



MICHALOPOULOU
& ASSOCIATES

Law under the microscope

«Νέας γενιάς» κατηγορίες δεδομένων και τι σημαίνει αυτό πρακτικά για το ρόλο του DPO

στην Ιατρική Κοινότητα
Τετάρτη 18 Απριλίου 2018



Αντικείμενο και Στόχοι του νέου Κανονισμού

- Έχει ως αντικείμενο τη θέσπιση κανόνων που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- Στόχος του νέου Κανονισμού είναι η ομοιόμορφη και αποτελεσματικότερη προστασία των πολιτών της ΕΕ –άμεση εφαρμογή στα κράτη-μέλη.
- Η εφαρμογή του είναι υποχρεωτική και άμεση, για όσους τηρούν και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για ιδιώτες και επιχειρήσεις, είτε για φορείς του Δημοσίου.
- Αφορά μικρές και μεγάλες επιχειρήσεις ανεξαρτήτως δραστηριότητας και κλάδου, ενώ καταλαμβάνει την επεξεργασία δεδομένων και την τήρηση αρχείου, είτε αυτή είναι μερικά ή ολικά αυτοματοποιημένη, είτε όχι.

GDPR

General
Data
Protection
Regulation



Κυριότερα Σημεία του Κανονισμού 679/2016

- Πρόκειται για **Κανονισμό** και όχι Οδηγία, επομένως **δεν εναπόκειται στα κράτη μέλη**, ο τρόπος και ο χρόνος εφαρμογής.
- **Εξω-εδαφική** Εφαρμογή-υπεύθυνους & εκτελούντες την επεξεργασία που είναι εγκατεστημένοι εκτός Ένωσης, αλλά επεξεργάζονται δεδομένα Ευρωπαίων Πολιτών
- **Νέα δικαιώματα** υποκειμένων
- **Νέες και αυστηρότερες υποχρεώσεις** υπευθύνων και εκτελούντων
- **Αρχή της Λογοδοσίας-δεν** απαιτείται πλέον **άδεια** από την αρμόδια Αρχή και μετακυλύεται η ευθύνη στον υπεύθυνο ή/και στον εκτελούντα την επεξεργασία
- Καθορισμός **νέων ρόλων** μέσα στην επιχείρηση(DPO)
- **Υψηλότερα πρόστιμα, έως και 20.000.000 ευρώ ή 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών** του προηγούμενου οικονομικού έτους.
- **Νέες κατηγορίες** ευαίσθητων δεδομένων, όπως τα **βιομετρικά και τα γενετικά δεδομένα** ενώ ειδικά για τις εταιρείες του Χώρου της Υγείας υπάρχει περαιτέρω εξειδίκευση των χαρακτηριζόμενων ως **δεδομένων υγείας**



Βιομετρικά Δεδομένα

- Με βάση τον Κανονισμό ως βιομετρικά δεδομένα ορίζονται «τα δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεδεμένη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες πρόσωπο ή δακτυλοσκοπικά δεδομένα»
- Βάσει του ορισμού αυτού τρία είναι τα βασικά στοιχεία των βιομετρικών δεδομένων:
 - α) ότι βασίζονται σε **ειδική τεχνική επεξεργασία**, στις βιομετρικές μεθόδους,
 - β) οι βιομετρικές τεχνικές έχουν ως αντικείμενο **το άτομο**,
 - γ) αποσκοπούν στην **αδιαμφισβήτητη ταυτοποίηση** ενός συγκεκριμένου φυσικού προσώπου.

Βιομετρικά Δεδομένα

- Η συλλογή των βιομετρικών δεδομένων γίνεται κατά τη διαδικασία της εγγραφής του ατόμου στο **βιομετρικό σύστημα**.
- **Βιομετρικά συστήματα:** εφαρμογές για την **αυτόματη αναγνώριση** ή και **επαλήθευση της ταυτότητας ενός φυσικού προσώπου** & την **πιστοποίηση της αυθεντικότητας** δηλούμενης ταυτότητας μέσω της χρήσης εξατομικευμένων σωματικών χαρακτηριστικών
- Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται από βιομετρικά συστήματα αφορούν τα φυσικά χαρακτηριστικά ενός ανθρώπου ή τα στοιχεία της συμπεριφοράς του τα οποία τον προσδιορίζουν μοναδικά.

Χαρακτηριστικά παραδείγματα χρήσης βιομετρικών συστημάτων:

- για την **ασφάλεια χρήσης λογισμικών**
- στην **ηλεκτρονική τραπεζική,**
- στην **ηλεκτρονική υγεία,**
- στην **επιστημονική έρευνα,**
- Στις **προηγμένες συσκευές κινητής τηλεφωνίας**



Γενετικά Δεδομένα

- Ως γενετικά δεδομένα κατά τον Κανονισμό ορίζονται «τα δεδομένα προσωπικού χαρακτήρα που **αφορούν τα γενετικά χαρακτηριστικά** φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, **ιδίως από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου** και τα οποία παρέχουν **μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου**»
- Παρέχουν επιστημονικές, ιατρικές και προσωπικές πληροφορίες καίριες για το άτομο αλλά συνάμα για τους ανιόντες και τους κατιόντες του.
- Οδηγούν σε διαπίστωση της ταυτότητας του προσώπου μέσω του γενετικού αποτυπώματος, καθώς είναι **μοναδικά** για τον καθένα
- Υπάρχουν σε όλους τους ανθρώπους (**καθολικά**)
- Είναι **μετρήσιμα**, καθώς τα σχετικά βιολογικά δείγματα μπορούν να αναλυθούν με τα σύγχρονα επιστημονικά εργαλεία

Σύννομη Επεξεργασία Ειδικών Κατηγοριών Προσωπικών Δεδομένων

Η επεξεργασία των **ειδικών κατηγοριών προσωπικών δεδομένων**-δηλαδή και των **βιομετρικών και γενετικών δεδομένων** απαγορεύεται ρητώς, εκτός και αν τηρείται μια από τις κάτωθι εκ του Κανονισμού προβλεπόμενες προϋποθέσεις:

- ✓ το υποκείμενο των δεδομένων έχει παράσχει **ρητή συγκατάθεση**,
- ✓ η επεξεργασία είναι απαραίτητη για την **εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου**,
- ✓ η επεξεργασία είναι απαραίτητη για την **προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί**



Σύννομη Επεξεργασία Ειδικών Κατηγοριών Προσωπικών Δεδομένων

- ✓ η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία **έχουν δημοσιοποιηθεί από το υποκείμενο των δεδομένων,**
- ✓ η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη **νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,**
- ✓ η επεξεργασία είναι απαραίτητη για σκοπούς **προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου,**
- ✓ η επεξεργασία είναι απαραίτητη για σκοπούς **επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.**

!!Με βάση το σχέδιο του **ελληνικού εφαρμοστικού νόμου** προκρίνεται για την επεξεργασία ειδικών κατηγοριών δεδομένων χρήση **τεχνικών μέτρων ασφάλειας** όπως:

- **Η ψευδωνυμοποίηση**
- **Η κρυπτογράφηση**

Υπεύθυνος Προστασίας Δεδομένων (DPO): Ο ρόλος και τα καθήκοντα του

Απαραίτητος ο διορισμός Υπευθύνου Προστασίας δεδομένων (DPO) όταν:

α) Η επεξεργασία διενεργείται από **Δημόσια αρχή** ή **φορέα**

β) οι *βασικές δραστηριότητες* του υπευθύνου ή του εκτελούντος την επεξεργασία περιλαμβάνουν **Τακτική και Συστηματική παρακολούθηση** των υποκειμένων των δεδομένων σε **μεγάλη κλίμακα**

γ) οι βασικές δραστηριότητες του υπευθύνου ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία **Ειδικών κατηγοριών δεδομένων (ευαίσθητα)**

πχ. Βιομετρικά, γενετικά, **δεδομένα υγείας**

Προσοχή: Στην έννοια των δραστηριοτήτων «*μεγάλης κλίμακας*» υπάγονται τα νοσοκομεία, οι ασφαλιστικές εταιρείες όπως και οι επιχειρήσεις ιατροτεχνολογικών προϊόντων που δύνανται να επεξεργάζονται πληθώρα προσωπικών δεδομένων και δη ευαίσθητων, όπως δεδομένων υγείας ασθενών.



Υπεύθυνος Προστασίας Δεδομένων (DPO): Ο ρόλος και τα καθήκοντα του

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 programs, policies & procedures.

Υπεύθυνος Προστασίας Δεδομένων (DPO): Ο ρόλος και τα καθήκοντα του

- Απολαμβάνει **Ανεξαρτησίας**
- Τήρηση **Εμπιστευτικότητας**
- Λογοδοτεί στο **Ανώτατο Διοικητικό** επίπεδο
- **Full # Part-time job? NOT a Manager!**
- Όμιλος Επιχειρήσεων: **1 and Only** αλλά με **εύκολη πρόσβαση** στον υπεύθυνο προστασίας ή εκτελούντα την επεξεργασία
- **DPO team** με κάποιο lead contact
- DPO contact details στην Αρχή
- Dedicated hotline?



Ευχαριστώ



Ιωάννα Μιχαλοπούλου
Δικηγόρος LL.M

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

imicha@lawgroup.gr | www.lawgroup.gr | **Linked in**