Ο ρόλος του Υπεύθυνου Προστασίας Δεδομένων (DPO) στον τομέα της υγείας

Παρουσίαση

Ράσση Κωνσταντία

Senior Consultant

ALPHA PLAN consultants

Εισαγωγή (1/2)

General Data Protection Regulation

Ο Νέος Κανονισμός:

- ✓**16 Απριλίου 2016** ψήφισμα του Ευρωπαϊκού Κοινοβουλίου, αφορά τον Γενικό Κανονισμό Προσωπικών Δεδομένων
- ✓**νομοθέτημα άμεσης εφαρμογής** σε όλα τα κράτη μέλη της Ε.Ε.
- ✓**επιβάλλει πρόσθετες υποχρεώσεις** σε Υπεύθυνους Επεξεργασίας και Εκτελούντες την επεξεργασία προσωπικών δεδομένων
- ✓θα τεθεί σε ισχύ στις **25 Μαΐου 2018**
- ✓Το νομοθέτημα καθιστά υποχρεωτικό το **διορισμό Data Protection Officer (DPO),** σε ορισμένες κατηγορίες επιχειρήσεων.

ALPHA PLAN consultants

Εισαγωγή (2/2)

Ο Νέος Κανονισμός:

- ✓ **η Επιτροπή του άρθρου 29** αποτελεί την **εποπτεύουσα αρχή** των Εθνικών Αρχών Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Συμβουλευτικό Όργανο της Ευρωπαϊκής Επιτροπής

- ✓ στις **16 Δεκεμβρίου 2016** εξέδωσε **διευκρινιστικές οδηγίες** σχετικά με τον ρόλο και την ευθύνη του DPO αποσαφηνίζοντας μερικά ερωτήματα αναφορικά με τον θεσμό που αποκτά νέα βαρύτητα μετά την εισαγωγή του Κανονισμού.

- ✓ στις **27 Φεβρουαρίου 2018** η **Α.Π.Δ.Π.Χ.** εξέδωσε διευκρινιστικές οδηγίες σχετικά με τον ρόλο και την ευθύνη του DPO.

Καθορισμός Data Protection Officer (DPO) σε μια Επιχείρηση

Τρεις βασικές κατηγορίες περιπτώσεων **διορισμού** (DPO):

1. η επεξεργασία διενεργείται από **δημόσια αρχή ή φορέα.**
2. Όταν απαιτείται **τακτική και συστηματική παρακολούθηση** των υποκειμένων των δεδομένων σε μεγάλη κλίμακα.
3. Όταν διενεργείται **μεγάλης κλίμακας επεξεργασίας ειδικών κατηγοριών δεδομένων** ή δεδομένα προσωπικού χαρακτήρα που αφορούν **ποινικές καταδίκες** και **αδικήματα**.

ALPHA PLAN consultants

Διευκρινήσεις της Επιτροπής του Άρθρου 29 (1/3)

- «**Βασικές δραστηριότητες**» = «αναπόσπαστο τμήμα της επιδίωξης των εταιρικών σκοπών του Υπευθύνου ή Εκτελούντος την Επεξεργασία» Π.χ:

  - Εταιρία παροχής υπηρεσιών ασφαλείας, η οποία ελέγχει / παρακολουθεί δημόσιο ή ιδιωτικό χώρο
  - Επεξεργασία Ιατρικών Φακέλων Ασθενών
  - Επεξεργασία προσωπικών δεδομένων υπαλλήλων από εξωτερικό συνεργάτη που διαχειρίζεται τη μισθοδοσία μιας εταιρίας

ALPHA PLAN consultants

Διευκρινήσεις της Επιτροπής του Άρθρου 29 (2/3)

- «**Συστηματική**» και «**Τακτική**» = παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα με μορφή on line παρακολούθησης π.χ.:

- Παρακολούθηση των μετακινήσεων του υποκειμένου (location tracking)
- Επεξεργασία που στοχεύει στον καθορισμό της καταναλωτικής συμπεριφοράς και συνηθειών του υποκειμένου για διαφημιστικούς σκοπούς (behavioral advertising)
- Καθορισμός Προφίλ του υποκειμένου με βάση συγκεκριμένα Π.Δ. που αφορούν την καταναλωτική του ταυτότητα, προτιμήσεις, επισκεψιμότητα σε συγκεκριμένα καταστήματα, (Profiling)

ALPHA PLAN consultants

Διευκρινήσεις της Επιτροπής του Άρθρου 29 (3/3)

- «**Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα**» σε «**Μεγάλη Κλίμακα**», όπως δεδομένα που αφορούν:

Ειδικές κατηγορίες

Θρησκεία

Πολιτικές Πεποιθήσεις

Σεξουαλικός Προσανατολισμός

Γενετικά Δεδομένα ή Υλικό

Βιομετρικά Στοιχεία

Συμμετοχή σε Συνδικαλιστικές Οργανώσεις

DPO

Μεγάλη Κλίμακα

1. Αριθμός Εμπλεκόμενων Υποκειμένων
2. Όγκος & Εύρος Δεδομένων
3. Διάρκεια Επεξεργασίας
4. Γεωγραφική Έκταση

ALPHA PLAN consultants

Παραδείγματα

Που δεν συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων,

- η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό και
- η επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

ALPHA PLAN consultants

Υποχρεώσεις Εργοδότη

Ο υπεύθυνος επεξεργασίας και ο **εκτελών** την επεξεργασία ορίζουν DPO εξασφαλίζουν ότι:

- ✓ **Συμμετέχει σε όλα** τα ζητήματα σχετικά με την Προστασία Προσωπικών Δεδομένων
- ✓ **Ελεύθερη** πρόσβαση σε δεδομένων και πράξεις επεξεργασίας
- ✓ **Έχει στη διάθεση του** τους απαραίτητους πόρους για την εκπλήρωση των καθηκόντων του
- ✓ **Εκπληρώνει** τα καθήκοντα του με ανεξάρτητο τρόπο
- ✓ **Δεν απολύεται,** ούτε υφίσταται κυρώσεις
- ✓ **Λογοδοτεί** απευθείας με το ανώτερο διοικητικό επίπεδο του εργοδότη
- ✓ Όταν ασκεί πρόσθετα καθήκοντα, αυτά να **μην συνεπάγονται σύγκρουση συμφερόντων**
- ✓ Δεσμεύεται από την τήρηση **Απορρήτου** & της **Εμπιστευτικότητας**

ALPHA PLAN consultants

Ορισμός του DPO

Ο υπεύθυνος επεξεργασίας και ο **εκτελών** την επεξεργασία ορίζουν DPO:

- ✓ Βάσει **επαγγελματικών προσόντων** και ιδίως βάσει της **εμπειρογνωσίας** που διαθέτει στον **τομέα του δικαίου** και των **πρακτικών περί προστασίας δεδομένων**
- ✓ Μπορεί να είναι **μέλος του προσωπικού** ή **εξωτερικός συνεργάτης**
- ✓ Δημοσιεύουν **τα στοιχεία επικοινωνίας** του DPO και τα ανακοινώνουν στην **εποπτική αρχή**

ALPHA PLAN consultants

Ένας DPO για περισσότερους φορείς ή οργανισμούς;

Όμιλος επιχειρήσεων ή περισσότεροι δημόσιοι φορείς, λαμβάνοντας υπόψη το μέγεθος και την οργανωτική τους δομή, **μπορούν να ορίσουν έναν μόνο DPO,** υπό την προϋπόθεση να είναι **διαθέσιμος και εύκολα προσβάσιμος** σε κάθε εγκατάσταση ή φορέα **είτε με φυσική παρουσία** στις ίδιες εγκαταστάσεις με τους υπαλλήλους, **είτε μέσω ανοικτής τηλεφωνικής γραμμής** ή **άλλου ασφαλούς μέσου επικοινωνίας** και σε γλώσσα που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα οικεία υποκείμενα των δεδομένων.

ALPHA PLAN consultants

Καθήκοντα DPO

Καθήκοντα DPO

- Ενημερώνει και συμβουλεύει
- Παρακολουθεί την Εσωτερική Συμμόρφωση
- Παρέχει συμβουλές για εκτίμηση Αντικτύπου (DPIA) & παρακολούθηση υλοποίησης
- Σημείο Επαφής ΑΠΔΠΧ & Υποκειμένου
- Συνεργασία με την ΑΠΔΠΧ

ALPHA PLAN consultants

Απαιτούμενα Προσόντα ενός DPO

- ✓ **κατανοεί σε βάθος** τις απαιτήσεις του GDPR
- ✓ **γνωρίζει τις δραστηριότητες** που ενέχουν επεξεργασία δεδομένων στον οργανισμό που εκπροσωπεί
- ✓ **γνωρίζει τις τεχνολογίες IT** και των μεθόδων ασφαλείας πληροφοριών που εφαρμόζονται
- ✓ **δείχνει ακεραιότητα** και **επαγγελματικό ήθος**
- ✓ **είναι ανεξάρτητος** προς αποφυγή **σύγκρουσης συμφερόντων** με άλλους εργασιακούς ρόλους που τυχόν κατέχει

ALPHA PLAN consultants

Αποστολή και Ευθύνη

- ✓ Η αποστολή του είναι κυρίως το να **προστατέψει** την επιχείρηση από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών **προστίμων**

- ✓ **ΔΕΝ ΘΑ ΕΧΕΙ ΠΡΟΣΩΠΙΚΗ ΕΥΘΥΝΗ**, αλλά η ευθύνη για την παραβίαση της νομοθεσίας σχετικά με τα Δεδομένα Προσωπικού Χαρακτήρα παραμένει στη Διοίκηση

ALPHA PLAN consultants

Παραδείγματα στον χώρο της υγείας

- ✓ Δικαιούται ένας ασθενής να ζητήσει από το νοσηλευτικό ίδρυμα να **διαγράψει τον ιατρικό του φάκελο** από τα αρχεία του;
- ✓ Δικαιούται το **νοσοκομείο να διαγράψει τους ιατρικούς φακέλους** των ασθενών από τα αρχεία του;
- ✓ Δικαιούται το νοσηλευτικό ίδρυμα να **χορηγήσει αντίγραφα του ιατρικού φακέλου ασθενούς που έχει αποβιώσει σε τρίτο**;
- ✓ Μπορούν οι **φορολογικές αρχές** να έχουν πρόσβαση στους ιατρικούς φακέλους των ασθενών;

ALPHA PLAN consultants

Παραδείγματα στον χώρο της υγείας

- ✓ Μπορεί κάποιος **τρίτος να λάβει αντίγραφα ιατρικού φακέλου** ασθενούς;
- ✓ Μπορεί **το νοσηλευτικό ίδρυμα** να χρησιμοποιήσει στοιχεία από τον ιατρικό φάκελο του ασθενούς **για να υποστηρίξει μια υπόθεσή του στα δικαστήρια**;
- ✓ Μπορεί **ιατρός του νοσηλευτικού ιδρύματος** να χρησιμοποιήσει **στοιχεία από τον ιατρικό φάκελο** του ασθενούς για να υποστηρίξει μια υπόθεσή του στα δικαστήρια;
- ✓ Μπορεί ένας **ιδιώτης ιατρός** να χρησιμοποιήσει στοιχεία από το ιατρικό αρχείο που τηρεί και **να τα δημοσιεύσει σε ένα επιστημονικό άρθρο**;

ALPHA PLAN consultants

Εσωτερικός ή Εξωτερικός DPO

ΕΣΩΤΕΡΙΚΟΣ

Γνωρίζει καλύτερα:

- τη φιλοσοφία
- τις πολιτικές και
- τα πρόσωπα ενός Οργανισμού

- Πρέπει να αναφέρεται στην ανώτατη Διοίκηση του Οργανισμού χωρίς να παρεμβάλλεται ενδιάμεσος αναφοράς

ALPHA PLAN consultants

Εσωτερικός ή Εξωτερικός DPO (2/2)

ΕΞΩΤΕΡΙΚΟΣ

- Εξασφαλίζει την απαιτούμενη λειτουργική ανεξαρτησία έναντι της Διοίκησης
- Μπορεί να διαφωνεί με τη Διοίκηση κατά την άσκηση των καθηκόντων, χωρίς ωστόσο αυτό να αποτελεί αιτία καταγγελίας της σύμβασής του

- Μικρότερο επίπεδο γνώσης λειτουργίας του Οργανισμού

Συμπεράσματα

Υποστηρίζεται ότι συγκεκριμένοι ρόλοι όπως:
HR Director, **Marketing Director**, **IT Director** και
εσωτερικός Νομικός Σύμβουλος
ΔΕΝ ΜΠΟΡΟΥΝ
να ασκούν ταυτόχρονα με τον ρόλο τους και καθήκοντα D.P.O.

Πανευρωπαϊκές έρευνες (μελέτη του iapp) συμπέραναν ότι:

α) μόνο το **60%** των επιχειρήσεων είναι έτοιμες
β) θα υπάρξει ανάγκη για διορισμού/ δημιουργία θέσεων εργασίας για **28.000 DPO !!!!!!**

ALPHA PLAN consultants

Εκπαίδευση

Η ουσιαστική επιμόρφωση των D.P.O. επιτυγχάνεται μέσω:

- ✓ μελέτης case studies,
- ✓ χρήση οδηγών για τηδημιουργία Privacy Impact Assessments και
- ✓ Incident Response Planning, τα οποία αποτελούν βασικά εργαλεία των DPO's.

Ο ΓΚΠΔ **δεν** θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO,
ούτε ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση
(σχετική ανακοίνωση της ΑΠΔΠΧ 7/2017)

ALPHA PLAN consultants

Πιστοποίηση

Ο κανονισμός παροτρύνει τη **θέσπιση** μηχανισμών πιστοποίησης προστασίας δεδομένων, σφραγίδων και σημάτων προστασίας.

- Δημιουργεί αποδείξεις και κατάλληλες **εγγυήσεις** για τον οργανισμό
- Είναι εθελοντική και διαθέσιμη μέσω **διαφανούς** διαδικασίας
- **Δεν περιορίζει** την ευθύνη του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία
- Χορηγείται από τους **φορείς** πιστοποίησης. Είναι **3ετής** και μπορεί να ανανεωθεί/ ανακληθεί

ALPHA PLAN consultants

Συμβούλιο Προστασίας

Το **Συμβούλιο Προστασίας** δεδομένων:

- εγκρίνει τα κριτήρια πιστοποίησης και αυτό μπορεί να οδηγήσει σε κοινή πιστοποίηση, την **Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων**
- συγκεντρώνει όλους τους **μηχανισμούς πιστοποίησης** και τις σφραγίδες και τα σήματα προστασίας δεδομένων σε μητρώο και τα καθιστά διαθέσιμα στο κοινό με κάθε μέσο.

Μηχανισμοί Συμμόρφωσης (1/2)

ISO 27001

- ✓ είναι το βιομηχανικό πρότυπο για τη διαχείριση της ασφάλειας των πληροφοριών
- ✓ βοηθά τους οργανισμούς να ανταποκριθούν στον GDPR, χωρίς βέβαια να καλύπτει απόλυτα όλες τις απαιτήσεις
- ✓ στο Annex A control, A.18.1.4 Ιδιωτικότητα & Προστασία Προσωπικών Δεδομένων Ταυτοποίησης (PII) απαιτεί από τους οργανισμούς να προστατεύουν την PII σύμφωνα με τη σχετική νομοθεσία και κανονισμούς
- ✓ συνιστά εφαρμογή κατάλληλων οργανωτικών και τεχνικών ελέγχων.

ALPHA PLAN consultants

Μηχανισμοί Συμμόρφωσης (2/2)

PRIVACY SEAL

- ✓ αποτελεί αναγνώριση από φορείς πιστοποίησης ότι ένα προϊόν ή μια διαδικασία συμμορφώνεται με τις διατάξεις της εκάστοτε νομοθεσίας για την προστασία των δεδομένων
- ✓ προσφέρει διάφορες σφραγίδες για την πιστοποίηση των προϊόντων/ ιδιωτικού απορρήτου
- ✓ αποδεικνύει τη συμμόρφωσή και ενισχύει την εμπιστοσύνη των πελατών, των επενδυτών και των επιχειρηματικών συνεργατών ενός οργανισμού με αναγνωρισμένη σφραγίδα απορρήτου!

ALPHA PLAN consultants

Ευχαριστούμε για τον χρόνο σας

ALPHA PLAN consultants