's a game changer for everyone"

Elizabeth Denham, Information Commissioner, *January 2017*

I. ΕΙΣΑΓΩΓΗ

- **Ο νέος Γενικός Κανονισμός για την προστασία προσωπικών δεδομένων (GDPR 679/2016) αναμένεται να τεθεί σε εφαρμογή στις 25 Μαϊου 2018.**
- **Έχει την ίδια μορφή και το ίδιο περιεχόμενο για όλα τα κράτη-μέλη της ΕΕ.**
- **Πρόστιμα έως 20.000.000 € ή 4% του παγκόσμιου τζίρου.**
- **Ο GDPR θα επηρεάσει κάθε επιχείρηση και κάθε δημόσια αρχή η οποία προβαίνει σε επεξεργασία προσωπικών δεδομένων.**
- **Ο νέος GDPR αφορά <u>κάθε τμήμα μίας επιχείρησης και όχι μόνο τα IT Departments.</u>**

ΙΙ. ΤΙ ΑΛΛΑΖΕΙ

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ GDPR

Ο GDPR εφαρμόζεται ανεξάρτητα εάν η επεξεργασία πραγματοποιείται εντός ή εκτός της ΕΕ από υπεύθυνους ή/και εκτελούντες με έδρα (κύρια εγκατάσταση) εντός ή εκτός της ΕΕ αρκεί η επεξεργασία να αφορά προσωπικά δεδομένα Ευρωπαίων πολιτών.

SOS Διασυνοριακή επεξεργασία!

ΤΙ ΑΦΟΡΑ?

Τα προσωπικά δεδομένα τα οποία τυγχάνουν επεξεργασίας.

ΤΙ ΝΟΕΙΤΑΙ ΩΣ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ?

η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή **η καταστροφή.**

ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ
Κάθε πληροφορία που αφορά **ταυτοποιημένο ή ταυτοποιήσιμο** φυσικό πρόσωπο.

ΔΕΔΟΜΕΝΑ ΥΓΕΙΑΣ
Ευαίσθητα δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου.

NEW Βιομετρικά:
Προκύπτουν από ειδική τεχνική επεξεργασία και επιβεβαιώνουν αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου πχ. εικόνες προσώπου, δακτυλοσκοπικά δεδομένα.

NEW Γενετικά δεδομένα: χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν πχ. DNA test.

NEW ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ

1) **Δικαίωμα πρόσβασης σε δεδομένα**
2) **Δικαίωμα διαγραφής ή δικαίωμα στην "λήθη"**
3) **Δικαίωμα περιορισμού της επεξεργασίας**
4) **Δικαίωμα στη φορητότητα των δεδομένων**
5) **Δικαίωμα εναντίωσης:**

SOS ΕΜΠΟΡΙΚΗ ΠΡΟΩΘΗΣΗ Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή (Direct Marketing)

- το αργότερο συγκατάθεση κατά την πρώτη επικοινωνία

εξαίρεση:

- - για ευρευνητικό σκοπό μόνο για λόγους δημοσίου συμφέροντος

SOS Profiling απαγορεύεται εκτός:

- - συγκατάθεση υποκειμένου
- - λόγοι δημοσίου συμφέροντος

SOS ΣΥΓΚΑΤΑΘΕΣΗ του υποκειμένου:

- **Ρητή**
- **Ειδική**
- **Ελεύθερη**
- **Συγκεκριμένη**
- **Εν επιγνώσει**
- **Ανακλητή ανά πάσα στιγμή**

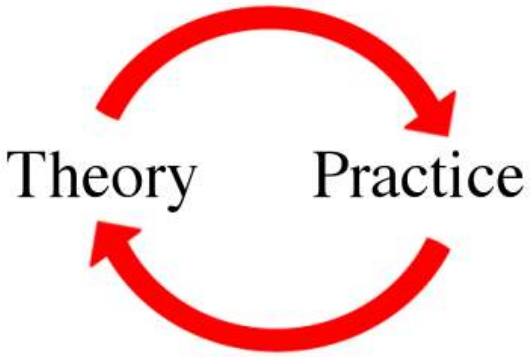
GDPR:

- Θα τεθεί σε εφαρμογή στις 25 Μαϊου, 2018
- TOP GDPR challenge: ACCOUNTABILITY → ΥΠΕΥΘΥΝΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ (CONTROLLERS) καθορίζουν τους σκοπούς, τρόπο επεξεργασίας
  &
  ΕΚΤΕΛΟΥΝΤΕΣ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ (PROCESSORS) επεξεργάζονται δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας
- Περισσότερα δικαιώματα για τα υποκείμενα προσωπικών δεδομένων vs περισσότερες υποχρεώσεις για τους υπευθύνους επεξεργασίας
- ΠΡΟΣΤΙΜΑ ΕΩΣ 20.000.000 € ή 4% του παγκόσμιου τζίρου/ παραβίαση υποκειμένου

III. ΤΙ ΣΗΜΑΙΝΕΙ ΠΡΑΚΤΙΚΑ ΓΙΑ ΤΙΣ ΕΤΑΙΡΕΙΕΣ ΣΥΜΜΟΡΦΩΣΗΣ ΑΣΘΕΝΩΝ?

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΝΟΜΙΜΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

- νομιμότητα, αντικειμενικότητα και διαφάνεια
- περιορισμός του σκοπού
- ελαχιστοποίηση των δεδομένων
- ακρίβεια
- περιορισμός της περιόδου αποθήκευσης
- ακεραιότητα και εμπιστευτικότητα
- λογοδοσία



NEW ΕΥΘΥΝΗ ΥΠΕΥΘΥΝΟΥ & ΕΚΤΕΛΟΥΝΤΟΣ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

1. Εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων
2. Εφαρμογή κατάλληλων πολιτικών (privacy policies)
3. Τήρηση κανόνων δεοντολογίας
4. Τήρηση μηχανισμού πιστοποίησης

ACTIONS

→ Προστασία εξ ορισμού (Data Protection by Default) & ήδη από το σχεδιασμό (Data Protection by Design)

→ Τήρηση Αρχείων Δραστηριοτήτων Επεξεργασίας

→ Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων Data Protection Impact Assessment (DPIA)

→ Τήρηση εγκεκριμένου Κώδικα Δεοντολογίας→ Διορισμός DPO

SOS ΔΙΑΠΙΣΤΩΣΗ ΠΑΡΑΒΙΑΣΗΣ

ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ: εντός 72 ΩΡΩΝ από τη στιγμή της λήψης γνώσης του γεγονότος→ **ΕΝΗΜΕΡΩΣΗ ΕΠΟΠΤΙΚΗΣ ΑΡΧΗΣ& ΥΠΟΚΕΙΜΕΝΟ ΔΕΔΟΜΕΝΩΝ:**

ΕΚΤΕΛΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ: αμέσως μόλις αντιληφθεί το γεγονός → ΥΠΕΥΘΥΝΟ ΕΠΕΞΕΡΓΑΣΙΑΣ

Υπεύθυνος Προστασίας δεδομένων (DPO)

ΚΑΘΗΚΟΝΤΑ ΤΟΥ DPO

- ενημέρωση & ευαισθητοποίηση εταιρείας
- παρακολούθηση της συμμόρφωσης με τον Κανονισμό και με την νομοθεσία
- παροχή συμβουλών για τις DPIA
- πρόσωπο επικοινωνίας με την Αρχή (& διαβούλευση) & τα υποκείμενα δικαιωμάτων
- σχεδιασμός της Πολιτικής Προστασίας Προσωπικών Δεδομένων και μηχανισμών Ελέγχου
- ανάπτυξη δίαυλου επικοινωνίας με όλα τα τμήματα (Νομικό, HR, IT, IS, Compliance)
- εφαρμογή των Compliance program, policies & procedures.

ΠΩΣ ΝΑ ΠΡΟΕΤΟΙΜΑΣΤΕΙΤΕ

- Αύξηση της ευαισθητοποίησης των υπευθύνων λήψης αποφάσεων και εχόντων θέσεων ευθύνης
- Καταγραφή των προσωπικών δεδομένων που συλλέγονται
- Διασφάλιση των δικαιωμάτων των υποκειμένων
- Εξασφάλιση νόμιμης βάσης για την επεξεργασία των προσωπικών δεδομένων
- Λήψη ρητής συγκατάθεσης υποκειμένων
- Διαχείριση παραβιάσεων
- Εφαρμογή Πολιτικής Απορρήτου“by design”, “by default”
- Σύνταξη Κώδικα Δεοντολογίας
- Τήρηση Έγγραφων Συμβάσεων με τον Υπεύθυνο Επεξεργασίας
- Ενημέρωση Υπευθύνου για τυχόν υπο-εκτελούντες την επεξεργασία
- Διορισμός DPO

"GDPR can be boiled down to two words:

"Transparency" and "Accountability"

Rob Lyke, Deputy Commissioner, May 2017

Ευχαριστώ

Ιωάννα Μιχαλοπούλου
Δικηγόρος LL.M

Corporate and Commercial Lawyer
Medical, Pharma & Life Sciences Law Specialist

imicha@lawgroup.gr | www.lawgroup.gr | LinkedIn